A. Introduction

1. **Title:** **Real Power Balancing Control Performance**

2. **Number:** **BAL-001-2**

3. **Purpose:** To control Interconnection frequency within defined limits.

4. **Applicability:**

   4.1. Balancing Authority

   4.1.1 A Balancing Authority receiving Overlap Regulation Service is not subject to Control Performance Standard 1 (CPS1) or Balancing Authority ACE Limit (BAAL) compliance evaluation.

   4.1.2 A Balancing Authority that is a member of a Regulation Reserve Sharing Group is the Responsible Entity only in periods during which the Balancing Authority is not in active status under the applicable agreement or the governing rules for the Regulation Reserve Sharing Group.

   4.2. Regulation Reserve Sharing Group

5. **(Proposed) Effective Date:**

   5.1. First day of the first calendar quarter that is twelve months beyond the date that this standard is approved by applicable regulatory authorities, or in those jurisdictions where regulatory approval is not required, the standard becomes effective the first day of the first calendar quarter that is twelve months beyond the date this standard is approved by the NERC Board of Trustees, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

B. Requirements

R1. The Responsible Entity shall operate such that the Control Performance Standard 1 (CPS1), calculated in accordance with Attachment 1, is greater than or equal to 100 percent for the applicable Interconnection in which it operates for each preceding 12 consecutive calendar month period, evaluated monthly. *[Violation Risk Factor: Medium] [Time Horizon: Real-time Operations]*

R2. Each Balancing Authority shall operate such that its clock-minute average of Reporting ACE does not exceed its clock-minute Balancing Authority ACE Limit (BAAL) for more than 30 consecutive clock-minutes, calculated in accordance with Attachment 2, for the applicable Interconnection in which the Balancing Authority operates.*[Violation Risk Factor: Medium] [Time Horizon: Real-time Operations]*

C. Measures

M1. The Responsible Entity shall provide evidence, upon request, such as dated calculation output from spreadsheets, system logs, software programs, or other evidence (either in hard copy or electronic format) to demonstrate compliance with Requirement R1.

M2. Each Balancing Authority shall provide evidence, upon request, such as dated calculation output from spreadsheets, system logs, software programs, or other evidence (either in hard copy or electronic format) to demonstrate compliance with Requirement R2.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Data Retention

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The Responsible Entity shall retain data or evidence to show compliance for the current year, plus three previous calendar years unless, directed by its Compliance Enforcement Authority, to retain specific evidence for a longer period of time as part of an investigation. Data required for the calculation of Regulation Reserve Sharing Group Reporting Ace, or Reporting ACE, CPS1, and BAAL shall be retained in digital format at the same scan rate at which the Reporting ACE is calculated for the current year, plus three previous calendar years.

If a Responsible Entity is found noncompliant, it shall keep information related to the noncompliance until found compliant, or for the time period specified above, whichever is longer.

The Compliance Enforcement Authority shall keep the last audit records and all subsequent requested and submitted records.

1.3. Compliance Monitoring and Assessment Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Investigation

Self-Reporting

Complaints

1.4. Additional Compliance Information

None.

2. Violation Severity Levels

R #	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	The CPS 1 value of the Responsible Entity, for the preceding 12 consecutive calendar month period, is less than 100 percent but greater than or equal to 95 percent for the applicable Interconnection.	The CPS 1 value of the Responsible Entity, for the preceding 12 consecutive calendar month period, is less than 95 percent, but greater than or equal to 90 percent for the applicable Interconnection.	The CPS 1 value of the Responsible Entity, for the preceding 12 consecutive calendar month period, is less than 90 percent, but greater than or equal to 85 percent for the applicable Interconnection.	The CPS 1 value of the Responsible Entity, for the preceding 12 consecutive calendar month period, is less than 85 percent for the applicable Interconnection.
R2	The Balancing Authority exceeded its clock-minute BAAL for more than 30 consecutive clock minutes but for 45 consecutive clock-minutes or less for the applicable Interconnection.	The Balancing Authority exceeded its clock-minute BAAL for greater than 45 consecutive clock minutes but for 60 consecutive clock-minutes or less for the applicable Interconnection.	The Balancing Authority exceeded its clock-minute BAAL for greater than 60 consecutive clock minutes but for 75 consecutive clock-minutes or less for the applicable Interconnection.	The Balancing Authority exceeded its clock-minute BAAL for greater than 75 consecutive clock-minutes for the applicable Interconnection.

E. Regional Variances

None.

F. Associated Documents

BAL-001-2, Real Power Balancing Control Performance Standard Background Document

Version History

Version	Date	Action	Change Tracking
0	February 8, 2005	BOT Approval	New
0	April 1, 2005	Effective Implementation Date	New
0	August 8, 2005	Removed "Proposed" from Effective Date	Errata
0	July 24, 2007	Corrected R3 to reference M1 and M2 instead of R1 and R2	Errata
0a	December 19, 2007	Added Appendix 2 – Interpretation of R1 approved by BOT on October 23, 2007	Revised
0a	January 16, 2008	In Section A.2., Added "a" to end of standard number In Section F, corrected automatic numbering from "2" to "1" and removed "approved" and added parenthesis to "(October 23, 2007)"	Errata
0	January 23, 2008	Reversed errata change from July 24, 2007	Errata
0.1a	October 29, 2008	Board approved errata changes; updated version number to "0.1a"	Errata
0.1a	May 13, 2009	Approved by FERC	
1		Inclusion of BAAL and WECC Variance and exclusion of CPS2	Revision
1	December 19, 2012	Adopted by NERC Board of Trustees	
2	August 15, 2013	Adopted by the NERC Board of Trustees	

Attachment 1
Equations Supporting Requirement R1 and Measure M1

CPS1 is calculated as follows:

$$CPS1 = (2 - CF) * 100\%$$

The frequency-related compliance factor (CF), is a ratio of the accumulating clock-minute compliance parameters for the most recent preceding 12 consecutive calendar months, divided by the square of the target frequency bound:

$$CF = \frac{CF_{12\text{- month}}}{(\varepsilon 1_I)^2}$$

Where $\varepsilon 1_I$ is the constant derived from a targeted frequency bound for each Interconnection as follows:

- Eastern Interconnection $\varepsilon 1_I = 0.018$ Hz
- Western Interconnection $\varepsilon 1_I = 0.0228$ Hz
- ERCOT Interconnection $\varepsilon 1_I = 0.030$ Hz
- Quebec Interconnection $\varepsilon 1_I = 0.021$ Hz

The rating index $CF_{12\text{-month}}$ is derived from the most recent preceding 12 consecutive calendar months of data. The accumulating clock-minute compliance parameters are derived from the one-minute averages of Reporting ACE, Frequency Error, and Frequency Bias Settings.

A clock-minute average is the average of the reporting Balancing Authority's valid measured variable (i.e., for Reporting ACE (RACE) and for Frequency Error) for each sampling cycle during a given clock-minute.

$$\left(\frac{RACE}{-10B}\right)_{\text{clock-minute}} = \frac{\left(\frac{\sum RACE_{\text{sampling cycles in clock-minute}}}{n_{\text{sampling cycles in clock-minute}}}\right)}{\text{-10B}}$$

And,

$$\Delta F_{\text{clock-minute}} = \frac{\sum \Delta F_{\text{sampling cycles in clock-minute}}}{n_{\text{sampling cycles in clock-minute}}}$$

The Balancing Authority's clock-minute compliance factor ($CF_{\text{clock-minute}}$) calculation is:

$$CF_{\text{clock-minute}} = \left[\left(\frac{RACE}{-10B} \right)_{\text{clock-minute}} * \Delta F_{\text{clock-minute}} \right]$$

Normally, 60 clock-minute averages of the reporting Balancing Authority's Reporting ACE and Frequency Error will be used to compute the hourly average compliance factor ($CF_{\text{clock-hour}}$).

$$CF_{\text{clock-hour}} = \frac{\sum CF_{\text{clock-minute}}}{n_{\text{clock-minute samples in hour}}}$$

The reporting Balancing Authority shall be able to recalculate and store each of the respective clock-hour averages ($CF_{\text{clock-hour average-month}}$) and the data samples for each 24-hour period (one for each clock-hour; i.e., hour ending (HE) 0100, HE 0200, ..., HE 2400). To calculate the monthly compliance factor (CF_{month}):

$$\text{CF}_{\text{clock-hour average-month}} = \frac{\sum_{\text{days-in-month}} [(\text{CF}_{\text{clock-hour}})(n_{\text{one-minute samples in clock-hour}})]}{\sum_{\text{days-in month}} [n_{\text{one-minute samples in clock-hour}}]}$$

$$\text{CF}_{\text{month}} = \frac{\sum_{\text{hours-in-day}} [(\text{CF}_{\text{clock-hour average-month}})(n_{\text{one-minute samples in clock-hour averages}})]}{\sum_{\text{hours-in day}} [n_{\text{one-minute samples in clock-hour averages}}]}$$

To calculate the 12-month compliance factor ($CF_{\text{12 month}}$):

$$\text{CF}_{\text{12-month}} = \frac{\sum_{\text{i=1}}^{12} (CF_{\text{month-i}})(n_{(\text{one-minute samples in month})-\text{i}})]}{\sum_{\text{i=1}}^{12} [n_{(\text{one-minute samples in month})\text{-i}}]}$$

To ensure that the average Reporting ACE and Frequency Error calculated for any one-minute interval is representative of that time interval, it is necessary that at least 50 percent of both the Reporting ACE and Frequency Error sample data during the one-minute interval is valid. If the recording of Reporting ACE or Frequency Error is interrupted such that less than 50 percent of the one-minute sample period data is available or valid, then that one-minute interval is excluded from the CPS1 calculation.

A Balancing Authority providing Overlap Regulation Service to another Balancing Authority calculates its CPS1 performance after combining its Reporting ACE and Frequency Bias

Settings with the Reporting ACE and Frequency Bias Settings of the Balancing Authority receiving the Regulation Service.

Attachment 2

Equations Supporting Requirement R2 and Measure M2

When actual frequency is equal to Scheduled Frequency, $BAAL_{High}$ and $BAAL_{Low}$ do not apply.

When actual frequency is less than Scheduled Frequency, $BAAL_{High}$ does not apply, and $BAAL_{Low}$ is calculated as:

$$BAAL_{Low} = \left(-10B_i \times \left(FTL_{Low} - F_S\right)\right) \times \frac{\left(FTL_{Low} - F_S\right)}{\left(F_A - F_S\right)}$$

When actual frequency is greater than Scheduled Frequency, $BAAL_{Low}$ does not apply and the $BAAL_{High}$ is calculated as:

$$BAAL_{High} = \left(-10B_i \times \left(FTL_{High} - F_S\right)\right) \times \frac{\left(FTL_{High} - F_S\right)}{\left(F_A - F_S\right)}$$

Where**:**

$BAAL_{Low}$ is the Low Balancing Authority ACE Limit (MW)

$BAAL_{High}$ is the High Balancing Authority ACE Limit (MW)

10 is a constant to convert the Frequency Bias Setting from MW/0.1 Hz to MW/Hz

B_i is the Frequency Bias Setting for a Balancing Authority (expressed as MW/0.1 Hz)

F_A is the measured frequency in Hz.

F_S is the scheduled frequency in Hz.

FTL_{Low} is the Low Frequency Trigger Limit (calculated as F_S - $3\varepsilon 1_I$ Hz)

FTL_{High} is the High Frequency Trigger Limit (calculated as F_S + $3\varepsilon 1_I$ Hz)

Where $\varepsilon 1_I$ is the constant derived from a targeted frequency bound for each Interconnection as follows:

- Eastern Interconnection $\varepsilon 1_I$ = 0.018 Hz
- Western Interconnection $\varepsilon 1_I$ = 0.0228 Hz
- ERCOT Interconnection $\varepsilon 1_I$ = 0.030 Hz
- Quebec Interconnection $\varepsilon 1_I$ = 0.021 Hz

To ensure that the average actual frequency calculated for any one-minute interval is representative of that time interval, it is necessary that at least 50% of the actual frequency sample data during that one-minute interval is valid. If the recording of actual frequency is interrupted such that less than 50 percent of the one-minute sample period

data is available or valid, then that one-minute interval is excluded from the BAAL calculation and the 30-minute clock would be reset to zero.

A Balancing Authority providing Overlap Regulation Service to another Balancing Authority calculates its BAAL performance after combining its Frequency Bias Setting with the Frequency Bias Setting of the Balancing Authority receiving Overlap Regulation Service.

Appendix QC-BAL-001-2
Provisions specific to the standard BAL-001-2 applicable in Québec

This appendix establishes specific provisions for the application of the standard in Québec. Provisions of the standard and of its appendix must be read together for the purposes of understanding and interpretation. Where the standard and appendix differ, the appendix shall prevail.

A. Introduction

1. Title: Real Power Balancing Control Performance

2. Number: BAL-001-2

3. Purpose: No specific provision

4. Applicability: No specific provision

5. Effective Date:

5.1. Adoption of the standard by the Régie de l'énergie: February 3, 2017

5.2. Adoption of the appendix by the Régie de l'énergie: February 3, 2017

5.3. Effective date of the standard and its appendix in Québec: April 1, 2017

B. Requirements

No specific provision

C. Measures

No specific provision

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

The Régie de l'énergie is responsible, in Québec, for compliance enforcement with respect to the reliability standard and its appendix that it adopts.

1.2. Data Retention

No specific provision

1.3. Compliance Monitoring and Assessment Processes

No specific provision

1.4. Additional Compliance Information

No specific provision

2. Violation Severity Levels

No specific provision

E. Regional Variances

No specific provision

F. Associated Documents

No specific provision

Attachment 1

No specific provision

Attachment 2

No specific provision

Revision History

Revision	Adoption Date	Action	Change Tracking
0	February 3, 2017	New appendix	New

A. Introduction

1. **Title:** Disturbance Control Standard – Contingency Reserve for Recovery from a Balancing Contingency Event

2. **Number:** BAL-002-3

3. **Purpose:** To ensure the Balancing Authority or Reserve Sharing Group balances resources and demand and returns the Balancing Authority's or Reserve Sharing Group's Area Control Error to defined values (subject to applicable limits) following a Reportable Balancing Contingency Event.

4. **Applicability:**

   4.1. Responsible Entity

   4.1.1. Balancing Authority

   4.1.1.1. A Balancing Authority that is a member of a Reserve Sharing Group is the Responsible Entity only in periods during which the Balancing Authority is not in active status under the applicable agreement or governing rules for the Reserve Sharing Group.

   4.1.2. Reserve Sharing Group

5. **Effective Date:** See the Implementation Plan for BAL-002-3.

B. Requirements and Measures

R1. The Responsible Entity experiencing a Reportable Balancing Contingency Event shall: *[Violation Risk Factor: High] [Time Horizon: Real-time Operations]*

1.1. within the Contingency Event Recovery Period, demonstrate recovery by returning its Reporting ACE to at least the recovery value of:

- zero (if its Pre-Reporting Contingency Event ACE Value was positive or equal to zero); however, any Balancing Contingency Event that occurs during the Contingency Event Recovery Period shall reduce the required recovery: (i) beginning at the time of, and (ii) by the magnitude of, such individual Balancing Contingency Event,

or,

- its Pre-Reporting Contingency Event ACE Value (if its Pre-Reporting Contingency Event ACE Value was negative); however, any Balancing Contingency Event that occurs during the Contingency Event Recovery Period shall reduce the required recovery: (i) beginning at the time of, and (ii) by the magnitude of, such individual Balancing Contingency Event.

1.2. document all Reportable Balancing Contingency Events using CR Form 1.

1.3. deploy Contingency Reserve, within system constraints, to respond to all Reportable Balancing Contingency Events, however, it is not subject to compliance with Requirement R1 part 1.1 if the Responsible Entity:

1.3.1 is (i) a Balancing Authority or (ii) a Reserve Sharing Group with at least one member that:

- is experiencing a Reliability Coordinator declared Energy Emergency Alert Level, and
- is utilizing its Contingency Reserve to mitigate an operating emergency in accordance with its emergency Operating Plan, and
- has depleted its Contingency Reserve to a level below its Most Severe Single Contingency, and
- has, during communications with its Reliability Coordinator in accordance with the Energy Emergency Alert procedures, (i) notified the Reliability Coordinator of the conditions described in the preceding two bullet points preventing the Responsible Entity from complying with Requirement R1 part 1.1, and (ii) provided the Reliability Coordinator with an ACE recovery plan, including target recovery time

or,

1.3.2 the Responsible Entity experiences:

- multiple Contingencies where the combined MW loss exceeds its Most Severe Single Contingency and that are defined as a single Balancing Contingency Event, or
- multiple Balancing Contingency Events within the sum of the time periods defined by the Contingency Event Recovery Period and Contingency Reserve Restoration Period whose combined magnitude exceeds the Responsible Entity's Most Severe Single Contingency.

M1. Each Responsible Entity shall have, and provide upon request, as evidence, a CR Form 1 with date and time of occurrence to show compliance with Requirement R1. If Requirement R1 part 1.3 applies, then dated documentation that demonstrates compliance with Requirement R1 part 1.3 must also be provided.

R2. Each Responsible Entity shall develop, review and maintain annually, and implement an Operating Process as part of its Operating Plan to determine its Most Severe Single Contingency and make preparations to have Contingency Reserve equal to, or greater than the Responsible Entity’s Most Severe Single Contingency available for maintaining system reliability. *[Violation Risk Factor: High] [Time Horizon: Operations Planning]*

M2. Each Responsible Entity will have the following documentation to show compliance with Requirement R2:

- a dated Operating Process;
- evidence to indicate that the Operating Process has been reviewed and maintained annually; and,
- evidence such as Operating Plans or other operator documentation that demonstrate that the entity determines its Most Severe Single Contingency and that Contingency Reserves equal to or greater than its Most Severe Single Contingency are included in this process.

R3. Each Responsible Entity, following a Reportable Balancing Contingency Event, shall restore its Contingency Reserve to at least its Most Severe Single Contingency, before the end of the Contingency Reserve Restoration Period, but any Balancing Contingency Event that occurs before the end of a Contingency Reserve Restoration Period resets the beginning of the Contingency Event Recovery Period. *[Violation Risk Factor: Medium] [Time Horizon: Real-time Operations]*

M3. Each Responsible Entity will have documentation demonstrating its Contingency Reserve was restored within the Contingency Reserve Restoration Period, such as historical data, computer logs or operator logs.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

"Compliance Enforcement Authority" means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention

The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The Responsible Entity shall retain data or evidence to show compliance for the current year, plus three previous calendar years, unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

If a Responsible Entity is found noncompliant, it shall keep information related to the noncompliance until found compliant, or for the time period specified above, whichever is longer.

The Compliance Enforcement Authority shall keep the last audit records and all subsequent requested and submitted records.

1.3. Compliance Monitoring and Assessment Processes:

As defined in the NERC Rules of Procedure, "Compliance Monitoring and Assessment Processes" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

1.4. Additional Compliance Information

The Responsible Entity may use Contingency Reserve for any Balancing Contingency Event and as required for any other applicable standards.

Table of Compliance Elements

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	The Responsible Entity achieved less than 100% but at least 90% of required recovery from a Reportable Balancing Contingency Event during the Contingency Event Recovery Period OR The Responsible Entity failed to use CR Form 1 to document a Reportable Balancing Contingency Event.	The Responsible Entity achieved less than 90% but at least 80% of required recovery from a Reportable Balancing Contingency Event during the Contingency Event Recovery Period.	The Responsible Entity achieved less than 80% but at least 70% of required recovery from a Reportable Balancing Contingency Event during the Contingency Event Recovery Period.	The Responsible Entity achieved less than 70% of required recovery from a Reportable Balancing Contingency Event during the Contingency Event Recovery Period.
R2.	The Responsible Entity developed and implemented an Operating Process to determine its Most Severe Single Contingency and to have Contingency Reserve equal to, or greater than the Responsible Entity's Most Severe Single Contingency but failed to maintain	N/A	The Responsible Entity developed an Operating Process to determine its Most Severe Single Contingency and to have Contingency Reserve equal to, or greater than the Responsible Entity's Most Severe Single Contingency but failed to implement the Operating Process.	The Responsible Entity failed to develop an Operating Process to determine its Most Severe Single Contingency and to have Contingency Reserve equal to, or greater than the Responsible Entity's Most Severe Single Contingency.

	annually the Operating Process.			
R3.	The Responsible Entity restored less than 100% but at least 90% of required Contingency Reserve following a Reportable Balancing Contingency Event during the Contingency Event Restoration Period.	The Responsible Entity restored less than 90% but at least 80% of required Contingency Reserve following a Reportable Balancing Contingency Event during the Contingency Event Restoration Period.	The Responsible Entity restored less than 80% but at least 70% of required Contingency Reserve following a Reportable Balancing Contingency Event during the Contingency Event Restoration Period.	The Responsible Entity restored less than 70% of required Contingency Reserve following a Reportable Balancing Contingency Event during the Contingency Event Restoration Period.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

CR Form 1

BAL-002-3 Rationales

Version History

Version	Date	Action	Change Tracking
0	April 1, 2005	Effective Date	New
0	August 8, 2005	Removed "Proposed" from Effective Date	Errata
0	February 14, 2006	Revised graph on page 3, "10 min." to "Recovery time." Removed fourth bullet.	Errata
1	September 9, 2010	Filed petition for revisions to BAL-002 Version 1 with the Commission	Revision
1	January 10, 2011	FERC letter ordered in Docket No. RD10-15-00 approving BAL-002-1	
1	April 1, 2012	Effective Date of BAL-002-1	
1a	November 7, 2012	Interpretation adopted by the NERC Board of Trustees	
1a	February 12, 2013	Interpretation submitted to FERC	
2	November 5, 2015	Adopted by NERC Board of Trustees	Complete revision
2	January 19, 2017	FERC Order approved BAL-002-2. Docket No. RM16-7-000	
2	October 2, 2017	FERC letter Order issued approving raising the VRF for Requirement R1 and R2 from Medium to High. Docket No. RD17-6-000.	
3	August 16, 2018	Adopted by NERC Board of Trustees	Revisions to address two FERC directives from Order No. 835
3	September 25, 2018	FERC Order approving BAL-002-3. Docket No. RD18-7-000	

Appendix QC-BAL-002-3
Provisions specific to the standard BAL-002-3 applicable in Québec

This appendix establishes specific provisions for the application of the standard in Québec. Provisions of the standard and of its appendix must be read together for the purposes of understanding and interpretation. Where the standard and appendix differ, the appendix shall prevail.

A. Introduction

1. Title: Disturbance Control Standard – Contingency Reserve for Recovery from a Balancing Contingency Event

2. Number: BAL-002-3

3. Purpose: No specific provision

4. Applicability: No specific provision

5. Effective Date:

5.1. Adoption of the standard by the Régie de l'énergie: June 8, 2020

5.2. Adoption of the appendix by the Régie de l'énergie: June 8, 2020

5.3. Effective date of the standard and its appendix in Québec: April 1, 2021

B. Requirements and Mesures

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

The Régie de l'énergie is responsible, in Québec, for compliance enforcement with respect to the reliability standard and its appendix that it adopts.

1.2. Evidence Retention

No specific provision

1.3. Compliance Monitoring and Assessment Processes

The Québec Reliability Standards Compliance Monitoring and Enforcement Program (QCMEP) of the Régie de l'énergie identifies the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

1.4. Additional Compliance Information

No specific provision

Table of Compliance Elements

No specific provision

D. Regional Differences

No specific provision

E. Interpretations

No specific provision

Appendix QC-BAL-002-3
Provisions specific to the standard BAL-002-3 applicable in Québec

F. Associated Documents

No specific provision

Revision History

Revision	Date	Action	Change Tracking
0	June 8, 2020	New appendix	New

A. Introduction

1. **Title: Frequency Response and Frequency Bias Setting**

2. **Number: BAL-003-2**

3. **Purpose:** To require sufficient Frequency Response from the Balancing Authority (BA) to maintain Interconnection Frequency within predefined bounds by arresting frequency deviations and supporting frequency until the frequency is restored to its scheduled value. To provide consistent methods for measuring Frequency Response and determining the Frequency Bias Setting.

4. **Applicability:**

   4.1. Functional Entities:

   4.1.1. Balancing Authority

   4.1.1.1. Balancing Authority is the responsible entity unless the Balancing Authority is a member of a Frequency Response Sharing Group, in which case, the Frequency Response Sharing Group becomes the responsible entity.

   4.1.2. Frequency Response Sharing Group

5. **Effective Date:** See Implementation Plan for BAL-003-2.

B. Requirements and Measures

R1. Each Frequency Response Sharing Group (FRSG) or Balancing Authority that is not a member of a FRSG shall achieve an annual Frequency Response Measure (FRM) (as calculated and reported in accordance with Attachment A) that is equal to or more negative than its Frequency Response Obligation (FRO) to ensure that sufficient Frequency Response is provided by each FRSG or BA that is not a member of a FRSG to maintain Interconnection Frequency Response equal to or more negative than the Interconnection Frequency Response Obligation. *[Risk Factor: High][Time Horizon: Real-time Operations]*

M1. Each Frequency Response Sharing Group or Balancing Authority that is not a member of a Frequency Response Sharing Group shall have evidence such as dated data plus documented formula in either hardcopy or electronic format that it achieved an annual FRM (in accordance with the methods specified by the ERO in Attachment A with data from FRS Form 1 reported to the ERO as specified in Attachment A) that is equal to or more negative than its FRO to demonstrate compliance with Requirement R1.

R2. Each Balancing Authority that is a member of a multiple Balancing Authority Interconnection and is not receiving Overlap Regulation Service and uses a fixed Frequency Bias Setting shall implement the Frequency Bias Setting determined in

accordance with Attachment A, as validated by the ERO, into its Area Control Error (ACE) calculation during the implementation period specified by the ERO and shall use this Frequency Bias Setting until directed to change by the ERO. *[Risk Factor: Medium][Time Horizon: Operations Planning]*

M2. The Balancing Authority that is a member of a multiple Balancing Authority Interconnection and is not receiving Overlap Regulation Service shall have evidence such as a dated document in hard copy or electronic format showing the ERO validated Frequency Bias Setting was implemented into its ACE calculation within the implementation period specified or other evidence to demonstrate compliance with Requirement R2.

R3. Each Balancing Authority that is a member of a multiple Balancing Authority Interconnection and is not receiving Overlap Regulation Service and is utilizing a variable Frequency Bias Setting shall maintain a Frequency Bias Setting that is: *[Risk Factor: Medium][Time Horizon: Operations Planning]*

3.1 Less than zero at all times, and

3.2 Equal to or more negative than its Frequency Response Obligation when Frequency varies from 60 Hz by more than +/- 0.036 Hz.

M3. The Balancing Authority that is a member of a multiple Balancing Authority Interconnection, is not receiving Overlap Regulation Service and is utilizing variable Frequency Bias shall have evidence such as a dated report in hard copy or electronic format showing the average clock-minute average Frequency Bias Setting was less than zero and during periods when the clock-minute average frequency was outside of the range 59.964 Hz to 60.036 Hz was equal to or more negative than its Frequency Response Obligation to demonstrate compliance with Requirement R3.

R4. Each Balancing Authority that is performing Overlap Regulation Service shall modify its Frequency Bias Setting in its ACE calculation, in order to represent the Frequency Bias Setting for the combined Balancing Authority Area, to be equivalent to either: *[Risk Factor: Medium][Time Horizon: Operations Planning]*

- The sum of the Frequency Bias Settings as shown on FRS Form 1 and FRS Form 2 for the participating Balancing Authorities as validated by the ERO, or

- The Frequency Bias Setting shown on FRS Form 1 and FRS Form 2 for the entirety of the participating Balancing Authorities' Areas.

M4. The Balancing Authority shall have evidence such as a dated operating log, database or list in hard copy or electronic format showing that when it performed Overlap Regulation Service, it modified its Frequency Bias Setting in its ACE calculation as specified in Requirement R4 to demonstrate compliance with Requirement R4.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: "Compliance Enforcement Authority" means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

- The Balancing Authority shall retain data or evidence to show compliance with Requirements R1, R2, R3 and R4, Measures M1, M2, M3 and M4 for the current year plus the previous three calendar years unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.
- The Frequency Response Sharing Group shall retain data or evidence to show compliance with Requirement R1 and Measure M1 for the current year plus the previous three calendar years unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.
- If a Balancing Authority or Frequency Response Sharing Group is found non-compliant, it shall keep information related to the non-compliance until found compliant or for the time period specified above, whichever is longer.
- The Compliance Enforcement Authority shall keep the last audit records and all subsequent requested and submitted records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

- For Interconnections that are also Balancing Authorities, Tie Line Bias control and flat frequency control are equivalent and either is acceptable.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	The Balancing Authority's, or Frequency Response Sharing Group's, FRM was less negative than its FRO by at most 15% or 15 MW/0.1 Hz, whichever one is the greater deviation from its FRO.	The Balancing Authority's, or Frequency Response Sharing Group's, FRM was less negative than its FRO by more than 15% but by at most 30% or 30 MW/0.1 Hz, whichever is the greater deviation from its FRO.	The Balancing Authority's, or Frequency Response Sharing Group's, FRM was less negative than its FRO by more than 30% but by at most 45% or 45 MW/0.1 Hz, whichever one is the greater deviation from its FRO.	The Balancing Authority's, or Frequency Response Sharing Group's, FRM was less negative than its FRO by more than 45% or by more than 45 MW/0.1 Hz, whichever is the greater deviation from its FRO.
R2.	The Balancing Authority in a multiple Balancing Authority Interconnection and not receiving Overlap Regulation Service and uses a fixed Frequency Bias Setting failed to implement the validated Frequency Bias Setting value into its ACE calculation within the implementation period specified but did so within 5 calendar days from the implementation period specified by the ERO.	The Balancing Authority in a multiple Balancing Authority Interconnection and not receiving Overlap Regulation Service and uses a fixed Frequency Bias Setting implemented the validated Frequency Bias Setting value into its ACE calculation in more than 5 calendar days but less than or equal to 15 calendar days from the implementation period specified by the ERO.	The Balancing Authority in a multiple Balancing Authority Interconnection and not receiving Overlap Regulation Service and uses a fixed Frequency Bias Setting implemented the validated Frequency Bias Setting value into its ACE calculation in more than 15 calendar days but less than or equal to 25 calendar days from the implementation period specified by the ERO.	The Balancing Authority in a multiple Balancing Authority Interconnection and not receiving Overlap Regulation Service and uses a fixed Frequency Bias Setting did not implement the validated Frequency Bias Setting value into its ACE calculation in more than 25 calendar days from the implementation period specified by the ERO.

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R3.	The Balancing Authority that is a member of a multiple Balancing Authority Interconnection and is not receiving Overlap Regulation Service and uses a variable Frequency Bias Setting average Frequency Bias Setting during periods when the clock-minute average frequency was outside of the range 59.964 Hz to 60.036 Hz was less negative than its Frequency Response Obligation by more than 1% but by at most 10%.	The Balancing Authority that is a member of a multiple Balancing Authority Interconnection and not receiving Overlap Regulation Service and uses a variable Frequency Bias Setting average Frequency Bias Setting during periods when the clock-minute average frequency was outside of the range 59.964 Hz to 60.036 Hz was less negative than its Frequency Response Obligation by more than 10% but by at most 20%.	The Balancing Authority that is a member of a multiple Balancing Authority Interconnection and not receiving Overlap Regulation Service and uses a variable Frequency Bias Setting average Frequency Bias Setting during periods when the clock-minute average frequency was outside of the range 59.964 Hz to 60.036 Hz was less negative than its Frequency Response Obligation by more than 20% but by at most 30%.	The Balancing Authority that is a multiple Balancing Authority Interconnection and not receiving Overlap Regulation Service and uses a variable Frequency Bias Setting average Frequency Bias Setting during periods when the clock-minute average frequency was outside of the range 59.964 Hz to 60.036 Hz was less negative than its Frequency Response obligation by more than 30%.
R4.	The Balancing Authority incorrectly changed the Frequency Bias Setting value used in its ACE calculation when providing Overlap Regulation Services with combined footprint setting-error less than or equal to 10% of the validated or calculated value.	The Balancing Authority incorrectly changed the Frequency Bias Setting value used in its ACE calculation when providing Overlap Regulation Services with combined footprint setting-error more than 10% but less than or equal to 20% of the	The Balancing Authority incorrectly changed the Frequency Bias Setting value used in its ACE calculation when providing Overlap Regulation Services with combined footprint setting-error more than 20% but less than or equal to 30% of the	The Balancing Authority incorrectly changed the Frequency Bias Setting value used in its ACE calculation when providing Overlap Regulation Services with combined footprint setting-error more than 30% of the validated or calculated value. OR

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		validated or calculated value.	validated or calculated value.	The Balancing Authority failed to change the Frequency Bias Setting value used in its ACE calculation when providing Overlap Regulation Services.

D. Regional Variances

None.

E. Associated Documents

Procedure for ERO Support of Frequency Response and Frequency Bias Setting Standard

FRS Form 1

FRS Form 2

Frequency Response Standard Background Document

Version History

Version	Date	Action	Change Tracking
0	April 1, 2005	Effective Date	New
0	August 8, 2005	Removed "Proposed" from Effective Date	Errata
0	March 16, 2007	FERC Approval — Order 693	New
0a	December 19, 2007	Added Appendix 1 — Interpretation of R3 approved by BOT on October 23, 2007	Addition
0a	July 21, 2008	FERC Approval of Interpretation of R3	Addition
0b	February 12, 2008	Added Appendix 2 — Interpretation of R2, R2.2, R5, and R5.1 approved by BOT on February 12, 2008	Addition
0.1b	January 16, 2008	Section F: added “1.”; changed hyphen to “en dash.” Changed font style for “Appendix 1” to Arial; updated version number to “0.1b”	Errata
0.1b	October 29, 2008	BOT approved errata changes	Errata
0.1a	May 13, 2009	FERC Approved errata changes – version changed to 0.1a (Interpretation of R2, R2.2, R5, and R5.1 not yet approved)	Errata
0.1b	May 21, 2009	FERC Approved Interpretation of R2, R2.2, R5, and R5.1	Addition
1	February 7, 2013	Adopted by NERC Board of Trustees	Complete Revision under Project 2007-12
1	January 16, 2014	FERC Order issued approving BAL-003-1. (Order becomes effective for R2, R3, and R4 April 1, 2015. R1 becomes effective April 1, 2016.)	
1	May 7, 2014	NERC Board of Trustees adopted revisions to VRF and VSLs in Requirement R1.	
1	November 26, 2014	FERC issued a letter order approved VRF and VSL revisions to Requirement R1.	

Version	Date	Action	Change Tracking
1.1	August 25, 2015	Added numbering to Introduction section, corrected parts numbering for R3, and adjusted font within section M4.	Errata
1.1	November 13, 2015	FERC Letter Order approved errata to BAL-003-1.1. Docket RD15-6-000	Errata
2	November 5, 2019	NERC Board of Trustees adopted BAL-003-2	New
2	July 15, 2020	FERC Letter Order approved errata to BAL-003-2. Docket RD20-9-000	

Attachment A

BAL-003-2 Frequency Response and Frequency Bias Setting Standard

Supporting Document

Interconnection Frequency Response Obligation

The ERO, in consultation with regional representatives, has established a target reliability criterion for each Interconnection called the Interconnection Frequency Response Obligation (IFRO). Preliminary values are provided below. Certain values are assessed annually according to the methodology which is detailed in the *Procedure for ERO Support of Frequency Response and Frequency Bias Setting Standard*.

Interconnection	**Eastern**	**Western**	**ERCOT**	**HQ**	Units
Max. Delta Frequency (MDF)	**0.420**	**0.280**	**0.405**	**0.947**	
Resource Loss Protection Criteria (RLPC)[1]	**3,209**	**2,850**	**2,750**	**2,000**	MW
Credit for Load Resources (CLR)			**1,209**		MW
Current IFRO (OY 2018)	**-1,015**	**-858**	**-381**	**-179**	MW/0.1 Hz
First-Step target IFRO[1]	**-915**	**-1018**	**-380**	**-211**	MW/0.1 Hz
Second-Step target IFRO[1, 2]	**-815**				
Final target IFRO[1, 2]	**-787**				

Table 1: Interconnection Frequency Response Obligations (base year 2017)

IFRO = (RLPC – CLR)/Max Delta Freq/10

1. *These values are evaluated annually for changes in each Interconnection.*
2. *To reduce risk, the Eastern Interconnection IFRO will be stepped down annually from the 2017 value of -1,015 MW/0.1 Hz in -100 MW/0.1 Hz increments. If during the step down process, Interconnection Frequency Response Measure (FRM) declines by more than 10 percent, the ERO will halt the reduction in IFRO until such time that a determination can be made as to the cause of the degradation.*

Balancing Authority Frequency Response Obligation and Frequency Bias Setting

For a multiple Balancing Authority interconnection, the Interconnection FRO shown in Table 1 is allocated based on the Balancing Authority annual load and annual generation. The FRO allocation will be based on the following method:

$$\text{FRO}_{\text{BA}} = \text{IFRO} \quad \times \frac{\text{Annual Gen}_{\text{BA}} + \text{Annual Load}_{\text{BA}}}{\text{Annual Gen}_{\text{Int}} + \text{Annual Load}_{\text{Int}}}$$

Where:

- Annual Gen_{BA} is the total annual output of generating plants within the Balancing Authority Area (BAA).
- Annual Load_{BA} is total annual Load within the BAA.
- Annual Gen_{Int} is the sum of all Annual Gen_{BA} values reported in that interconnection.
- Annual Load_{Int} is the sum of all Annual Load_{BA} values reported in that interconnection.

Balancing Authorities that elect to form a FRSG will calculate a FRSG FRO by adding together the individual BA FRO's.

Balancing Authorities that elect to form a FRSG as a means to jointly meet the FRO will calculate their FRM performance one of two ways:

- Calculate a group NI_{A} and measure the group response to all events in the reporting year on a single FRS Form 1, or
- Submit a joint Form 1 with the "FRSG" tab completed for the aggregate performance of the participating Balancing Authorities.

Balancing Authorities that merge or transfer load or generation are encouraged to notify the ERO of the change in footprint and corresponding changes in allocation such that the net obligation to the Interconnection remains the same and so that CPS limits can be adjusted.

Each Balancing Authority reports its previous year's FRM, Frequency Bias Setting and Frequency Bias type (fixed or variable) to the ERO each year to allow the ERO to validate the revised Frequency Bias Settings on FRS Form 1. In addition, each Balancing Authority will report its two largest potential resource losses and any applicable N-2 RAS events in the form. If the ERO posts the official list of events after the date specified in the timeline below, Balancing Authorities will be given 30 days from the date the ERO posts the official list of events to submit their FRS Form 1.

Once the ERO reviews the data submitted in FRS Form 1 and FRS Form 2 for all Balancing Authorities, the ERO will use FRS Form 1 data to post the following information for each Balancing Authority for the upcoming year:

- Frequency Bias Setting
- Frequency Response Obligation (FRO)

Once the data listed above is fully posted, the ERO will announce the three-day implementation period for changing the Frequency Bias Setting if it differs from that shown in the timeline below.

A Balancing Authority using a fixed Frequency Bias Setting sets its Frequency Bias Setting to the greater of (in absolute value):

- Any number the Balancing Authority chooses between 100 percent and 125 percent of its Frequency Response Measure as calculated on FRS Form 1
- Interconnection Minimum as determined by the ERO

For purposes of calculating the minimum Frequency Bias Setting, a Balancing Authority participating in a FRSG will need to calculate its stand-alone FRM using FRS Form 1 and FRS Form 2 to determine its minimum Frequency Bias Setting.

A Balancing Authority providing Overlap Regulation will report the historic peak demand and generation of its combined Balancing Authorities' areas on FRS Form 1 as described in Requirement R4.

Frequency Response Measure

The Balancing Authority will calculate its FRM from Single Event Frequency Response Data (SEFRD), defined as: "the data from an individual event in a Balancing Authority area that is used to calculate its Frequency Response, expressed in MW/0.1Hz" as calculated on FRS Form 2 for each event shown on FRS Form 1. The events in FRS Form 1 are selected by the ERO using the *Procedure for ERO Support of Frequency Response and Frequency Bias Setting Standard*. The SEFRD for a typical Balancing Authority in an Interconnection with more than one Balancing Authority is the change in its Net Actual Interchange on its tie lines with adjacent Balancing Authorities divided by the change in Interconnection frequency. Some Balancing Authorities may choose to apply corrections to their Net Actual Interchange (NA_I) values to account for factors such as nonconforming loads. FRS Form 1 and 2 shows the types of adjustments that are allowed. Note that with the exception of the Contingent BA column, any adjustments made must be made for all events in an evaluation year.[1]

The ERO will use a standardized sampling interval of approximately 16 seconds before the event, up to the time of the event for the pre-event NA_I, and frequency (A values), and approximately 20 to 52 seconds after the event for the post-event NA_I (B values) in the computation of SEFRD values, dependent on the data scan rate of the Balancing Authority's Energy Management System (EMS).

All events listed on FRS Form 1 need to be included in the annual submission of FRS Forms 1 and 2. The only time a Balancing Authority should exclude an event is if its tie-line data or its Frequency data is corrupt, or its EMS was unavailable. FRS Form 2 has instructions on how to

[1] As an example, if an entity has non-conforming loads and makes an adjustment for one event, all events must show the non-conforming load, even if the non-conforming load does not impact the calculation. This ensures that the reports are not utilizing the adjustments only when they are favorable to the BA.

correct the BA's data if the given event is internal to the BA or if other authorized adjustments are used.

Assuming data entry is correct, FRS Form 1 will automatically calculate the Balancing Authority's FRM for the past 12 months as the median of the SEFRD values. A Balancing Authority electing to report as an FRSG or a provider of Overlap Regulation Service will provide an FRS Form 1 for the aggregate of its participants.

To allow Balancing Authorities to plan its operations, events with a "Point C" that cause the Interconnection Frequency to be lower than that shown in Table 1 above (for example, an event in the Eastern Interconnection that causes the Interconnection Frequency to go to 59.4 Hz) or higher than an equal change in frequency going above 60 Hz may be included in the list of events for that Interconnection. However, the calculation of the Balancing Authority response to such an event will be adjusted to show a frequency change only to the Target Minimum Frequency shown in Table 1 above (in the previous example this adjustment would cause Frequency to be shown as 59.5 Hz rather than 59.4 HZ) or a high frequency amount of an equal quantity. Should such an event happen, the ERO will provide additional guidance.

Balancing Authorities that elect to form a FRSG as a means to jointly meet the FRO will calculate their FRM performance one of two ways:

- Calculate a group NI_A and measure the group response to all events in the reporting year on a single FRS Form 1, or
- Jointly submit the individual Balancing Authority's Form 1s, with a summary spreadsheet that contains the sum of each participant's individual event performance.

Timeline for Balancing Authority Frequency Response and Frequency Bias Setting Activities

Described below is the timeline for the exchange of information between the ERO and Balancing Authorities to:

- Facilitate the assignment of Balancing Authority FRO
- Calculate Balancing Authority FRM
- Determine Balancing Authority Frequency Bias Settings

Target Business Date	Activity
March 1	**FRS Form 1 is posted by the ERO* with all selected events for the operating year for BA usage.**
April 1	**BAs and FRSGs complete their frequency response forms for all four quarters, including the BAs' FBS calculations, returning the results to the ERO.**
May 1	**The ERO validates FBS values, computes the sum of all FBS values for each Interconnection.**
May 15	**The BAs not required to file FERC Form 714 receive a request to provide load and generation data as described in the *Procedure for ERO Support of Frequency Response and Frequency Bias Setting Standard*** to support FRO assignments and determining minimum FBS for the upcoming year. Data to be provided by July 15.**
June 1	The BA implements any changes to their FBS.
November 1	The ERO assigns FRO values and Minimum FBS for the upcoming year to the BAs.

* If 4th quarter posting of FRS Form 1s is delayed, the ERO may adjust the other timelines in this table by a similar amount.

** Procedure for ERO Support of Frequency Response and Frequency Bias Setting Standard

Appendix BAL-003-2-QC-1
Specific provisions applicable in Québec for standard BAL-003-2 – Frequency Response and Frequency Bias Setting

This appendix establishes specific provisions for the application of the standard in Québec. Provisions of the standard and of this appendix must be read jointly for comprehension and interpretation purposes. Where the standard and appendix differ, the appendix shall prevail.

A. Introduction

1. **Title:** No specific provisions.
2. **Number:** No specific provisions.
3. **Purpose:** No specific provisions.
4. **Applicability:** No specific provisions.
5. **Effective Date:**

5.1. Adoption of the standard by the Régie de l'énergie:	September 30, 2021
5.2. Adoption of the appendix by the Régie de l'énergie:	September 30, 2021
5.3. Effective date of the standard and its appendix in Québec:	December 1st, 2021

B. Requirements and Measures

Specific provision for requirement R2:

In Québec, a Frequency Bias Setting becomes mandatory only after an approval by the Régie. Each Balancing Authority that receives a request to modify a Frequency Bias Setting must submit the request to the Reliability Coordinator who will file it for approval with the Régie.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

In Québec, "Compliance Enforcement Authority" means the Régie de l'énergie in its roles of monitoring and enforcing compliance with respect to the Reliability Standard and to this appendix.

1.2. Evidence retention

No specific provisions.

1.3. Compliance Monitoring and Enforcement Program

The Régie de l'énergie establishes the monitoring processes used to evaluate data or information for the purpose of determining compliance or non-compliance with the Reliability Standard and with this appendix.

Violation Severity Levels (VSL)

No specific provisions.

D. Regional Variances

No specific provisions.

E. Associated Documents

No specific provisions.

Appendix BAL-003-2-QC-1
Specific provisions applicable in Québec for standard BAL-003-2 – Frequency Response and Frequency Bias Setting

Attachment A

No specific provisions.

Version History

Version	Date	Action	Change Tracking
1	September 30, 2021	New appendix as per decision D-2021-126.	New

A. Introduction

1. **Title:** Balancing Authority Control

2. **Number:** BAL-005-1

3. **Purpose:** This standard establishes requirements for acquiring data necessary to calculate Reporting Area Control Error (Reporting ACE). The standard also specifies a minimum periodicity, accuracy, and availability requirement for acquisition of the data and for providing the information to the System Operator.

4. **Applicability:**

   4.1. Functional Entities:

   4.1.1. Balancing Authority

Effective Date: See Implementation Plan for BAL-005-1

B. Requirements and Measures

R1. The Balancing Authority shall use a design scan rate of no more than six seconds in acquiring data necessary to calculate Reporting ACE. *[Violation Risk Factor: Medium] [Time Horizon: Real-time Operations]*

M1. Each Balancing Authority will have dated documentation demonstrating that the data necessary to calculate Reporting ACE was designed to be scanned at a rate of no more than six seconds. Acceptable evidence may include historical data, dated archive files; or data from other databases, spreadsheets, or displays that demonstrate compliance.

R2. A Balancing Authority that is unable to calculate Reporting ACE for more than 30-consecutive minutes shall notify its Reliability Coordinator within 45 minutes of the beginning of the inability to calculate Reporting ACE. *[Violation Risk Factor: Medium] [Time Horizon: Real-time Operations]*

M2. Each Balancing Authority will have dated records to show when it was unable to calculate Reporting ACE for more than 30 consecutive minutes and that it notified its Reliability Coordinator within 45 minutes of the beginning of the inability to calculate Reporting ACE. Such evidence may include, but is not limited to, dated voice recordings, operating logs, or other communication documentation.

R3. Each Balancing Authority shall use frequency metering equipment for the calculation of Reporting ACE: *[Violation Risk Factor: Medium] [Time Horizon: Real-time Operations]*

3.1. that is available a minimum of 99.95% for each calendar year; and,

3.2. with a minimum accuracy of 0.001 Hz.

M3. The Balancing Authority shall have evidence such as dated documents or other evidence in hard copy or electronic format showing the frequency metering equipment used for the calculation of Reporting ACE had a minimum availability of 99.95% for each calendar year and had a minimum accuracy of 0.001 Hz to demonstrate compliance with Requirement R3.

R4. The Balancing Authority shall make available to the operator information associated with Reporting ACE including, but not limited to, quality flags indicating missing or invalid data. *[Violation Risk Factor: Medium] [Time Horizon: Real-time Operations]*

M4. Each Balancing Authority Area shall have evidence such as a graphical display or dated alarm log that provides indication of data validity for the real-time Reporting ACE based on both the calculated result and all of the associated inputs therein.

R5. Each Balancing Authority's system used to calculate Reporting ACE shall be available a minimum of 99.5% of each calendar year. *[Violation Risk Factor: Medium] [Time Horizon: Operations Assessment]*

M5. Each Balancing Authority will have dated documentation demonstrating that the system necessary to calculate Reporting ACE has a minimum availability of 99.5% for each calendar year. Acceptable evidence may include historical data, dated archive files; or data from other databases, spreadsheets, or displays that demonstrate compliance.

R6. Each Balancing Authority that is within a multiple Balancing Authority Interconnection shall implement an Operating Process to identify and mitigate errors affecting the accuracy of scan rate data used in the calculation of Reporting ACE for each Balancing Authority Area. *[Violation Risk Factor: Medium] [Time Horizon: Same-day Operations]*

M6. Each Balancing Authority shall have a current Operating Process meeting the provisions of Requirement R6 and evidence to show that the process was implemented, such as dated communications or incorporation in System Operator task verification.

R7. Each Balancing Authority shall ensure that each Tie-Line, Pseudo-Tie, and Dynamic Schedule with an Adjacent Balancing Authority is equipped with: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

- **7.1.** a common source to provide information to both Balancing Authorities for the scan rate values used in the calculation of Reporting ACE; and,
- **7.2.** a time synchronized common source to determine hourly megawatt-hour values agreed-upon to aid in the identification and mitigation of errors.

M7. The Balancing Authority shall have dated evidence such as voice recordings or transcripts, operator logs, electronic communications, or other equivalent evidence that will be used to demonstrate a common source for the components used in the calculation of Reporting ACE with its Adjacent Balancing Authority.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention

The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

- The applicable entity shall keep data or evidence to show compliance for the current year, plus three previous calendar years.

1.3. Compliance Monitoring and Assessment Processes:

As defined in the NERC Rules of Procedure, "Compliance Monitoring and Assessment Processes" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

1.4. Additional Compliance Information

None

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	Real-time Operations	Medium	N/A	N/A	N/A	Balancing Authority was using a design scan rate of greater than six seconds to acquire the data necessary to calculate Reporting ACE.
R2.	Real-time Operations	Medium	The Balancing Authority failed to notify its Reliability Coordinator within 45 minutes of the beginning of the inability to calculate Reporting ACE but notified its Reliability Coordinator in less than or equal to 50 minutes from the beginning of the	The Balancing Authority failed to notify its Reliability Coordinator within 50 minutes of the beginning of an inability to calculate Reporting ACE but notified its Reliability Coordinator in less than or equal to 55 minutes from the beginning of an	The Balancing Authority failed to notify its Reliability Coordinator within 55 minutes of the beginning of an inability to calculate Reporting ACE but notified its Reliability Coordinator in less than or equal to 60 minutes from the beginning of an	The Balancing Authority failed to notify its Reliability Coordinator within 60 minutes of the beginning of an inability to calculate Reporting ACE.

			inability to calculate Reporting ACE.	inability to calculate Reporting ACE.	inability to calculate Reporting ACE.	
R3.	Real-time Operations	Medium	The Balancing Authority's frequency metering equipment used for the calculation of Reporting ACE was available less than 99.95% of the calendar year but was available greater than or equal to 99.94 % of the calendar year.	The Balancing Authority's frequency metering equipment used for the calculation of Reporting ACE was available less than 99.94% of the calendar year but was available greater than or equal to 99.93 % of the calendar year.	The Balancing Authority's frequency metering equipment used for the calculation of Reporting ACE was available less than 99.93% of the calendar year but was available greater than or equal to 99.92 % of the calendar year.	The Balancing Authority's frequency metering equipment used for the calculation of Reporting ACE was available less than 99.92% of the calendar year Or The Balancing Authority's frequency metering equipment used for the calculation of Reporting ACE failed to have a minimum accuracy of 0.001 Hz.
R4.	Real-time Operations	Medium	N/A	N/A	N/A	The Balancing Authority failed to make available information indicating missing or invalid data associated with

						Reporting ACE to its operators.
R5.	Operations Assessment	Medium	The Balancing Authority's system used for the calculation of Reporting ACE was available less than 99.5% of the calendar year but was available greater than or equal to 99.4 % of the calendar year.	The Balancing Authority's system used for the calculation of Reporting ACE was available less than 99.4% of the calendar year but was available greater than or equal to 99.3 % of the calendar year.	The Balancing Authority's system used for the calculation of Reporting ACE was available less than 99.3% of the calendar year but was available greater than or equal to 99.2 % of the calendar year.	The Balancing Authority's system used for the calculation of Reporting ACE was available less than 99.2% of the calendar year.
R6.	Same-day Operations	Medium	N/A	N/A	N/A	The Balancing Authority failed to implement an Operating Process to identify and mitigate errors affecting the scan-rate accuracy of data used in the calculation of Reporting ACE.
R7.	Operations Planning	Medium	N/A	N/A	N/A	The Balancing Authority failed to use a common source for Tie-Lines, Pseudo-ties and Dynamic

						Schedules with its Adjacent Balancing Authorities **Or** **The Balancing Authority failed to use a time synchronized common source for hourly megawatt hour values that are agreed-upon to aid in the identification and mitigation of errors.**

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
0	February 8, 2005	Adopted by NERC Board of Trustees	New
0	April 1, 2005	Effective Date	New
0	August 8, 2005	Removed "Proposed" from Effective Date	Errata
0a	December 19, 2007	Added Appendix 1 – Interpretation of R17 approved by BOT on May 2, 2007	Addition
0a	January 16, 2008	Section F: added "1."; changed hyphen to "en dash." Changed font style for "Appendix 1" to Arial	Errata
0b	February 12, 2008	Replaced Appendix 1 – Interpretation of R17 approved by BOT on February 12, 2008 (BOT approved retirement of Interpretation included in BAL-005-0a)	Replacement
0.1b	October 29, 2008	BOT approved errata changes; updated version number to "0.1b"	Errata
0.1b	May 13, 2009	FERC approved – Updated Effective Date	Addition
0.2b	March 8, 2012	Errata adopted by Standards Committee; (replaced Appendix 1 with the FERC-approved revised interpretation of R17 and corrected standard version referenced in Interpretation by changing from "BAL-005-1" to "BAL-005-0)	Errata
0.2b	September 13, 2012	FERC approved – Updated Effective Date	Addition

0.2b	February 7, 2013	R2 and associated elements approved by NERC Board of Trustees for retirement as part of the Paragraph 81 project (Project 2013-02) pending applicable regulatory approval.	
0.2b	November 21, 2013	R2 and associated elements approved by FERC for retirement as part of the Paragraph 81 project (Project 2013-02) effective January 21, 2014.	
1	February 11, 2016	Adopted by NERC Board of Trustees	Complete re-write of standard
1	September 20. 2017	FERC Order No. 836 approved BAL-005-1.	

Rationale

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon Board approval, the text from the rationale boxes will be moved to this section.

Rationale for Requirement R1: Real-time operation of a Balancing Authority requires real-time information. A sufficient scan rate is key to an Operator's trust in real-time information. Without a sufficient scan rate, an operator may question the accuracy of data during events, which would degrade the operator's ability to maintain reliability.

Rationale for Requirement R2: The RC is responsible for coordinating the reliability of bulk electric systems for member BA's. When a BA is unable to calculate its ACE for an extended period of time, this information must be communicated to the RC within 15 minutes thereafter so that the RC has sufficient knowledge of system conditions to assess any unintended reliability consequences that may occur on the wide area.

Rationale for Requirement R3: Frequency is the basic measurement for interconnection health, and a critical component for calculating Reporting ACE. Without sufficient available frequency data the BA operator will lack situational awareness and will be unable to make correct decisions when maintaining reliability.

Rationale for Requirement R4: System operators utilize Reporting ACE as a primary metric to determine operating actions or instructions. When data inputs into the ACE calculation are incorrect, the operator should be made aware through visual display. When an operator questions the validity of data, actions are delayed and the probability of adverse events occurring can increase.

Rationale for Requirement R5: Reporting ACE is an essential measurement of the BA's contribution to the reliability of the Interconnection. Since Reporting ACE is a measure of the BA's reliability performance for BAL-001, and BAL-002, it is critical that Reporting ACE be sufficiently available to assure reliability.

Rationale for Requirement R6: Reporting ACE is a measure of the BA's reliability performance for BAL-001, and BAL-002. Without a process to address persistent errors in the ACE calculation, the operator can lose trust in the validity of Reporting ACE resulting in delayed or incorrect decisions regarding the reliability of the bulk electric system.

Rationale for Requirement R7: Reporting ACE is an essential measurement of the BA's contribution to the reliability of the Interconnection. Common source data is critical to calculating Reporting ACE that is consistent between Balancing Authorities. When data sources are not common, confusion can be created between BAs resulting in delayed or incorrect operator action.

The intent of Requirement R7 Part 7.1 is to provide accuracy in the measurement and calculations used in Reporting ACE. It specifies the need for common metering points for instantaneous values for the tie-line megawatt flow values between Balancing Authority Areas. Common data source requirements also apply to instantaneous values for pseudo-ties and dynamic schedules, and can extend to more than two Balancing Authorities that participate in allocating shares of a generation resource in supplementary regulation, for example.

The intent of Requirement R7 Part 7.2 is to enable accuracy in the measurements and calculations used in Reporting ACE. It specifies the need for common metering points for hourly accumulated values for the time synchronized tie line MWh values agreed-upon between Balancing Authority Areas. These time synchronized agreed-upon values are necessary for use in the Operating Process required in R6 to identify and mitigate errors in the scan-rate values used in Reporting ACE.

Appendix QC-BAL-005-1
Provisions specific to the standard BAL-005-1 applicable in Québec

This appendix establishes specific provisions for the application of the standard in Québec. Provisions of the standard and of its appendix must be read together for the purposes of understanding and interpretation. Where the standard and appendix differ, the appendix shall prevail.

A. Introduction

1. Title: **Balancing Authority Control**

2. Number: BAL-005-1

3. Purpose: No specific provision

4. Applicability: No specific provision

5. Effective Date:

5.1. Adoption of the standard by the Régie de l'énergie: June 8, 2020

5.2. Adoption of the appendix by the Régie de l'énergie: June 8, 2020

5.3. Effective date of the standard and its appendix in Québec: July 1, 2021

B. Requirements and Measures

No specific provision

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

The Régie de l'énergie is responsible, in Québec, for compliance monitoring with respect to the reliability standard and its appendix that it adopts.

1.2. Evidence Retention

No specific provision

1.3. Compliance Monitoring and Assessment Processes

The Québec Reliability Standards Compliance Monitoring and Enforcement Program (QCMEP) of the Régie de l'énergie identifies the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

1.4. Additional Compliance Information

No specific provision

Table of Compliance Elements

No specific provision

D. Regional Variances

No specific provision

Appendix QC-BAL-005-1
Provisions specific to the standard BAL-005-1 applicable in Québec

E. Interpretations

No specific provision

F. Associated Documents

No specific provision

Version History

Version	Date	Action	Change Tracking
0	June 8, 2020	New appendix	New

A. Introduction

1. Title: Cyber Security — BES Cyber System Categorization

2. Number: CIP-002-5.1a

3. Purpose: To identify and categorize BES Cyber Systems and their associated BES Cyber Assets for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES. Identification and categorization of BES Cyber Systems support appropriate protection against compromises that could lead to misoperation or instability in the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1. Balancing Authority

4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1. Each underfrequency load shedding (UFLS) or undervoltage load shedding (UVLS) system that:

4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2. Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Interchange Coordinator or Interchange Authority

4.1.6. Reliability Coordinator

4.1.7. Transmission Operator

4.1.8. Transmission Owner

4.2. **Facilities:** For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-002-5.1a:

4.2.3.1. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

5. Effective Dates:

1. **24 Months Minimum** – CIP-002-5.1a shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval.
2. In those jurisdictions where no regulatory approval is required CIP-002-5.1a shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

6. Background:

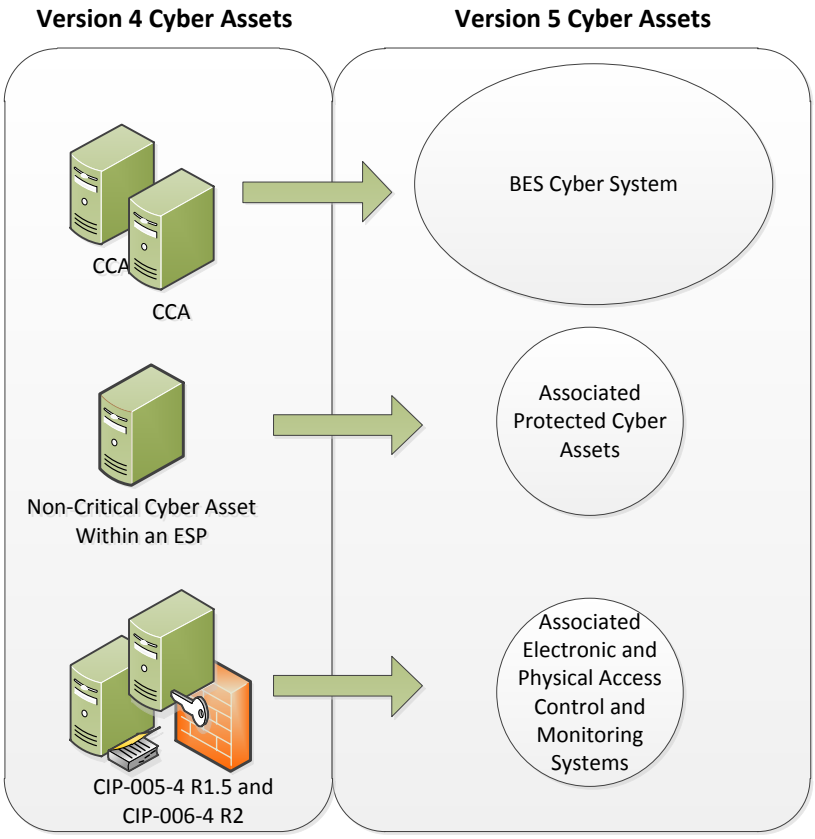
This standard provides "bright-line" criteria for applicable Responsible Entities to categorize their BES Cyber Systems based on the impact of their associated Facilities, systems, and equipment, which, if destroyed, degraded, misused, or otherwise rendered unavailable, would affect the reliable operation of the Bulk Electric System. Several concepts provide the basis for the approach to the standard.

Throughout the standards, unless otherwise stated, bulleted items in the requirements are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section and the criteria in Attachment 1 of CIP-002 use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

BES Cyber Systems

One of the fundamental differences between Versions 4 and 5 of the CIP Cyber Security Standards is the shift from identifying Critical Cyber Assets to identifying BES Cyber Systems. This change results from the drafting team's review of the NIST Risk Management Framework and the use of an analogous term "information system" as the target for categorizing and applying security controls.



In transitioning from Version 4 to Version 5, a BES Cyber System can be viewed simply as a grouping of Critical Cyber Assets (as that term is used in Version 4). The CIP Cyber Security Standards use the "BES Cyber System" term primarily to provide a higher level for referencing the object of a requirement. For example, it becomes possible to apply requirements dealing with recovery and malware protection to a grouping rather than individual Cyber Assets, and it becomes clearer in the requirement that malware protection applies to the system as a whole and may not be necessary for every individual device to comply.

Another reason for using the term "BES Cyber System" is to provide a convenient level at which a Responsible Entity can organize their documented implementation of the requirements and compliance evidence. Responsible Entities can use the well-developed concept of a *security plan* for each BES Cyber System to document the programs, processes, and plans in place to comply with security requirements.

It is left up to the Responsible Entity to determine the level of granularity at which to identify a BES Cyber System within the qualifications in the definition of BES Cyber System. For example, the Responsible Entity might choose to view an entire plant control system as a single BES Cyber System, or it might choose to view certain components of the plant control system as distinct BES Cyber Systems. The Responsible Entity should take into consideration the operational environment and

scope of management when defining the BES Cyber System boundary in order to maximize efficiency in secure operations. Defining the boundary too tightly may result in redundant paperwork and authorizations, while defining the boundary too broadly could make the secure operation of the BES Cyber System difficult to monitor and assess.

Reliable Operation of the BES

The scope of the CIP Cyber Security Standards is restricted to BES Cyber Systems that would impact the reliable operation of the BES. In order to identify BES Cyber Systems, Responsible Entities determine whether the BES Cyber Systems perform or support any BES reliability function according to those reliability tasks identified for their reliability function and the corresponding functional entity's responsibilities as defined in its relationships with other functional entities in the NERC Functional Model. This ensures that the *initial* scope for consideration includes only those BES Cyber Systems and their associated BES Cyber Assets that perform or support the reliable operation of the BES. The definition of BES Cyber Asset provides the basis for this scoping.

Real-time Operations

One characteristic of the BES Cyber Asset is a real-time scoping characteristic. The time horizon that is significant for BES Cyber Systems and BES Cyber Assets subject to the application of these Version 5 CIP Cyber Security Standards is defined as that which is material to real-time operations for the reliable operation of the BES. To provide a better defined time horizon than "Real-time," BES Cyber Assets are those Cyber Assets that, if rendered unavailable, degraded, or misused, would adversely impact the reliable operation of the BES within 15 minutes of the activation or exercise of the compromise. This time window must not include in its consideration the activation of redundant BES Cyber Assets or BES Cyber Systems: from the cyber security standpoint, redundancy does not mitigate cyber security vulnerabilities.

Categorization Criteria

The criteria defined in Attachment 1 are used to categorize BES Cyber Systems into impact categories. Requirement 1 only requires the discrete identification of BES Cyber Systems for those in the high impact and medium impact categories. All BES Cyber Systems for Facilities not included in Attachment 1 – Impact Rating Criteria, Criteria 1.1 to 1.4 and Criteria 2.1 to 2.11 default to be low impact.

This general process of categorization of BES Cyber Systems based on impact on the reliable operation of the BES is consistent with risk management approaches for the purpose of application of cyber security requirements in the remainder of the Version 5 CIP Cyber Security Standards.

Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets that are associated with BES Cyber Systems

BES Cyber Systems have associated Cyber Assets, which, if compromised, pose a threat to the BES Cyber System by virtue of: (a) their location within the Electronic Security Perimeter (Protected Cyber Assets), or (b) the security control function they perform (Electronic Access Control or Monitoring Systems and Physical Access Control Systems). These Cyber Assets include:

Electronic Access Control or Monitoring Systems ("EACMS") – Examples include: Electronic Access Points, Intermediate Systems, authentication servers (e.g., RADIUS servers, Active Directory servers, Certificate Authorities), security event monitoring systems, and intrusion detection systems.

Physical Access Control Systems ("PACS")– Examples include: authentication servers, card systems, and badge control systems.

Protected Cyber Assets ("PCA") – Examples may include, to the extent they are within the ESP: file servers, ftp servers, time servers, LAN switches, networked printers, digital fault recorders, and emission monitoring systems.

B. Requirements and Measures

R1. Each Responsible Entity shall implement a process that considers each of the following assets for purposes of parts 1.1 through 1.3: *[Violation Risk Factor: High][Time Horizon: Operations Planning]*

i. Control Centers and backup Control Centers;
ii. Transmission stations and substations;
iii. Generation resources;
iv. Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements;
v. Special Protection Systems that support the reliable operation of the Bulk Electric System; and
vi. For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above.

1.1. Identify each of the high impact BES Cyber Systems according to Attachment 1, Section 1, if any, at each asset;

1.2. Identify each of the medium impact BES Cyber Systems according to Attachment 1, Section 2, if any, at each asset; and

1.3. Identify each asset that contains a low impact BES Cyber System according to Attachment 1, Section 3, if any (a discrete list of low impact BES Cyber Systems is not required).

M1. Acceptable evidence includes, but is not limited to, dated electronic or physical lists required by Requirement R1, and Parts 1.1 and 1.2.

R2. The Responsible Entity shall: *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

2.1 Review the identifications in Requirement R1 and its parts (and update them if there are changes identified) at least once every 15 calendar months, even if it has no identified items in Requirement R1, and

2.2 Have its CIP Senior Manager or delegate approve the identifications required by Requirement R1 at least once every 15 calendar months, even if it has no identified items in Requirement R1.

M2. Acceptable evidence includes, but is not limited to, electronic or physical dated records to demonstrate that the Responsible Entity has reviewed and updated, where necessary, the identifications required in Requirement R1 and its parts, and has had its CIP Senior Manager or delegate approve the identifications required in Requirement R1 and its parts at least once every 15 calendar months, even if it has none identified in Requirement R1 and its parts, as required by Requirement R2.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.

- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information

- None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-002-5.1a)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**High**	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, five percent or fewer BES assets have not been considered according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, 2 or fewer BES assets in Requirement R1, have not been considered according to Requirement R1; OR For Responsible Entities with more than a total of 100 high and medium impact BES Cyber	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, more than five percent but less than or equal to 10 percent of BES assets have not been considered, according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, more than two, but fewer than or equal to four BES assets in Requirement R1, have not been considered according to Requirement R1; OR	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, more than 10 percent but less than or equal to 15 percent of BES assets have not been considered, according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, more than four, but fewer than or equal to six BES assets in Requirement R1, have not been considered according to Requirement R1; OR	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, more than 15 percent of BES assets have not been considered, according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, more than six BES assets in Requirement R1, have not been considered according to Requirement R1; OR For Responsible Entities with more than a total of 100 high and medium impact BES Cyber

R #	Time Horizon	VRF	Violation Severity Levels (CIP-002-5.1a)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Systems, five percent or fewer of identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, five or fewer identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact BES Cyber	For Responsible Entities with more than a total of 100 high and medium impact BES Cyber Systems, more than five percent but less than or equal to 10 percent of identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high and medium impact and BES Cyber Systems, more than five but less than or equal to 10 identified BES Cyber Systems have not been categorized or have been incorrectly	For Responsible Entities with more than a total of 100 high or medium impact BES Cyber Systems, more than 10 percent but less than or equal to 15 percent of identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high or medium impact and BES Cyber Assets, more than 10 but less than or equal to 15 identified BES Cyber Assets have not been categorized or have been incorrectly	Systems, more than 15 percent of identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, more than 15 identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact BES Cyber

R #	Time Horizon	VRF	Violation Severity Levels (CIP-002-5.1a)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Systems, five percent or fewer high or medium BES Cyber Systems have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, five or fewer high or medium BES Cyber Systems have not been identified.	categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact BES Cyber Systems, more than five percent but less than or equal to 10 percent high or medium BES Cyber Systems have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, more than five but less than or equal to 10 high or medium BES Cyber Systems have not been identified.	categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact BES Cyber Systems, more than 10 percent but less than or equal to 15 percent high or medium BES Cyber Systems have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, more than 10 but less than or equal to 15 high or medium BES Cyber Systems have not been identified.	Systems, more than 15 percent of high or medium impact BES Cyber Systems have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, more than 15 high or medium impact BES Cyber Systems have not been identified.

R #	Time Horizon	VRF	Violation Severity Levels (CIP-002-5.1a)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R2	**Operations Planning**	**Lower**	The Responsible Entity did not complete its review and update for the identification required for R1 within 15 calendar months but less than or equal to 16 calendar months of the previous review. (R2.1) OR The Responsible Entity did not complete its approval of the identifications required by R1 by the CIP Senior Manager or delegate according to Requirement R2 within 15 calendar months but less than or equal to 16 calendar months of the previous approval. (R2.2)	The Responsible Entity did not complete its review and update for the identification required for R1 within 16 calendar months but less than or equal to 17 calendar months of the previous review. (R2.1) OR The Responsible Entity failed to complete its approval of the identifications required by R1 by the CIP Senior Manager or delegate according to Requirement R2 within 16 calendar months but less than or equal to 17 calendar months of the previous approval. (R2.2)	The Responsible Entity did not complete its review and update for the identification required for R1 within 17 calendar months but less than or equal to 18 calendar months of the previous review. (R2.1) OR The Responsible Entity failed to complete its approval of the identifications required by R1 by the CIP Senior Manager or delegate according to Requirement R2 within 17 calendar months but less than or equal to 18 calendar months of the previous approval. (R2.2)	The Responsible Entity did not complete its review and update for the identification required for R1 within 18 calendar months of the previous review. (R2.1) OR The Responsible Entity failed to complete its approval of the identifications required by R1 by the CIP Senior Manager or delegate according to Requirement R2 within 18 calendar months of the previous approval. (R2.2)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

CIP-002-5.1a - Attachment 1

Impact Rating Criteria

The criteria defined in Attachment 1 do not constitute stand-alone compliance requirements, but are criteria characterizing the level of impact and are referenced by requirements.

1. High Impact Rating (H)

Each BES Cyber System used by and located at any of the following:

1.1. Each Control Center or backup Control Center used to perform the functional obligations of the Reliability Coordinator.

1.2. Each Control Center or backup Control Center used to perform the functional obligations of the Balancing Authority: 1) for generation equal to or greater than an aggregate of 3000 MW in a single Interconnection, or 2) for one or more of the assets that meet criterion 2.3, 2.6, or 2.9.

1.3. Each Control Center or backup Control Center used to perform the functional obligations of the Transmission Operator for one or more of the assets that meet criterion 2.2, 2.4, 2.5, 2.7, 2.8, 2.9, or 2.10.

1.4 Each Control Center or backup Control Center used to perform the functional obligations of the Generator Operator for one or more of the assets that meet criterion 2.1, 2.3, 2.6, or 2.9.

2. Medium Impact Rating (M)

Each BES Cyber System, not included in Section 1 above, associated with any of the following:

2.1. Commissioned generation, by each group of generating units at a single plant location, with an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection. For each group of generating units, the only BES Cyber Systems that meet this criterion are those shared BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection.

2.2. Each BES reactive resource or group of resources at a single location (excluding generation Facilities) with an aggregate maximum Reactive Power nameplate rating of 1000 MVAR or greater (excluding those at generation Facilities). The only BES Cyber Systems that meet this criterion are those shared BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of resources that in aggregate equal or exceed 1000 MVAR.

2.3. Each generation Facility that its Planning Coordinator or Transmission Planner designates, and informs the Generator Owner or Generator Operator, as necessary to avoid an Adverse Reliability Impact in the planning horizon of more than one year.

2.4. Transmission Facilities operated at 500 kV or higher. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.

2.5. Transmission Facilities that are operating between 200 kV and 499 kV at a single station or substation, where the station or substation is connected at 200 kV or higher voltages to three or more other Transmission stations or substations and has an "aggregate weighted value" exceeding 3000 according to the table below. The "aggregate weighted value" for a single station or substation is determined by summing the "weight value per line" shown in the table below for each incoming and each outgoing BES Transmission Line that is connected to another Transmission station or substation. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.

Voltage Value of a Line	Weight Value per Line
less than 200 kV (not applicable)	(not applicable)
200 kV to 299 kV	700
300 kV to 499 kV	1300
500 kV and above	0

2.6. Generation at a single plant location or Transmission Facilities at a single station or substation location that are identified by its Reliability Coordinator, Planning Coordinator, or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.

2.7. Transmission Facilities identified as essential to meeting Nuclear Plant Interface Requirements.

2.8. Transmission Facilities, including generation interconnection Facilities, providing the generation interconnection required to connect generator output to the Transmission Systems that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of the generation Facilities identified by any Generator Owner as a result of its application of Attachment 1, criterion 2.1 or 2.3.

2.9. Each Special Protection System (SPS), Remedial Action Scheme (RAS), or automated switching System that operates BES Elements, that, if destroyed, degraded, misused or otherwise rendered unavailable, would cause one or more Interconnection Reliability Operating Limits (IROLs) violations for failure to operate as designed or cause a reduction in one or more IROLs if destroyed, degraded, misused, or otherwise rendered unavailable.

2.10. Each system or group of Elements that performs automatic Load shedding under a common control system, without human operator initiation, of 300 MW or more implementing undervoltage load shedding (UVLS) or underfrequency load shedding (UFLS) under a load shedding program that is subject to one or more requirements in a NERC or regional reliability standard.

2.11. Each Control Center or backup Control Center, not already included in High Impact Rating (H) above, used to perform the functional obligations of the Generator Operator for an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection.

2.12. Each Control Center or backup Control Center used to perform the functional obligations of the Transmission Operator not included in High Impact Rating (H), above.

2.13. Each Control Center or backup Control Center, not already included in High Impact Rating (H) above, used to perform the functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MW in a single Interconnection.

3. Low Impact Rating (L)

BES Cyber Systems not included in Sections 1 or 2 above that are associated with any of the following assets and that meet the applicability qualifications in Section 4 - Applicability, part 4.2 – Facilities, of this standard:

3.1. Control Centers and backup Control Centers.

3.2. Transmission stations and substations.

3.3. Generation resources.

3.4. Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements.

3.5. Special Protection Systems that support the reliable operation of the Bulk Electric System.

3.6. For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in section 4.1, that is subject to the requirements of the standard. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the qualified set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards. This section is especially significant in CIP-002-5.1a and represents the total scope of Facilities, systems, and equipment to which the criteria in Attachment 1 apply. This is important because it determines the balance of these Facilities, systems, and equipment that are Low Impact once those that qualify under the High and Medium Impact categories are filtered out.

For the purpose of identifying groups of Facilities, systems, and equipment, whether by location or otherwise, the Responsible Entity identifies assets as described in Requirement R1 of CIP-002-5.1a. This is a process familiar to Responsible Entities that have to comply with versions 1, 2, 3, and 4 of the CIP standards for Critical Assets. As in versions 1, 2, 3, and 4, Responsible Entities may use substations, generation plants, and Control Centers at single site locations as identifiers of these groups of Facilities, systems, and equipment.

CIP-002-5.1a

CIP-002-5.1a requires that applicable Responsible Entities categorize their BES Cyber Systems and associated BES Cyber Assets according to the criteria in Attachment 1. A BES Cyber Asset includes in its definition, "…that if rendered unavailable, degraded, or misused would, within 15 minutes adversely impact the reliable operation of the BES."

The following provides guidance that a Responsible Entity may use to identify the BES Cyber Systems that would be in scope. The concept of BES reliability operating service is useful in providing Responsible Entities with the option of a defined process for scoping those BES Cyber

Systems that would be subject to CIP-002-5.1a. The concept includes a number of named BES reliability operating services. These named services include:

Dynamic Response to BES conditions
Balancing Load and Generation
Controlling Frequency (Real Power)
Controlling Voltage (Reactive Power)
Managing Constraints
Monitoring & Control
Restoration of BES
Situational Awareness
Inter-Entity Real-Time Coordination and Communication

Responsibility for the reliable operation of the BES is spread across all Entity Registrations. Each entity registration has its own special contribution to reliable operations and the following discussion helps identify which entity registration, in the context of those functional entities to which these CIP standards apply, performs which reliability operating service, as a process to identify BES Cyber Systems that would be in scope. The following provides guidance for Responsible Entities to determine applicable reliability operations services according to their Function Registration type.

Entity Registration	RC	BA	TOP	TO	DP	GOP	GO
Dynamic Response		X	X	X	X	X	X
Balancing Load & Generation	X	X	X	X	X	X	X
Controlling Frequency		X				X	X
Controlling Voltage			X	X	X		X
Managing Constraints	X		X			X	
Monitoring and Control			X			X	
Restoration			X			X	
Situation Awareness	X	X	X			X	
Inter-Entity coordination	X	X	X	X		X	X

Dynamic Response

The Dynamic Response Operating Service includes those actions performed by BES Elements or subsystems which are automatically triggered to initiate a response to a BES condition. These actions are triggered by a single element or control device or a combination of these elements or devices in concert to perform an action or cause a condition in reaction to the triggering action or condition. The types of dynamic responses that may be considered as potentially having an impact on the BES are:

- Spinning reserves (contingency reserves)
  - Providing actual reserve generation when called upon (GO,GOP)
  - Monitoring that reserves are sufficient (BA)
- Governor Response
  - Control system used to actuate governor response (GO)
- Protection Systems (transmission & generation)
  - Lines, buses, transformers, generators (DP, TO, TOP, GO, GOP)
  - Zone protection for breaker failure (DP, TO, TOP)
  - Breaker protection (DP, TO, TOP)
  - Current, frequency, speed, phase (TO,TOP, GO,GOP)
- Special Protection Systems or Remedial Action Schemes
  - Sensors, relays, and breakers, possibly software (DP, TO, TOP)
- Under and Over Frequency relay protection (includes automatic load shedding)
  - Sensors, relays & breakers (DP)
- Under and Over Voltage relay protection (includes automatic load shedding)
  - Sensors, relays & breakers (DP)
- Power System Stabilizers (GO)

Balancing Load and Generation

The Balancing Load and Generation Operations Service includes activities, actions and conditions necessary for monitoring and controlling generation and load in the operations planning horizon and in real-time. Aspects of the Balancing Load and Generation function include, but are not limited to:

- Calculation of Area Control Error (ACE)
  - Field data sources (real time tie flows, frequency sources, time error, etc) (TO, TOP)
  - Software used to perform calculation (BA)
- Demand Response
  - Ability to identify load change need (BA)
  - Ability to implement load changes (TOP,DP)
- Manually Initiated Load shedding
  - Ability to identify load change need (BA)
  - Ability to implement load changes (TOP, DP)

- Non-spinning reserve (contingency reserve)
  - Know generation status, capability, ramp rate, start time (GO, BA)
  - Start units and provide energy (GOP)

Controlling Frequency (Real Power)

The Controlling Frequency Operations Service includes activities, actions and conditions which ensure, in real time, that frequency remains within bounds acceptable for the reliability or operability of the BES. Aspects of the Controlling Frequency function include, but are limited to:

- Generation Control (such as AGC)
  - ACE, current generator output, ramp rate, unit characteristics (BA, GOP, GO)
  - Software to calculate unit adjustments (BA)
  - Transmit adjustments to individual units (GOP)
  - Unit controls implementing adjustments (GOP)
- Regulation (regulating reserves)
  - Frequency source, schedule (BA)
  - Governor control system (GO)

Controlling Voltage (Reactive Power)

The Controlling Voltage Operations Service includes activities, actions and conditions which ensure, in real time, that voltage remains within bounds acceptable for the reliability or operability of the BES. Aspects of the Controlling Voltage function include, but are not limited to:

- Automatic Voltage Regulation (AVR)
  - Sensors, stator control system, feedback (GO)
- Capacitive resources
  - Status, control (manual or auto), feedback (TOP, TO,DP)
- Inductive resources (transformer tap changer, or inductors)
  - Status, control (manual or auto), feedback (TOP,TO,DP)
- Static VAR Compensators (SVC)
  - Status, computations, control (manual or auto), feedback (TOP, TO,DP)

Managing Constraints

Managing Constraints includes activities, actions and conditions that are necessary to ensure that elements of the BES operate within design limits and constraints established for the reliability and operability of the BES. Aspects of the Managing Constraints include, but are not limited to:

- Available Transfer Capability (ATC) (TOP)
- Interchange schedules (TOP, RC)
- Generation re-dispatch and unit commit (GOP)
- Identify and monitor SOL's & IROL's (TOP, RC)
- Identify and monitor Flow gates (TOP, RC)

Monitoring and Control

Monitoring and Control includes those activities, actions and conditions that provide monitoring and control of BES Elements. An example aspect of the Control and Operation function is:

- All methods of operating breakers and switches
  - SCADA (TOP, GOP)
  - Substation automation (TOP)

Restoration of BES

The Restoration of BES Operations Service includes activities, actions and conditions necessary to go from a shutdown condition to an operating condition delivering electric power without external assistance. Aspects of the Restoration of BES function include, but are not limited to:

- Restoration including planned cranking path
  - Through black start units (TOP, GOP)
  - Through tie lines (TOP, GOP)
- Off-site power for nuclear facilities. (TOP, TO, BA, RC, DP, GO, GOP)
- Coordination (TOP, TO, BA, RC, DP, GO, GOP)

Situational Awareness

The Situational Awareness function includes activities, actions and conditions established by policy, directive or standard operating procedure necessary to assess the current condition of the BES and anticipate effects of planned and unplanned changes to conditions. Aspects of the Situation Awareness function include:

- Monitoring and alerting (such as EMS alarms) (TOP, GOP, RC,BA)
- Change management (TOP,GOP,RC,BA)
- Current Day and Next Day planning (TOP)
- Contingency Analysis (RC)
- Frequency monitoring (BA, RC)

Inter-Entity Coordination

The Inter-Entity coordination and communication function includes activities, actions, and conditions established by policy, directive, or standard operating procedure necessary for the coordination and communication between Responsible Entities to ensure the reliability and operability of the BES. Aspects of the Inter-Entity Coordination and Communication function include:

- Scheduled interchange (BA,TOP,GOP,RC)
- Facility operational data and status (TO, TOP, GO, GOP, RC, BA)
- Operational directives (TOP, RC, BA)

Applicability to Distribution Providers

It is expected that only Distribution Providers that own or operate facilities that qualify in the Applicability section will be subject to these Version 5 Cyber Security Standards. Distribution Providers that do not own or operate any facility that qualifies are not subject to these standards. The qualifications are based on the requirements for registration as a Distribution Provider and on the requirements applicable to Distribution Providers in NERC Standard EOP-005.

Requirement R1:

Requirement R1 implements the methodology for the categorization of BES Cyber Systems according to their impact on the BES. Using the traditional risk assessment equation, it reduces the measure of the risk to an impact (consequence) assessment, assuming the vulnerability index of 1 (the Systems are assumed to be vulnerable) and a probability of threat of 1 (100 percent). The criteria in Attachment 1 provide a measure of the impact of the BES assets supported by these BES Cyber Systems.

Responsible Entities are required to identify and categorize those BES Cyber Systems that have high and medium impact. BES Cyber Systems for BES assets not specified in Attachment 1, Criteria 1.1 – 1.4 and Criteria 2.1 – 2.11 default to low impact.

Attachment 1

Overall Application

In the application of the criteria in Attachment 1, Responsible Entities should note that the approach used is based on the impact of the BES Cyber System as measured by the bright-line criteria defined in Attachment 1.

- When the drafting team uses the term "Facilities", there is some latitude to Responsible Entities to determine included Facilities. The term Facility is defined in the NERC Glossary of Terms as "A set of electrical equipment that operates as a single Bulk Electric System Element (e.g., a line, a generator, a shunt compensator, transformer, etc.)." In most cases, the criteria refer to a group of Facilities in a given location that supports the reliable operation of the BES. For example, for Transmission assets, the substation may be designated as the group of Facilities. However, in a substation that includes equipment that supports BES operations along with equipment that only supports Distribution operations, the Responsible Entity may be better served to consider only the group of Facilities that supports BES operation. In that case, the Responsible Entity may designate the group of Facilities by location, with qualifications on the group of Facilities that supports reliable operation of the BES, as the Facilities that are subject to the criteria for categorization of BES Cyber Systems. Generation Facilities are separately discussed in the Generation section below. In CIP-002-5.1a, these groups of Facilities, systems, and equipment are sometimes designated as BES assets. For example, an identified BES asset may be a named substation, generating plant, or Control Center. Responsible Entities have flexibility in how they group Facilities, systems, and equipment at a location.
- In certain cases, a BES Cyber System may be categorized by meeting multiple criteria. In such cases, the Responsible Entity may choose to document all criteria that result in the categorization. This will avoid inadvertent miscategorization when it no longer meets one of the criteria, but still meets another.
- It is recommended that each BES Cyber System should be listed by only one Responsible Entity. Where there is joint ownership, it is advisable that the owning Responsible Entities should formally agree on the designated Responsible Entity responsible for compliance with the standards.

High Impact Rating (H)

This category includes those BES Cyber Systems, used by and at Control Centers (and the associated data centers included in the definition of Control Centers), that perform the functional obligations of the Reliability Coordinator (RC), Balancing Authority (BA), Transmission Operator (TOP), or Generator Operator (GOP), as defined under the Tasks heading of the applicable Function and the Relationship with Other Entities heading of the functional entity in the NERC Functional Model, and as scoped by the qualification in Attachment 1, Criteria 1.1, 1.2, 1.3 and 1.4. While those entities that have been registered as the above-named functional entities are specifically referenced, it must be noted that there may be agreements where some

of the functional obligations of a Transmission Operator may be delegated to a Transmission Owner (TO). In these cases, BES Cyber Systems at these TO Control Centers that perform these functional obligations would be subject to categorization as high impact. The criteria notably specifically emphasize functional obligations, not necessarily the RC, BA, TOP, or GOP facilities. One must note that the definition of Control Center specifically refers to reliability tasks for RCs, Bas, TOPs, and GOPs. A TO BES Cyber System in a TO facility that does not perform or does not have an agreement with a TOP to perform any of these functional tasks does not meet the definition of a Control Center. However, if that BES Cyber System operates any of the facilities that meet criteria in the Medium Impact category, that BES Cyber System would be categorized as a Medium Impact BES Cyber System.

The 3000 MW threshold defined in criterion 1.2 for BA Control Centers provides a sufficient differentiation of the threshold defined for Medium Impact BA Control Centers. An analysis of BA footprints shows that the majority of Bas with significant impact are covered under this criterion.

Additional thresholds as specified in the criteria apply for this category.

Medium Impact Rating (M)

Generation

The criteria in Attachment 1's medium impact category that generally apply to Generation Owner and Operator (GO/GOP) Registered Entities are criteria 2.1, 2.3, 2.6, 2.9, and 2.11. Criterion 2.13 for BA Control Centers is also included here.

- Criterion 2.1 designates as medium impact those BES Cyber Systems that impact generation with a net Real Power capability exceeding 1500 MW. The 1500 MW criterion is sourced partly from the Contingency Reserve requirements in NERC standard BAL-002, whose purpose is "to ensure the Balancing Authority is able to utilize its Contingency Reserve to balance resources and demand and return Interconnection frequency within defined limits following a Reportable Disturbance." In particular, it requires that "as a minimum, the Balancing Authority or Reserve Sharing Group shall carry at least enough Contingency Reserve to cover the most severe single contingency." The drafting team used 1500 MW as a number derived from the most significant Contingency Reserves operated in various Bas in all regions.

  In the use of net Real Power capability, the drafting team sought to use a value that could be verified through existing requirements as proposed by NERC standard MOD-024 and current development efforts in that area.

  By using 1500 MW as a bright-line, the intent of the drafting team was to ensure that BES Cyber Systems with common mode vulnerabilities that could result in the loss of 1500 MW or more of generation at a single plant for a unit or group of units are adequately protected.

The drafting team also used additional time and value parameters to ensure the bright-lines and the values used to measure against them were relatively stable over the review period. Hence, where multiple values of net Real Power capability could be used for the Facilities' qualification against these bright-lines, the highest value was used.

- In Criterion 2.3, the drafting team sought to ensure that BES Cyber Systems for those generation Facilities that have been designated by the Planning Coordinator or Transmission Planner as necessary to avoid BES Adverse Reliability Impacts in the planning horizon of one year or more are categorized as medium impact. In specifying a planning horizon of one year or more, the intent is to ensure that those are units that are identified as a result of a "long term" reliability planning, i.e that the plans are spanning an operating period of at least 12 months: it does not mean that the operating day for the unit is necessarily beyond one year, but that the period that is being planned for is more than 1 year: it is specifically intended to avoid designating generation that is required to be run to remediate short term emergency reliability issues. These Facilities may be designated as "Reliability Must Run," and this designation is distinct from those generation Facilities designated as "must run" for market stabilization purposes. Because the use of the term "must run" creates some confusion in many areas, the drafting team chose to avoid using this term and instead drafted the requirement in more generic reliability language. In particular, the focus on preventing an Adverse Reliability Impact dictates that these units are designated as must run for reliability purposes beyond the local area. Those units designated as must run for voltage support in the local area would not generally be given this designation. In cases where there is no designated Planning Coordinator, the Transmission Planner is included as the Registered Entity that performs this designation.

  If it is determined through System studies that a unit must run in order to preserve the reliability of the BES, such as due to a Category C3 contingency as defined in TPL-003, then BES Cyber Systems for that unit are categorized as medium impact.

  The TPL standards require that, where the studies and plans indicate additional actions, that these studies and plans be communicated by the Planning Coordinator or Transmission Planner in writing to the Regional Entity/RRO. Actions necessary for the implementation of these plans by affected parties (generation owners/operators and Reliability Coordinators or other necessary party) are usually formalized in the form of an agreement and/or contract.

- Criterion 2.6 includes BES Cyber Systems for those Generation Facilities that have been identified as critical to the derivation of IROLs and their associated contingencies, as specified by FAC-014-2, **Establish and Communicate System Operating Limits**, R5.1.1 and R5.1.3.

  IROLs may be based on dynamic System phenomena such as instability or voltage collapse. Derivation of these IROLs and their associated contingencies often considers the effect of generation inertia and AVR response.

- Criterion 2.9 categorizes BES Cyber Systems for Special Protection Systems and Remedial Action Schemes as medium impact. Special Protection Systems and Remedial Action Schemes may be implemented to prevent disturbances that would result in exceeding IROLs if they do not provide the function required at the time it is required or if it operates outside of the parameters it was designed for. Generation Owners and Generator Operators which own BES Cyber Systems for such Systems and schemes designate them as medium impact.

- Criterion 2.11 categorizes as medium impact BES Cyber Systems used by and at Control Centers that perform the functional obligations of the Generator Operator for an aggregate generation of 1500 MW or higher in a single interconnection, and that have not already been included in Part 1.

- Criterion 2.13 categorizes as medium impact those BA Control Centers that "control" 1500 MW of generation or more in a single interconnection and that have not already been included in Part 1. The 1500 MW threshold is consistent with the impact level and rationale specified for Criterion 2.1.

Transmission

The SDT uses the phrases "Transmission Facilities at a single station or substation" and "Transmission stations or substations" to recognize the existence of both stations and substations. Many entities in industry consider a substation to be a location with physical borders (i.e. fence, wall, etc.) that contains at least an autotransformer. Locations also exist that do not contain autotransformers, and many entities in industry refer to those locations as stations (or switchyards). Therefore, the SDT chose to use both "station" and "substation" to refer to the locations where groups of Transmission Facilities exist.

- Criteria 2.2, 2.4 through 2.10, and 2.12 in Attachment 1 are the criteria that are applicable to Transmission Owners and Operators. In many of the criteria, the impact threshold is defined as the capability of the failure or compromise of a System to result in exceeding one or more Interconnection Reliability Operating Limits (IROLs). Criterion 2.2 includes BES Cyber Systems for those Facilities in Transmission Systems that provide reactive resources to enhance and preserve the reliability of the BES. The nameplate value is used here because there is no NERC requirement to verify actual capability of these Facilities. The value of 1000 MVARs used in this criterion is a value deemed reasonable for the purpose of determining criticality.

- Criterion 2.4 includes BES Cyber Systems for any Transmission Facility at a substation operated at 500 kV or higher. While the drafting team felt that Facilities operated at 500 kV or higher did not require any further qualification for their role as components of the backbone on the Interconnected BES, Facilities in the lower EHV range should have additional qualifying criteria for inclusion in the medium impact category.

It must be noted that if the collector bus for a generation plant (i.e. the plant is smaller in aggregate than the threshold set for generation in Criterion 2.1) is operated at 500kV, the collector bus should be considered a Generation Interconnection Facility, and not a Transmission Facility, according to the "Final Report from the Ad Hoc Group for Generation Requirements at the Transmission Interface." This collector bus would not be a facility for a medium impact BES Cyber System because it does not significantly affect the 500kV Transmission grid; it only affects a plant which is below the generation threshold.

- Criterion 2.5 includes BES Cyber Systems for facilities at the lower end of BES Transmission with qualifications for inclusion if they are deemed highly likely to have significant impact on the BES. While the criterion has been specified as part of the rationale for requiring protection for significant impact on the BES, the drafting team included, in this criterion, additional qualifications that would ensure the required level of impact to the BES. The drafting team:

    - Excluded radial facilities that would only provide support for single generation facilities.

    - Specified interconnection to at least three transmission stations or substations to ensure that the level of impact would be appropriate.

  The total aggregated weighted value of 3,000 was derived from weighted values related to three connected 345 kV lines and five connected 230 kV lines at a transmission station or substation. The total aggregated weighted value is used to account for the true impact to the BES, irrespective of line kV rating and mix of multiple kV rated lines.

  Additionally, in NERC's document "Integrated Risk Assessment Approach – Refinement to Severity Risk Index", Attachment 1, the report used an average MVA line loading based on kV rating:

    - 230 kV –> 700 MVA

    - 345 kV –> 1,300 MVA

    - 500 kV –> 2,000 MVA

    - 765 kV –> 3,000 MVA

  In the terms of applicable lines and connecting "other Transmission stations or substations" determinations, the following should be considered:

    - For autotransformers in a station, Responsible Entities have flexibility in determining whether the groups of Facilities are considered a single substation or station location or multiple substations or stations. In most cases, Responsible Entities would probably consider them as Facilities at a single substation or station unless geographically dispersed. In these cases of these transformers being within the "fence" of the substation or station, autotransformers may not count as separate

connections to other stations. The use of common BES Cyber Systems may negate any rationale for any consideration otherwise. In the case of autotransformers that are geographically dispersed from a station location, the calculation would take into account the connections in and out of each station or substation location.

- Multiple-point (or multiple-tap) lines are considered to contribute a single weight value per line and affect the number of connections to other stations. Therefore, a single 230 kV multiple-point line between three Transmission stations or substations would contribute an aggregated weighted value of 700 and connect Transmission Facilities at a single station or substation to two other Transmission stations or substations.

- Multiple lines between two Transmission stations or substations are considered to contribute multiple weight values per line, but these multiple lines between the two stations only connect one station to one other station. Therefore, two 345 kV lines between two Transmission stations or substations would contribute an aggregated weighted value of 2600 and connect Transmission Facilities at a single station or substation to one other Transmission station or substation.

Criterion 2.5's qualification for Transmission Facilities at a Transmission station or substation is based on 2 distinct conditions.

1. The first condition is that Transmission Facilities at a single station or substation where that station or substation connect, at voltage levels of 200 kV or higher to three (3) other stations or substations, to three other stations or substations. This qualification is meant to ensure that connections that operate at voltages of 500 kV or higher are included in the count of connections to other stations or substations as well.
2. The second qualification is that the aggregate value of all lines entering or leaving the station or substation must exceed 3000. This qualification does not include the consideration of lines operating at lower than 200 kV, or 500 kV or higher, the latter already qualifying as medium impact under criterion 2.4. : there is no value to be assigned to lines at voltages of less than 200 kV or 500 kV or higher in the table of values for the contribution to the aggregate value of 3000.

The Transmission Facilities at the station or substation must meet both qualifications to be considered as qualified under criterion 2.5.

- Criterion 2.6 include BES Cyber Systems for those Transmission Facilities that have been identified as critical to the derivation of IROLs and their associated contingencies, as specified by FAC-014-2, **Establish and Communicate System Operating Limits**, R5.1.1 and R5.1.3.

- Criterion 2.7 is sourced from the NUC-001 NERC standard, Requirement R9.2.2, for the support of Nuclear Facilities. NUC-001 ensures that reliability of NPIR's are ensured through adequate coordination between the Nuclear Generator Owner/Operator and its Transmission provider "for the purpose of ensuring nuclear plant safe operation and shutdown." In particular, there are specific requirements to coordinate physical and cyber security protection of these interfaces.

- Criterion 2.8 designates as medium impact those BES Cyber Systems that impact Transmission Facilities necessary to directly support generation that meet the criteria in Criteria 2.1 (generation Facilities with output greater than 1500 MW) and 2.3 (generation Facilities generally designated as "must run" for wide area reliability in the planning horizon). The Responsible Entity can request a formal statement from the Generation owner as to the qualification of generation Facilities connected to their Transmission systems.

- Criterion 2.9 designates as medium impact those BES Cyber Systems for those Special Protection Systems (SPS), Remedial Action Schemes (RAS), or automated switching Systems installed to ensure BES operation within IROLs. The degradation, compromise or unavailability of these BES Cyber Systems would result in exceeding IROLs if they fail to operate as designed. By the definition of IROL, the loss or compromise of any of these have Wide Area impacts.

- Criterion 2.10 designates as medium impact those BES Cyber Systems for Systems or Elements that perform automatic Load shedding, without human operator initiation, of 300 MW or more. The SDT spent considerable time discussing the wording of Criterion 2.10, and chose the term "Each" to represent that the criterion applied to a discrete System or Facility. In the drafting of this criterion, the drafting team sought to include only those Systems that did not require human operator initiation, and targeted in particular those underfrequency load shedding (UFLS) Facilities and systems and undervoltage load shedding (UVLS) systems and Elements that would be subject to a regional Load shedding requirement to prevent Adverse Reliability Impact. These include automated UFLS systems or UVLS systems that are capable of Load shedding 300 MW or more. It should be noted that those qualifying systems which require a human operator to arm the system, but once armed, trigger automatically, are still to be considered as not requiring human operator initiation and should be designated as medium impact. The 300 MW threshold has been defined as the aggregate of the highest MW Load value, as defined by the applicable regional Load Shedding standards, for the preceding 12 months to account for seasonal fluctuations.

  This particular threshold (300 MW) was provided in CIP, Version 1. The SDT believes that the threshold should be lower than the 1500MW generation requirement since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System and hence requires a lower threshold. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

In ERCOT, the Load acting as a Resource ("LaaR") Demand Response Program is not part of the regional load shedding program, but an ancillary services market. In general, similar demand response programs that are not part of the NERC or regional reliability Load shedding programs, but are offered as components of an ancillary services market do not qualify under this criterion.

The language used in section 4 for UVLS and UFLS and in criterion 2.10 of Attachment 1 is designed to be consistent with requirements set in the PRC standards for UFLS and UVLS.

- Criterion 2.12 categorizes as medium impact those BES Cyber Systems used by and at Control Centers and associated data centers performing the functional obligations of a Transmission Operator and that have not already been categorized as high impact.

- Criterion 2.13 categorizes as Medium Impact those BA Control Centers that "control" 1500 MW of generation or more in a single Interconnection. The 1500 MW threshold is consistent with the impact level and rationale specified for Criterion 2.1.

Low Impact Rating (L)

BES Cyber Systems not categorized in high impact or medium impact default to low impact. Note that low impact BES Cyber Systems do not require discrete identification.

Restoration Facilities

- Several discussions on the CIP Version 5 standards suggest entities owning Blackstart Resources and Cranking Paths might elect to remove those services to avoid higher compliance costs. For example, one Reliability Coordinator reported a 25% reduction of Blackstart Resources as a result of the Version 1 language, and there could be more entities that make this choice under Version 5.

  In response, the CIP Version 5 drafting team sought informal input from NERC's Operating and Planning Committees. The committees indicate there has already been a reduction in Blackstart Resources because of increased CIP compliance costs, environmental rules, and other risks; continued inclusion within Version 5 at a category that would very significantly increase compliance costs can result in further reduction of a vulnerable pool.

  The drafting team moved from the categorization of restoration assets such as Blackstart Resources and Cranking Paths as medium impact (as was the case in earlier drafts) to categorization of these assets as low impact as a result of these considerations. This will not relieve asset owners of all responsibilities, as would have been the case in CIP-002, Versions 1-4 (since only Cyber Assets with routable connectivity which are essential to restoration assets are included in those versions). Under the low impact categorization, those assets will be protected in the areas of cyber security awareness, physical access control, and electronic access control, and they will have obligations regarding incident response. This represents a net gain to bulk power system reliability, however, since many of those assets do not meet criteria for inclusion under Versions 1-4.

Weighing the risks to overall BES reliability, the drafting team determined that this re-categorization represents the option that would be the least detrimental to restoration function and, thus, overall BES reliability. Removing Blackstart Resources and Cranking Paths from medium impact promotes overall reliability, as the likely alternative is fewer Blackstart Resources supporting timely restoration when needed.

BES Cyber Systems for generation resources that have been designated as Blackstart Resources in the Transmission Operator's restoration plan default to low impact. NERC Standard EOP-005-2 requires the Transmission Operator to have a Restoration Plan and to list its Blackstart Resources in its plan, as well as requirements to test these Resources. This criterion designates only those generation Blackstart Resources that have been designated as such in the Transmission Operator's restoration plan. The glossary term Blackstart Capability Plan has been retired.

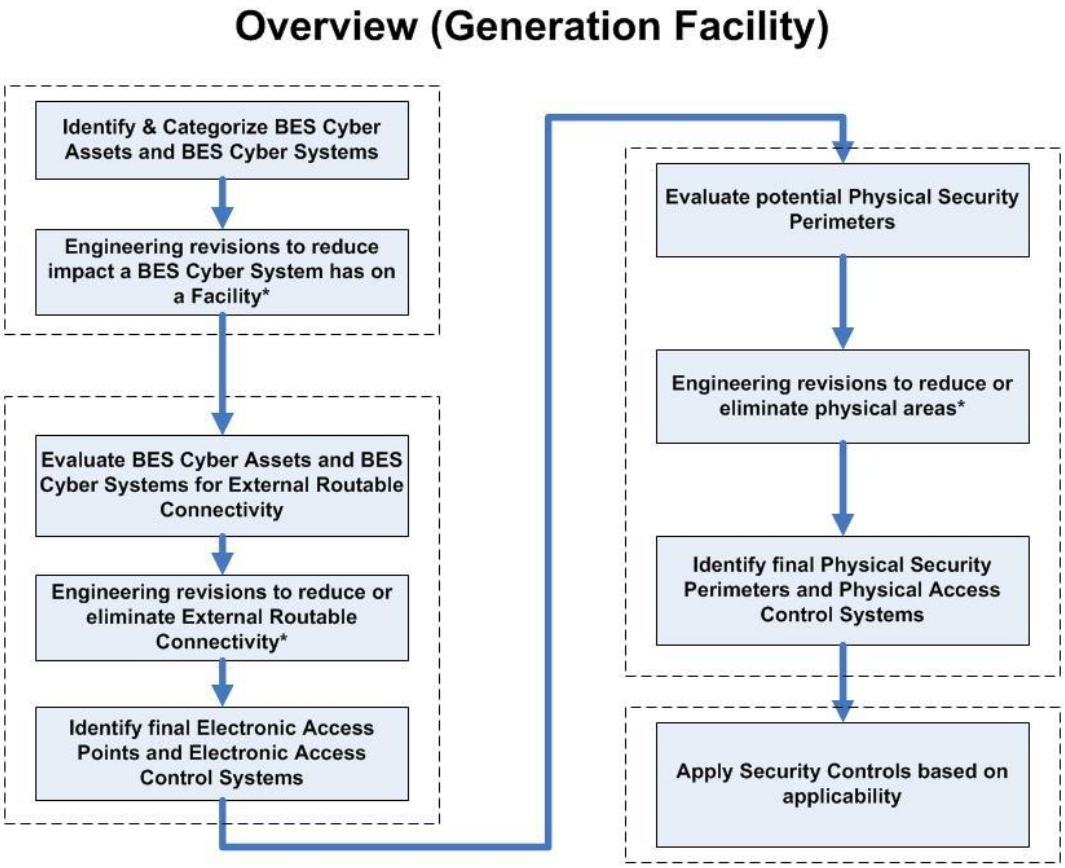
Regarding concerns of communication to BES Asset Owners and Operators of their role in the Restoration Plan, Transmission Operators are required in NERC Standard EOP-005-2 to "provide the entities identified in its approved restoration plan with a description of any changes to their roles and specific tasks prior to the implementation date of the plan."

- BES Cyber Systems for Facilities and Elements comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource to the first Interconnection point of the generation unit(s) to be started, as identified in the Transmission Operator's restoration plan, default to the category of low impact: however, these systems are explicitly called out to ensure consideration for inclusion in the scope of the version 5 CIP standards. This requirement for inclusion in the scope is sourced from requirements in NERC standard EOP-005-2, which requires the Transmission Operator to include in its Restoration Plan the Cranking Paths and initial switching requirements from the Blackstart Resource and the unit(s) to be started.

  Distribution Providers may note that they may have BES Cyber Systems that must be scoped in if they have Elements listed in the Transmission Operator's Restoration Plan that are components of the Cranking Path.

Use Case: CIP Process Flow

The following CIP use case process flow for a generator Operator/Owner was provided by a participant in the development of the Version 5 standards and is provided here as an example of a process used to identify and categorize BES Cyber Systems and BES Cyber Assets; review, develop, and implement strategies to mitigate overall risks; and apply applicable security controls.



* - Engineering revisions will need to be reviewed for cost justification, operational\safety requirements, support requirements, and technical limitations.

Rationale:

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for R1:

BES Cyber Systems at each site location have varying impact on the reliable operation of the Bulk Electric System. Attachment 1 provides a set of "bright-line" criteria that the Responsible Entity must use to identify these BES Cyber Systems in accordance with the impact on the BES. BES Cyber Systems must be identified and categorized according to their impact so that the appropriate measures can be applied, commensurate with their impact. These impact categories will be the basis for the application of appropriate requirements in CIP-003-CIP-011.

Rationale for R2:

The lists required by Requirement R1 are reviewed on a periodic basis to ensure that all BES Cyber Systems required to be categorized have been properly identified and categorized. The miscategorization or non-categorization of a BES Cyber System can lead to the application of inadequate or non-existent cyber security controls that can lead to compromise or misuse that can affect the real-time operation of the BES. The CIP Senior Manager's approval ensures proper oversight of the process by the appropriate Responsible Entity personnel.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a Responsible Entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3.	Update

		Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5.1	9/30/13	Replaced “Devices” with “Systems” in a definition in background section.	Errata
5.1	11/22/13	FERC Order issued approving CIP-002-5.1.	
5.1a	11/02/16	Adopted by the NERC Board of Trustees.	
5.1a	12/14/2016	FERC letter Order approving CIP-002-5.1a. Docket No. RD17-2-000.	

Appendix 1

Requirement Number and Text of Requirement
CIP-002-5.1, Requirement R1 R1. Each Responsible Entity shall implement a process that considers each of the following assets for purposes of parts 1.1 through 1.3: i. Control Centers and backup Control Centers; ii. Transmission stations and substations; iii. Generation resources; iv. Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements; v. Special Protection Systems that support the reliable operation of the Bulk Electric System; and vi. For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above. 1.1. Identify each of the high impact BES Cyber Systems according to Attachment 1, Section 1, if any, at each asset; 1.2. Identify each of the medium impact BES Cyber Systems according to Attachment 1, Section 2, if any, at each asset; and 1.3. Identify each asset that contains a low impact BES Cyber System according to Attachment 1, Section 3, if any (a discrete list of low impact BES Cyber Systems is not required). Attachment 1, Criterion 2.1 2. Medium Impact Rating (M) Each BES Cyber System, not included in Section 1 above, associated with any of the following: 2.1. Commissioned generation, by each group of generating units at a single plant location, with an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection. For each group of generating units, the only BES Cyber Systems that meet this criterion are those shared BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection.

Questions

Energy Sector Security Consortium, Inc. (EnergySec) submitted a Request for Interpretation (RFI) seeking clarification of Criterion 2.1 of Attachment 1 in Reliability Standard CIP-002-5.1 regarding the use of the phrase "shared BES Cyber Systems."

The Interpretation Drafting Team identified the following questions in the RFI:

1. Whether the phrase "shared BES Cyber Systems" means that the evaluation for Criterion 2.1 shall be performed individually for each discrete BES Cyber System at a single plant location, or collectively for groups of BES Cyber Systems?
2. Whether the phrase "shared BES Cyber Systems" refers to discrete BES Cyber Systems that are shared by multiple units, or groups of BES Cyber Systems that could collectively impact multiple units?
3. If the phrase applies collectively to groups of BES Cyber Systems, what criteria should be used to determine which BES Cyber Systems should be grouped for collective evaluation?

Responses

Question 1: Whether the phrase "shared BES Cyber Systems," means that the evaluation for Criterion 2.1 shall be performed individually for each discrete BES Cyber System at a single plant location, or collectively for groups of BES Cyber Systems?

The evaluation as to whether a BES Cyber System is shared should be performed individually for each discrete BES Cyber System. In the standard language of CIP-002-5.1, there is no reference to or obligation to group BES Cyber Systems. Requirement R1, part 1.2 states "Identify *each* of the medium impact BES Cyber Systems according to Attachment 1, Section 2…" Further, the preamble of Section 2 of CIP-002-5.1 Attachment 1 states "*Each BES Cyber System*…associated with any of the following [criteria]." (emphasis added)

Additionally, the Background section of CIP-002-5.1 states that "[i]t is left up to the Responsible Entity to determine the level of granularity at which to identify a BES Cyber System within the qualifications in the definition of BES Cyber System." The Background section also provides:

> The Responsible Entity should take into consideration the operational environment and scope of management when defining the BES Cyber System boundary in order to maximize efficiency in secure operations. Defining the boundary too tightly may result in redundant paperwork and authorizations, while defining the boundary too broadly could make the secure operation of the BES Cyber System difficult to monitor and assess.

Question 2: Whether the phrase "shared BES Cyber Systems" refers to discrete BES Cyber Systems that are shared by multiple units, or groups of BES Cyber Systems that could collectively impact multiple units?

The phrase "shared BES Cyber Systems" refers to discrete BES Cyber Systems that are shared by multiple generation units.

The use of the term "shared" is also clarified in the NERC Frequently Asked Questions (FAQ) document issued by NERC Compliance to support implementation of the CIP Reliability Standards. FAQ #49 provides:

> Shared BES Cyber Systems are those that are associated with any combination of units in a single Interconnection, as referenced in CIP-002-5.1, Attachment 1, impact rating criteria 2.1 and 2.2. For criterion 2.1 "BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection." For criterion 2.2: "BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of resources that in aggregate equal or exceed 1000 MVAR. Also refer to the Lesson Learned for CIP-002-5.1 Requirement R1: **Impact Rating of Generation Resource Shared BES Cyber Systems** for further information and examples.

Question 3: If the phrase applies collectively to groups of BES Cyber Systems, what criteria should be used to determine which BES Cyber Systems should be grouped for collective evaluation?

The phrase applies to each discrete BES Cyber System.

Appendix QC-CIP-002-5.1a
Provisions specific to the standard CIP-002-5.1a applicable in Québec

This appendix establishes specific provisions for the application of the standard in Québec. Provisions of the standard and of its appendix must be read together for the purposes of understanding and interpretation. Where the standard and appendix differ, the appendix shall prevail.

A. Introduction

1. **Title:** Cyber Security — BES Cyber System Categorization

2. **Number:** CIP-002-5.1a

3. **Purpose:** No specific provision

4. **Applicability:**

   Functional Entities

   No specific provision

   Facilities

   This standard only applies to the facilities of the Main Transmission System (RTP) and to the facilities specified for the Distribution Provider. In the application of this standard, all references to the terms "Bulk Electric System" or "BES" shall be replaced by the terms "Main Transmission System" or "RTP" respectively.

   Additional Exemptions

   The following are exempt from this standard:

   - Any generating facility that meets the two following conditions: (1) the nameplate capacity of the facility is 300 MVA or less, and (2) no unit of the facility can be synchronized with a neighbouring system.
   - Step-up substations of generating facilities identified in the preceding point.

5. **Effective Date:**

   5.1. Adoption of the standard by the Régie de l'énergie: March 15, 2019

   5.2. Adoption of the appendix by the Régie de l'énergie: March 15, 2019

   5.3. Effective date of the standard and its appendix in Québec:

   April 1, 2019

   The enforcement dates are the same as in CIP-002-5.1 :

   For entities that have assets classified as critical for CIP Standards (version 1):

   - April 1, 2019 for "high" or "medium" impact BES Cyber Systems;
   - April 1, 2019 for "low" impact BES Cyber Systems.

For entities that have neither assets classified as critical for CIP Standards (version 1) nor generation facilities for industrial use:

- April 1, 2019 for “high” or “medium” impact BES Cyber Systems;
- October 1, 2019 for “low” impact BES Cyber Systems.

For entities that have generation facilities for industrial use:

- April 1, 2019 for “high” or “medium” impact BES Cyber Systems;
- April 1, 2020 for “low” impact BES Cyber Systems.

6. Background: No specific provision

B. Requirements and Measures

No specific provision

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

The Régie de l’énergie is responsible, in Québec, for compliance enforcement with respect to the reliability standard and its appendix that it adopts.

1.2. Evidence Retention

No specific provision

1.3. Compliance Monitoring and Assessment Processes

No specific provision

1.4. Additional Compliance Information

No specific provision

2. Table of Compliance Elements

No specific provision

D. Regional Variances

No specific provision

E. Interpretations

No specific provision

F. Associated Documents

No specific provision

CIP-002-5.1a — Attachment 1

No specific provision

Guidelines and Technical Basis

No specific provision

Rationale

No specific provision

Revision History

Revision	Date	Action	Change Tracking
0	March 15, 2019	New appendix.	New

A. Introduction

1. Title: Cyber Security — Security Management Controls

2. Number: CIP-003-8

3. Purpose: To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1. Balancing Authority

4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in Section 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-003-8:

4.2.3.1. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESPs).

4.2.3.3. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

5. Effective Dates:

See Implementation Plan for CIP-003-8.

6. Background:

Standard CIP-003 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.

The term policy refers to one or a collection of written documents that are used to communicate the Responsible Entities' management goals, objectives and expectations for how the Responsible Entity will protect its BES Cyber Systems. The use of policies also establishes an overall governance foundation for creating a culture of security and compliance with laws, regulations, and standards.

The term documented processes refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements.

The terms program and plan are sometimes used in place of documented processes where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as plans (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term program may refer to the organization's overall implementation of its policies, plans, and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Reliability Standards could also be referred to as a program. However, the terms program and plan do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high, medium, and low impact BES Cyber Systems. For example, a single cyber security awareness program could meet the requirements across multiple BES Cyber Systems.

Measures provide examples of evidence to show documentation and implementation of the requirement. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the BES. A review of UFLS

tolerances defined within Regional Reliability Standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

B. Requirements and Measures

R1. Each Responsible Entity shall review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies that collectively address the following topics: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1. For its high impact and medium impact BES Cyber Systems, if any:

1.1.1. Personnel and training (CIP-004);

1.1.2. Electronic Security Perimeters (CIP-005) including Interactive Remote Access;

1.1.3. Physical security of BES Cyber Systems (CIP-006);

1.1.4. System security management (CIP-007);

1.1.5. Incident reporting and response planning (CIP-008);

1.1.6. Recovery plans for BES Cyber Systems (CIP-009);

1.1.7. Configuration change management and vulnerability assessments (CIP-010);

1.1.8. Information protection (CIP-011); and

1.1.9. Declaring and responding to CIP Exceptional Circumstances.

1.2. For its assets identified in CIP-002 containing low impact BES Cyber Systems, if any:

1.2.1. Cyber security awareness;

1.2.2. Physical security controls;

1.2.3. Electronic access controls;

1.2.4. Cyber Security Incident response;

1.2.5. Transient Cyber Assets and Removable Media malicious code risk mitigation; and

1.2.6. Declaring and responding to CIP Exceptional Circumstances.

M1. Examples of evidence may include, but are not limited to, policy documents; revision history, records of review, or workflow evidence from a document management system that indicate review of each cyber security policy at least once every 15 calendar months; and documented approval by the CIP Senior Manager for each cyber security policy.

R2. Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall implement one or more documented cyber security plan(s) for its low impact BES Cyber Systems that include the sections in Attachment 1. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

Note: An inventory, list, or discrete identification of low impact BES Cyber Systems or their BES Cyber Assets is not required. Lists of authorized users are not required.

M2. Evidence shall include each of the documented cyber security plan(s) that collectively include each of the sections in Attachment 1 and additional evidence to demonstrate implementation of the cyber security plan(s). Additional examples of evidence per section are located in Attachment 2.

R3. Each Responsible Entity shall identify a CIP Senior Manager by name and document any change within 30 calendar days of the change. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. An example of evidence may include, but is not limited to, a dated and approved document from a high level official designating the name of the individual identified as the CIP Senior Manager.

R4. The Responsible Entity shall implement a documented process to delegate authority, unless no delegations are used. Where allowed by the CIP Standards, the CIP Senior Manager may delegate authority for specific actions to a delegate or delegates. These delegations shall be documented, including the name or title of the delegate, the specific actions delegated, and the date of the delegation; approved by the CIP Senior Manager; and updated within 30 days of any change to the delegation. Delegation changes do not need to be reinstated with a change to the delegator. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M4. An example of evidence may include, but is not limited to, a dated document, approved by the CIP Senior Manager, listing individuals (by name or title) who are delegated the authority to approve or authorize specifically identified items.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority:
As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:
The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audits
- Self-Certifications
- Spot Checking
- Compliance Investigations
- Self-Reporting
- Complaints

1.4. Additional Compliance Information:
None.

Violation Severity Levels

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-8)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address one of the nine topics required by R1. (R1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 15 calendar months but did	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address two of the nine topics required by R1. (R1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 16 calendar months but did	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address three of the nine topics required by R1. (R1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 17 calendar months but did complete this review in less than or equal to 18	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address four or more of the nine topics required by R1. (R1.1) OR The Responsible Entity did not have any documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1. (R1.1) OR The Responsible Entity did not

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-8)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			complete this review in less than or equal to 16 calendar months of the previous review. (R1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (R1.1)	complete this review in less than or equal to 17 calendar months of the previous review. (R1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of the previous approval. (R1.1)	calendar months of the previous review. (R1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (R1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact	complete its review of the one or more documented cyber security policies as required by R1 within 18 calendar months of the previous review. (R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (R1.1) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-8)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address one of the six topics required by R1. (R1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 within 15 calendar	OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address two of the six topics required by R1. (R1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 within 16 calendar	BES Cyber Systems, but did not address three of the six topics required by R1. (R1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its	The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address four or more of the six topics required by R1. (R1.2) OR The Responsible Entity did not have any documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by R1. (R1.2) OR The Responsible Entity did not

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-8)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			months but did complete this review in less than or equal to 16 calendar months of the previous review. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of	months but did complete this review in less than or equal to 17 calendar months of the previous review. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 16 calendar months but did complete this approval in less than or equal to 17	assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (R1.2)	complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (R1.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-8)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			the previous approval. (R1.2)	calendar months of the previous approval. (R1.2)		
R2	**Operations Planning**	**Lower**	The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document cyber security awareness according to Requirement R2, Attachment 1, Section 1. (R2) OR The Responsible Entity implemented electronic access controls but failed to document its cyber security plan(s) for electronic access controls according to Requirement R2,	The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to reinforce cyber security practices at least once every 15 calendar months according to Requirement R2, Attachment 1, Section 1. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed	The Responsible Entity documented the physical access controls for its assets containing low impact BES Cyber Systems, but failed to implement the physical security controls according to Requirement R2, Attachment 1, Section 2. (R2) OR The Responsible Entity documented its cyber security plan(s) for electronic access controls for its assets containing low impact BES Cyber Systems, but failed to permit only necessary inbound and outbound electronic	The Responsible Entity failed to document and implement one or more cyber security plan(s) for its assets containing low impact BES Cyber Systems according to Requirement R2, Attachment 1. (R2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-8)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Attachment 1, Section 3. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document one or more Cyber Security Incident response plan(s) according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented one or more Cyber Security Incident response plan(s) within its cyber security plan(s) for its assets containing	to document physical security controls according to Requirement R2, Attachment 1, Section 2. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document electronic access controls according to Requirement R2, Attachment 1, Section 3. (R2) OR The Responsible Entity documented its cyber security plan(s) for electronic access controls but	access controls according to Requirement R2, Attachment 1, Section 3.1. (R2) OR The Responsible Entity documented one or more Cyber Security Incident response plan(s) within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to test each Cyber Security Incident response plan(s) at least once every 36 calendar months according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented the determination of	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-8)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			low impact BES Cyber Systems, but failed to update each Cyber Security Incident response plan(s) within 180 days according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to manage its Transient Cyber Asset(s) according to Requirement R2, Attachment 1, Section 5.1. (R2) OR The Responsible Entity documented	failed to implement authentication for all Dial-up Connectivity that provides access to low impact BES Cyber System(s), per Cyber Asset capability according to Requirement R2, Attachment 1, Section 3.2 (R2) OR The Responsible Entity documented one or more incident response plan(s) within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to include the process for identification, classification, and response to Cyber Security Incidents	whether an identified Cyber Security Incident is a Reportable Cyber Security Incident, but failed to notify the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation for the introduction of malicious code for Transient Cyber Assets managed by the Responsible Entity according to Requirement R2,	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-8)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			its plan(s) for Transient Cyber Assets, but failed to document the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (R2)	according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document the determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2,	Attachment 1, Section 5.1. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to Requirement R2, Attachment 1, Section 5.2. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation for	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-8)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				Attachment 1, Section 4. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document mitigation for the introduction of malicious code for Transient Cyber Assets managed by the Responsible Entity according to Requirement R2, Attachment 1, Sections 5.1 and 5.3. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber	the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact BES Cyber System according to Requirement R2, Attachment 1, Section 5.3. (R2)	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-8)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				Assets and Removable Media, but failed to document mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to Requirement R2, Attachment 1, Section 5.2. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement the Removable Media section(s) according to Requirement R2,		

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-8)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				Attachment 1, Section 5.3. (R2)		
R3	**Operations Planning**	**Medium**	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 30 calendar days but did document this change in less than 40 calendar days of the change. (R3)	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 40 calendar days but did document this change in less than 50 calendar days of the change. (R3)	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 50 calendar days but did document this change in less than 60 calendar days of the change. (R3)	The Responsible Entity has not identified, by name, a CIP Senior Manager. OR The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 60 calendar days of the change. (R3)
R4	**Operations Planning**	**Lower**	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate	The Responsible Entity has used delegated authority for actions where allowed by the CIP Standards, but does not have a process

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-8)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			not document changes to the delegate within 30 calendar days but did document this change in less than 40 calendar days of the change. (R4)	not document changes to the delegate within 40 calendar days but did document this change in less than 50 calendar days of the change. (R4)	within 50 calendar days but did document this change in less than 60 calendar days of the change. (R4)	to delegate actions from the CIP Senior Manager. (R4) OR The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 60 calendar days of the change. (R4)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.

Version	Date	Action	Change Tracking
5	11/22/13	FERC Order issued approving CIP-003-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
6	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
6	1/21/16	FERC Order issued approving CIP-003-6. Docket No. RM15-14-000	
7	2/9/17	Adopted by the NERC Board of Trustees.	Revised to address FERC Order No. 822 directives regarding (1) the definition of LERC and (2) transient devices.
7	4/19/18	FERC Order issued approving CIP-003-7. Docket No. RM17-11-000	

Version	Date	Action	Change Tracking
8	5/9/19	Adopted by the NERC Board of Trustees.	Removed SPS references. Revised to address FERC Order No. 843 regarding mitigating the risk of malicious code.
8	7/31/2019	FERC Order issued approving CIP-003-8. Docket No. RD19-5-000.	

Attachment 1

Required Sections for Cyber Security Plan(s) for Assets Containing Low Impact BES Cyber Systems

Responsible Entities shall include each of the sections provided below in the cyber security plan(s) required under Requirement R2.

Responsible Entities with multiple-impact BES Cyber Systems ratings can utilize policies, procedures, and processes for their high or medium impact BES Cyber Systems to fulfill the sections for the development of low impact cyber security plan(s). Each Responsible Entity can develop a cyber security plan(s) either by individual asset or groups of assets.

Section 1. Cyber Security Awareness: Each Responsible Entity shall reinforce, at least once every 15 calendar months, cyber security practices (which may include associated physical security practices).

Section 2. Physical Security Controls: Each Responsible Entity shall control physical access, based on need as determined by the Responsible Entity, to (1) the asset or the locations of the low impact BES Cyber Systems within the asset, and (2) the Cyber Asset(s), as specified by the Responsible Entity, that provide electronic access control(s) implemented for Section 3.1, if any.

Section 3. Electronic Access Controls: For each asset containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement electronic access controls to:

3.1 Permit only necessary inbound and outbound electronic access as determined by the Responsible Entity for any communications that are:

i. between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s);

ii. using a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s); and

iii. not used for time-sensitive protection or control functions between intelligent electronic devices (e.g., communications using protocol IEC TR-61850-90-5 R-GOOSE).

3.2 Authenticate all Dial-up Connectivity, if any, that provides access to low impact BES Cyber System(s), per Cyber Asset capability.

Section 4. Cyber Security Incident Response: Each Responsible Entity shall have one or more Cyber Security Incident response plan(s), either by asset or group of assets, which shall include:

4.1 Identification, classification, and response to Cyber Security Incidents;

4.2 Determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the

Electricity Information Sharing and Analysis Center (E-ISAC), unless prohibited by law;

4.3 Identification of the roles and responsibilities for Cyber Security Incident response by groups or individuals;

4.4 Incident handling for Cyber Security Incidents;

4.5 Testing the Cyber Security Incident response plan(s) at least once every 36 calendar months by: (1) responding to an actual Reportable Cyber Security Incident; (2) using a drill or tabletop exercise of a Reportable Cyber Security Incident; or (3) using an operational exercise of a Reportable Cyber Security Incident; and

4.6 Updating the Cyber Security Incident response plan(s), if needed, within 180 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident.

Section 5. Transient Cyber Asset and Removable Media Malicious Code Risk Mitigation: Each Responsible Entity shall implement, except under CIP Exceptional Circumstances, one or more plan(s) to achieve the objective of mitigating the risk of the introduction of malicious code to low impact BES Cyber Systems through the use of Transient Cyber Assets or Removable Media. The plan(s) shall include:

5.1 For Transient Cyber Asset(s) managed by the Responsible Entity, if any, the use of one or a combination of the following in an ongoing or on-demand manner (per Transient Cyber Asset capability):

- Antivirus software, including manual or managed updates of signatures or patterns;
- Application whitelisting; or
- Other method(s) to mitigate the introduction of malicious code.

5.2 For Transient Cyber Asset(s) managed by a party other than the Responsible Entity, if any:

5.2.1 Use one or a combination of the following prior to connecting the Transient Cyber Asset to a low impact BES Cyber System (per Transient Cyber Asset capability):

- Review of antivirus update level;
- Review of antivirus update process used by the party;
- Review of application whitelisting used by the party;
- Review use of live operating system and software executable only from read-only media;
- Review of system hardening used by the party; or

- Other method(s) to mitigate the introduction of malicious code.

5.2.2 For any method used pursuant to 5.2.1, Responsible Entities shall determine whether any additional mitigation actions are necessary and implement such actions prior to connecting the Transient Cyber Asset.

5.3 For Removable Media, the use of each of the following:

5.3.1 Method(s) to detect malicious code on Removable Media using a Cyber Asset other than a BES Cyber System; and

5.3.2 Mitigation of the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact BES Cyber System.

Attachment 2

Examples of Evidence for Cyber Security Plan(s) for Assets Containing Low Impact BES Cyber Systems

Section 1. Cyber Security Awareness: An example of evidence for Section 1 may include, but is not limited to, documentation that the reinforcement of cyber security practices occurred at least once every 15 calendar months. The evidence could be documentation through one or more of the following methods:

- Direct communications (for example, e-mails, memos, or computer-based training);
- Indirect communications (for example, posters, intranet, or brochures); or
- Management support and reinforcement (for example, presentations or meetings).

Section 2. Physical Security Controls: Examples of evidence for Section 2 may include, but are not limited to:

- Documentation of the selected access control(s) (e.g., card key, locks, perimeter controls), monitoring controls (e.g., alarm systems, human observation), or other operational, procedural, or technical physical security controls that control physical access to both:
  a. The asset, if any, or the locations of the low impact BES Cyber Systems within the asset; and
  b. The Cyber Asset(s) specified by the Responsible Entity that provide(s) electronic access controls implemented for Attachment 1, Section 3.1, if any.

Section 3. Electronic Access Controls: Examples of evidence for Section 3 may include, but are not limited to:

1. Documentation showing that at each asset or group of assets containing low impact BES Cyber Systems, routable communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset is restricted by electronic access controls to permit only inbound and outbound electronic access that the Responsible Entity deems necessary, except where an entity provides rationale that communication is used for time-sensitive protection or control functions between intelligent electronic devices. Examples of such documentation may include, but are not limited to representative diagrams that illustrate control of inbound and outbound communication(s) between the low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s) or lists of implemented electronic access controls (e.g., access control lists restricting IP addresses, ports, or services; implementing unidirectional gateways).

2. Documentation of authentication for Dial-up Connectivity (e.g., dial out only to a preprogrammed number to deliver data, dial-back modems, modems that must be remotely controlled by the control center or control room, or access control on the BES Cyber System).

Section 4. Cyber Security Incident Response: An example of evidence for Section 4 may include, but is not limited to, dated documentation, such as policies, procedures, or process documents of one or more Cyber Security Incident response plan(s) developed either by asset or group of assets that include the following processes:

1. to identify, classify, and respond to Cyber Security Incidents; to determine whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and for notifying the Electricity Information Sharing and Analysis Center (E-ISAC);
2. to identify and document the roles and responsibilities for Cyber Security Incident response by groups or individuals (e.g., initiating, documenting, monitoring, reporting, etc.);
3. for incident handling of a Cyber Security Incident (e.g., containment, eradication, or recovery/incident resolution);
4. for testing the plan(s) along with the dated documentation that a test has been completed at least once every 36 calendar months; and
5. to update, as needed, Cyber Security Incident response plan(s) within 180 calendar days after completion of a test or actual Reportable Cyber Security Incident.

Section 5. Transient Cyber Asset and Removable Media Malicious Code Risk Mitigation:

1. Examples of evidence for Section 5.1 may include, but are not limited to, documentation of the method(s) used to mitigate the introduction of malicious code such as antivirus software and processes for managing signature or pattern updates, application whitelisting practices, processes to restrict communication, or other method(s) to mitigate the introduction of malicious code. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the vendor or Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.
2. Examples of evidence for Section 5.2.1 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of the installed antivirus update level; memoranda, electronic mail, system documentation, policies or contracts from the party other than the Responsible Entity that identify the antivirus update process, the use of application whitelisting, use of live operating systems or system hardening performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail or contracts that

identifies the Responsible Entity's acceptance that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate malicious code for Transient Cyber Asset(s) managed by a party other than the Responsible Entity. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Examples of evidence for Attachment 1, Section 5.2.2 may include, but are not limited to, documentation from change management systems, electronic mail, or contracts that identifies a review to determine whether additional mitigation is necessary and has been implemented prior to connecting the Transient Cyber Asset managed by a party other than the Responsible Entity.

3. Examples of evidence for Section 5.3.1 may include, but are not limited to, documented process(es) of the method(s) used to detect malicious code such as results of scan settings for Removable Media, or implementation of on-demand scanning. Examples of evidence for Section 5.3.2 may include, but are not limited to, documented process(es) for the method(s) used for mitigating the threat of detected malicious code on Removable Media, such as logs from the method(s) used to detect malicious code that show the results of scanning and the mitigation of detected malicious code on Removable Media or documented confirmation by the entity that the Removable Media was deemed to be free of malicious code.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

In developing policies in compliance with Requirement R1, the number of policies and their content should be guided by a Responsible Entity's management structure and operating conditions. Policies might be included as part of a general information security program for the entire organization, or as components of specific programs. The Responsible Entity has the flexibility to develop a single comprehensive cyber security policy covering the required topics, or it may choose to develop a single high-level umbrella policy and provide additional policy detail in lower level documents in its documentation hierarchy. In the case of a high-level umbrella policy, the Responsible Entity would be expected to provide the high-level policy as well as the additional documentation in order to demonstrate compliance with CIP-003-8, Requirement R1.

If a Responsible Entity has any high or medium impact BES Cyber Systems, the one or more cyber security policies must cover the nine subject matter areas required by CIP-003-8, Requirement R1, Part 1.1. If a Responsible Entity has identified from CIP-002 any assets containing low impact BES Cyber Systems, the one or more cyber security policies must cover the six subject matter areas required by Requirement R1, Part 1.2.

Responsible Entities that have multiple-impact rated BES Cyber Systems are not required to create separate cyber security policies for high, medium, or low impact BES Cyber Systems. The Responsible Entities have the flexibility to develop policies that cover all three impact ratings.

Implementation of the cyber security policy is not specifically included in CIP-003-8, Requirement R1 as it is envisioned that the implementation of this policy is evidenced through successful implementation of CIP-003 through CIP-011. However, Responsible Entities are encouraged not to limit the scope of their cyber security policies to only those requirements in NERC cyber security Reliability Standards, but to develop a holistic cyber security policy

appropriate for its organization. Elements of a policy that extend beyond the scope of NERC's cyber security Reliability Standards will not be considered candidates for potential violations although they will help demonstrate the organization's internal culture of compliance and posture towards cyber security.

For Part 1.1, the Responsible Entity may consider the following for each of the required topics in its one or more cyber security policies for medium and high impact BES Cyber Systems, if any:

1.1.1 Personnel and training (CIP-004)

- Organization position on acceptable background investigations
- Identification of possible disciplinary action for violating this policy
- Account management

1.1.2 Electronic Security Perimeters (CIP-005) including Interactive Remote Access

- Organization stance on use of wireless networks
- Identification of acceptable authentication methods
- Identification of trusted and untrusted resources
- Monitoring and logging of ingress and egress at Electronic Access Points
- Maintaining up-to-date anti-malware software before initiating Interactive Remote Access
- Maintaining up-to-date patch levels for operating systems and applications used to initiate Interactive Remote Access
- Disabling VPN "split-tunneling" or "dual-homed" workstations before initiating Interactive Remote Access
- For vendors, contractors, or consultants: include language in contracts that requires adherence to the Responsible Entity's Interactive Remote Access controls

1.1.3 Physical security of BES Cyber Systems (CIP-006)

- Strategy for protecting Cyber Assets from unauthorized physical access
- Acceptable physical access control methods
- Monitoring and logging of physical ingress

1.1.4 System security management (CIP-007)

- Strategies for system hardening
- Acceptable methods of authentication and access control
- Password policies including length, complexity, enforcement, prevention of brute force attempts
- Monitoring and logging of BES Cyber Systems

1.1.5 Incident reporting and response planning (CIP-008)

- Recognition of Cyber Security Incidents
- Appropriate notifications upon discovery of an incident
- Obligations to report Cyber Security Incidents

1.1.6 Recovery plans for BES Cyber Systems (CIP-009)

- Availability of spare components
- Availability of system backups

1.1.7 Configuration change management and vulnerability assessments (CIP-010)

- Initiation of change requests
- Approval of changes
- Break-fix processes

1.1.8 Information protection (CIP-011)

- Information access control methods
- Notification of unauthorized information disclosure
- Information access on a need-to-know basis

1.1.9 Declaring and responding to CIP Exceptional Circumstances

- Processes to invoke special procedures in the event of a CIP Exceptional Circumstance
- Processes to allow for exceptions to policy that do not violate CIP requirements

For Part 1.2, the Responsible Entity may consider the following for each of the required topics in its one or more cyber security policies for assets containing low impact BES Cyber Systems, if any:

1.2.1 Cyber security awareness

- Method(s) for delivery of security awareness
- Identification of groups to receive cyber security awareness

1.2.2 Physical security controls

- Acceptable approach(es) for selection of physical security control(s)

1.2.3 Electronic access controls

- Acceptable approach(es) for selection of electronic access control(s)

1.2.4 Cyber Security Incident response

- Recognition of Cyber Security Incidents

- Appropriate notifications upon discovery of an incident
- Obligations to report Cyber Security Incidents

1.2.5 Transient Cyber Assets and Removable Media Malicious Code Risk Mitigation

- Acceptable use of Transient Cyber Asset(s) and Removable Media
- Method(s) to mitigate the risk of the introduction of malicious code to low impact BES Cyber Systems from Transient Cyber Assets and Removable Media
- Method(s) to request Transient Cyber Asset and Removable Media

1.2.6 Declaring and responding to CIP Exceptional Circumstances

- Process(es) to declare a CIP Exceptional Circumstance
- Process(es) to respond to a declared CIP Exceptional Circumstance

Requirements relating to exceptions to a Responsible Entity's security policies were removed because it is a general management issue that is not within the scope of a reliability requirement. It is an internal policy requirement and not a reliability requirement. However, Responsible Entities are encouraged to continue this practice as a component of their cyber security policies.

In this and all subsequent required approvals in the NERC CIP Reliability Standards, the Responsible Entity may elect to use hardcopy or electronic approvals to the extent that there is sufficient evidence to ensure the authenticity of the approving party.

Requirement R2:

The intent of Requirement R2 is for each Responsible Entity to create, document, and implement one or more cyber security plan(s) that address the security objective for the protection of low impact BES Cyber Systems. The required protections are designed to be part of a program that covers the low impact BES Cyber Systems collectively at an asset level (based on the list of assets containing low impact BES Cyber Systems identified in CIP-002), but not at an individual device or system level.

Requirement R2, Attachment 1

As noted, Attachment 1 contains the sections that must be included in the cyber security plan(s). The intent is to allow entities that have a combination of high, medium, and low impact BES Cyber Systems the flexibility to choose, if desired, to cover their low impact BES Cyber Systems (or any subset) under their programs used for the high or medium impact BES Cyber Systems rather than maintain two separate programs. The purpose of the cyber security plan(s) in Requirement R2 is for Responsible Entities to use the cyber security plan(s) as a means of documenting their approaches to meeting the subject matter areas. The cyber security plan(s) can be used to reference other policies and procedures that demonstrate "how" the Responsible Entity is meeting each of the subject matter areas, or Responsible Entities can develop comprehensive cyber security plan(s) that contain all of the detailed implementation content solely within the cyber security plan itself. To meet the obligation for the cyber security plan, the expectation is that the cyber security plan contains or references sufficient details to address the implementation of each of the required subject matters areas.

Guidance for each of the subject matter areas of Attachment 1 is provided below.

Requirement R2, Attachment 1, Section 1 – Cyber Security Awareness

The intent of the cyber security awareness program is for entities to reinforce good cyber security practices with their personnel at least once every 15 calendar months. The entity has the discretion to determine the topics to be addressed and the manner in which it will communicate these topics. As evidence of compliance, the Responsible Entity should be able to produce the awareness material that was delivered according to the delivery method(s) (e.g., posters, emails, or topics at staff meetings, etc.). The standard drafting team does not intend for Responsible Entities to be required to maintain lists of recipients and track the reception of the awareness material by personnel.

Although the focus of the awareness is cyber security, it does not mean that only technology-related topics can be included in the program. Appropriate physical security topics (e.g., tailgating awareness and protection of badges for physical security, or "If you see something, say something" campaigns, etc.) are valid for cyber security awareness. The intent is to cover topics concerning any aspect of the protection of BES Cyber Systems.

Requirement R2, Attachment 1, Section 2 – Physical Security Controls

The Responsible Entity must document and implement methods to control physical access to (1) the asset or the locations of low impact BES Cyber Systems within the asset, and (2) Cyber Assets that implement the electronic access control(s) specified by the Responsible Entity in Attachment 1, Section 3.1, if any. If these Cyber Assets implementing the electronic access controls are located within the same asset as the low impact BES Cyber Asset(s) and inherit the same physical access controls and the same need as outlined in Section 2, this may be noted by the Responsible Entity in either its policies or cyber security plan(s) to avoid duplicate documentation of the same controls.

The Responsible Entity has the flexibility to select the methods used to meet the objective of controlling physical access to (1) the asset(s) containing low impact BES Cyber System(s) or the low impact BES Cyber Systems themselves and (2) the electronic access control Cyber Assets specified by the Responsible Entity, if any. The Responsible Entity may use one or a

combination of physical access controls, monitoring controls, or other operational, procedural, or technical physical security controls. Entities may use perimeter controls (e.g., fences with locked gates, guards, or site access policies, etc.) or more granular areas of physical access control in areas where low impact BES Cyber Systems are located, such as control rooms or control houses.

The security objective is to control the physical access based on need as determined by the Responsible Entity. The need for physical access can be documented at the policy level. The standard drafting team did not intend to obligate an entity to specify a need for each physical access or authorization of an individual for physical access.

Monitoring as a physical security control can be used as a complement or an alternative to physical access control. Examples of monitoring controls include, but are not limited to: (1) alarm systems to detect motion or entry into a controlled area, or (2) human observation of a controlled area. Monitoring does not necessarily require logging and maintaining logs but could include monitoring that physical access has occurred or been attempted (e.g., door alarm, or human observation, etc.). The standard drafting team's intent is that the monitoring does not need to be per low impact BES Cyber System but should be at the appropriate level to meet the security objective of controlling physical access.

User authorization programs and lists of authorized users for physical access are not required although they are an option to meet the security objective.

Requirement R2, Attachment 1, Section 3 – Electronic Access Controls

Section 3 requires the establishment of electronic access controls for assets containing low impact BES Cyber Systems when there is routable protocol communication or Dial-up Connectivity between Cyber Asset(s) outside of the asset containing the low impact BES Cyber System(s) and the low impact BES Cyber System(s) within such asset. The establishment of electronic access controls is intended to reduce the risks associated with uncontrolled communication using routable protocols or Dial-up Connectivity.

When implementing Attachment 1, Section 3.1, Responsible Entities should note that electronic access controls to permit only necessary inbound and outbound electronic access are required for communications when those communications meet all three of the criteria identified in Attachment 1, Section 3.1. The Responsible Entity should evaluate the communications and when all three criteria are met, the Responsible Entity must document and implement electronic access control(s).

When identifying electronic access controls, Responsible Entities are provided flexibility in the selection of the electronic access controls that meet their operational needs while meeting the security objective of allowing only necessary inbound and outbound electronic access to low impact BES Cyber Systems that use routable protocols between a low impact BES Cyber System(s) and Cyber Asset(s) outside the asset.

In essence, the intent is for Responsible Entities to determine whether there is communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s) that uses a routable protocol when entering or leaving the asset or Dial-up Connectivity to the low impact BES Cyber System(s). Where such

communication is present, Responsible Entities should document and implement electronic access control(s). Where routable protocol communication for time-sensitive protection or control functions between intelligent electronic devices that meets the exclusion language is present, Responsible Entities should document that communication, but are not required to establish any specific electronic access controls.

The inputs to this requirement are the assets identified in CIP-002 as containing low impact BES Cyber System(s); therefore, the determination of routable protocol communications or Dial-up Connectivity is an attribute of the asset. However, it is not intended for communication that provides no access to or from the low impact BES Cyber System(s), but happens to be located at the asset with the low impact BES Cyber System(s), to be evaluated for electronic access controls.

Electronic Access Control Exclusion

In order to avoid future technology issues, the obligations for electronic access controls exclude communications between intelligent electronic devices that use routable communication protocols for time-sensitive protection or control functions, such as IEC TR-61850-90-5 R-GOOSE messaging. Time-sensitive in this context generally means functions that would be negatively impacted by the latency introduced in the communications by the required electronic access controls. This time-sensitivity exclusion does not apply to SCADA communications which typically operate on scan rates of 2 seconds or greater. While technically time-sensitive, SCADA communications over routable protocols can withstand the delay introduced by electronic access controls. Examples of excluded time-sensitive communications are those communications which may necessitate the tripping of a breaker within a few cycles. A Responsible Entity using this technology is not expected to implement the electronic access controls noted herein. This exception was included so as not to inhibit the functionality of the time-sensitive characteristics related to this technology and not to preclude the use of such time-sensitive reliability enhancing functions if they use a routable protocol in the future.

Considerations for Determining Routable Protocol Communications

To determine whether electronic access controls need to be implemented, the Responsible Entity has to determine whether there is communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s) that uses a routable protocol when entering or leaving the asset.

When determining whether a routable protocol is entering or leaving the asset containing the low impact BES Cyber System(s), Responsible Entities have flexibility in identifying an approach. One approach is for Responsible Entities to identify an “electronic boundary” associated with the asset containing low impact BES Cyber System(s). This is not an Electronic Security Perimeter *per se*, but a demarcation that demonstrates the routable protocol communication entering or leaving the asset between a low impact BES Cyber System and Cyber Asset(s) outside the asset to then have electronic access controls implemented. This electronic boundary may vary by asset type (Control Center, substation, generation resource) and the specific configuration of the asset. If this approach is used, the intent is for the Responsible Entity to define the electronic boundary such that the low impact BES Cyber System(s) located

at the asset are contained within the "electronic boundary." This is strictly for determining which routable protocol communications and networks are internal or inside or local to the asset and which are external to or outside the asset.

Alternatively, the Responsible Entity may find the concepts of what is inside and outside to be intuitively obvious for a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s) communicating to a low impact BES Cyber System(s) inside the asset. This may be the case when a low impact BES Cyber System(s) is communicating with a Cyber Asset many miles away and a clear and unambiguous demarcation exists. In this case, a Responsible Entity may decide not to identify an "electronic boundary," but rather to simply leverage the unambiguous asset demarcation to ensure that the electronic access controls are placed between the low impact BES Cyber System(s) and the Cyber Asset(s) outside the asset.

Determining Electronic Access Controls

Once a Responsible Entity has determined that there is routable communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s) that uses a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s), the intent is for the Responsible Entity to document and implement its chosen electronic access control(s). The control(s) are intended to allow only "necessary" inbound and outbound electronic access as determined by the Responsible Entity. However the Responsible Entity chooses to document the inbound and outbound access permissions and the need, the intent is that the Responsible Entity is able to explain the reasons for the electronic access permitted. The reasoning for "necessary" inbound and outbound electronic access controls may be documented within the Responsible Entity's cyber security plan(s), within a comment on an access control list, a database, spreadsheet or other policies or procedures associated with the electronic access controls.

Concept Diagrams

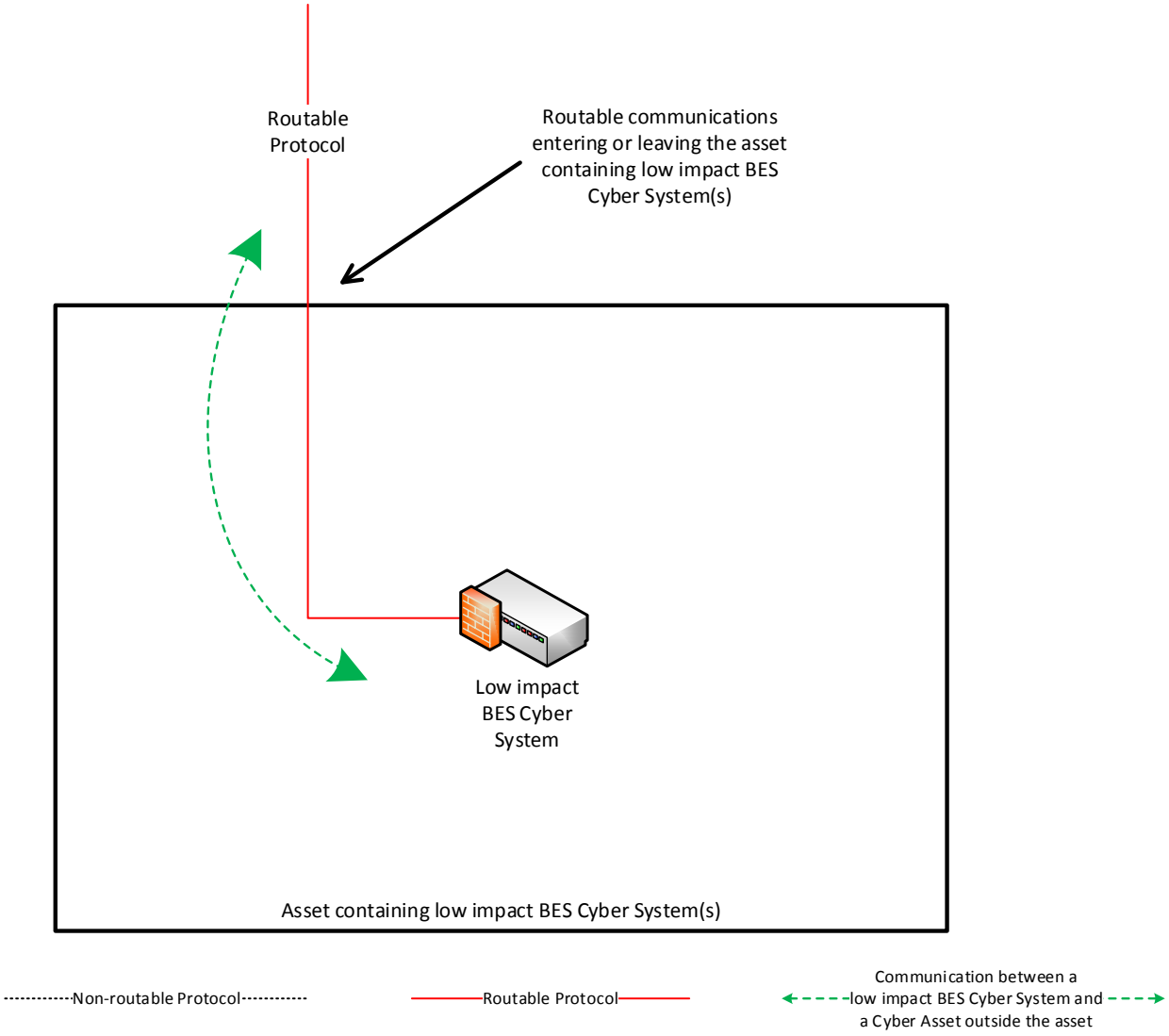
The diagrams on the following pages are provided as examples to illustrate various electronic access controls at a conceptual level. Regardless of the concepts or configurations chosen by the Responsible Entity, the intent is to achieve the security objective of permitting only necessary inbound and outbound electronic access for communication between low impact BES Cyber Systems and Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s) using a routable protocol when entering or leaving the asset.

NOTE:

- This is not an exhaustive list of applicable concepts.
- The same legend is used in each diagram; however, the diagram may not contain all of the articles represented in the legend.

Reference Model 1 – Host-based Inbound & Outbound Access Permissions

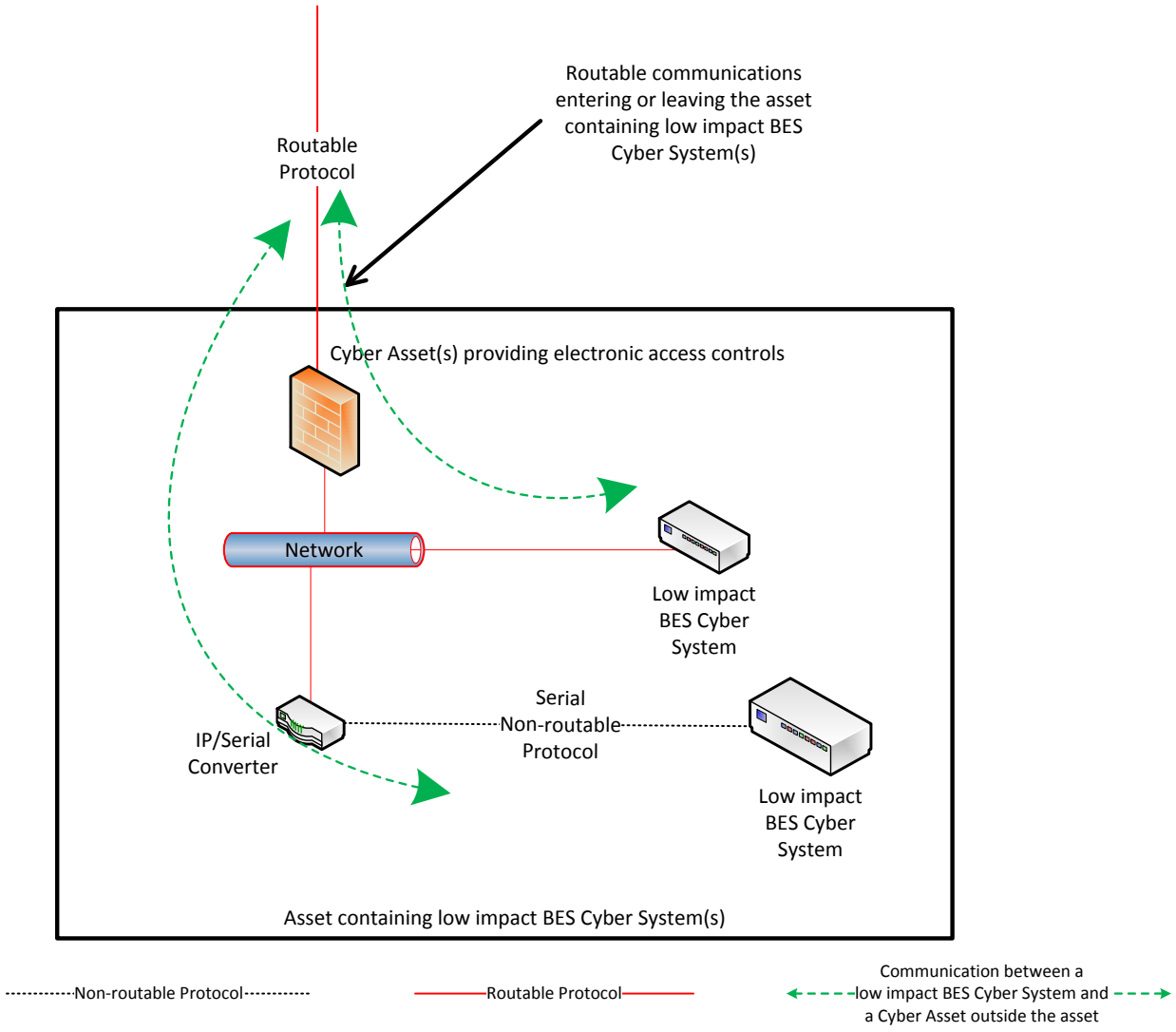
The Responsible Entity may choose to utilize a host-based firewall technology on the low impact BES Cyber System(s) itself that manages the inbound and outbound electronic access permissions so that only necessary inbound and outbound electronic access is allowed between the low impact BES Cyber System(s) and the Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s). When permitting the inbound and outbound electronic access permissions using access control lists, the Responsible Entity could restrict communication(s) using source and destination addresses or ranges of addresses. Responsible Entities could also restrict communication(s) using ports or services based on the capability of the electronic access control, the low impact BES Cyber System(s), or the application(s).



Reference Model 1

Reference Model 2 – Network-based Inbound & Outbound Access Permissions

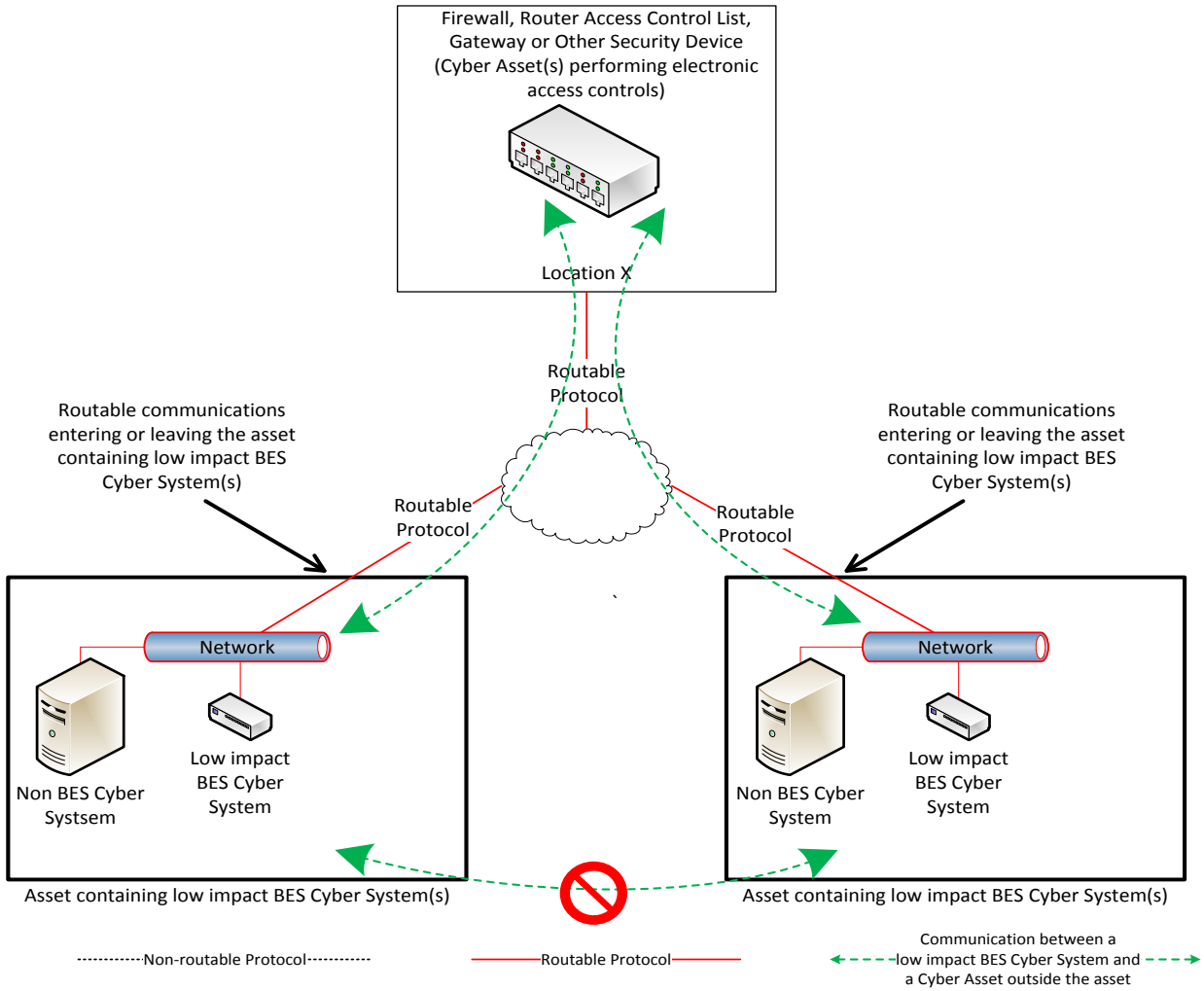
The Responsible Entity may choose to use a security device that permits only necessary inbound and outbound electronic access to the low impact BES Cyber System(s) within the asset containing the low impact BES Cyber System(s). In this example, two low impact BES Cyber Systems are accessed using the routable protocol that is entering or leaving the asset containing the low impact BES Cyber System(s). The IP/Serial converter is continuing the same communications session from the Cyber Asset(s) that are outside the asset to the low impact BES Cyber System(s). The security device provides the electronic access controls to permit only necessary inbound and outbound routable protocol access to the low impact BES Cyber System(s). When permitting the inbound and outbound electronic access permissions using access control lists, the Responsible Entity could restrict communication(s) using source and destination addresses or ranges of addresses. Responsible Entities could also restrict communication(s) using ports or services based on the capability of the electronic access control, the low impact BES Cyber System(s), or the application(s).



Reference Model 2

Reference Model 3 – Centralized Network-based Inbound & Outbound Access Permissions

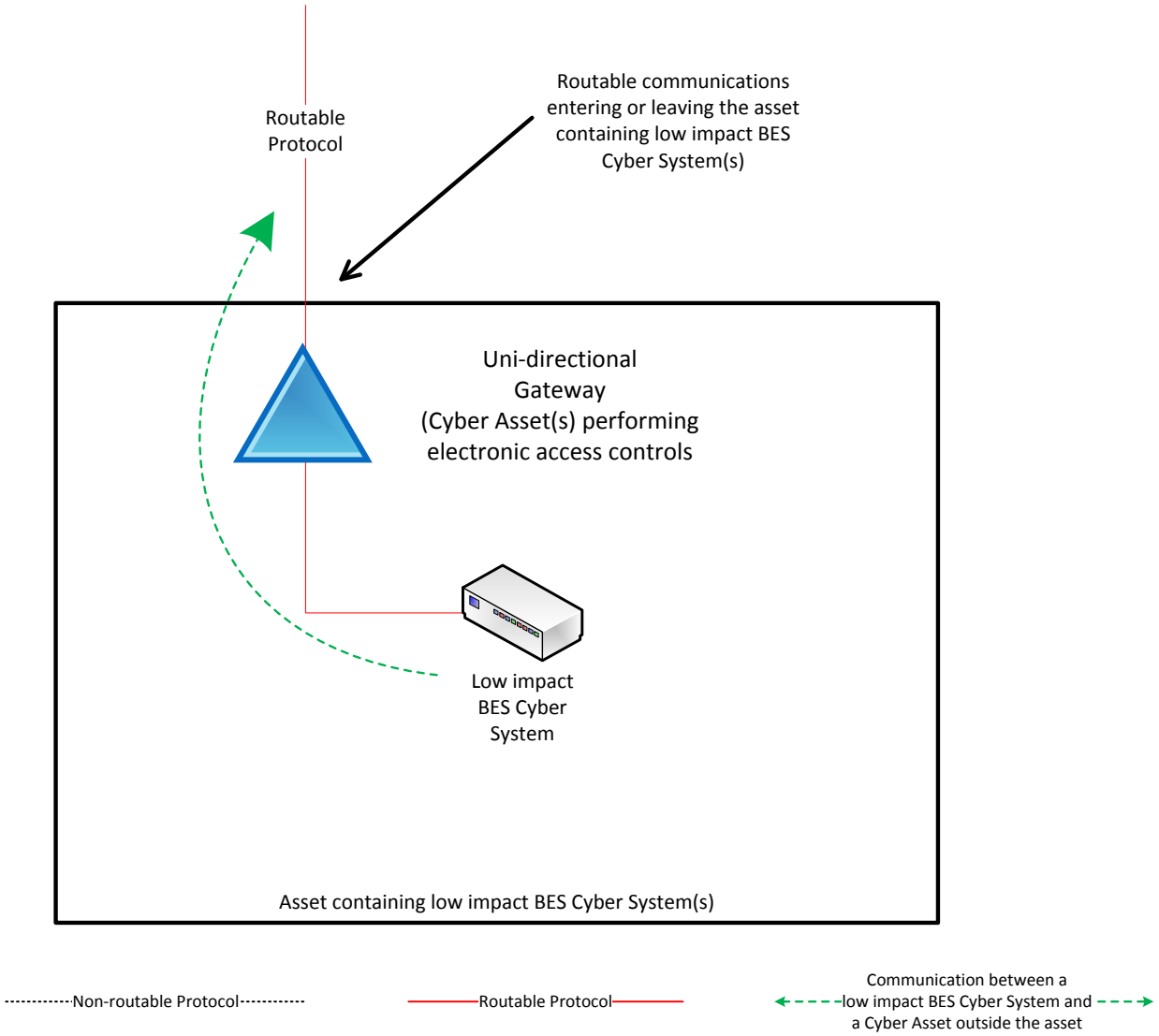
The Responsible Entity may choose to utilize a security device at a centralized location that may or may not be at another asset containing low impact BES Cyber System(s). The electronic access control(s) do not necessarily have to reside inside the asset containing the low impact BES Cyber System(s). A security device is in place at "Location X" to act as the electronic access control and permit only necessary inbound and outbound routable protocol access between the low impact BES Cyber System(s) and the Cyber Asset(s) outside each asset containing low impact BES Cyber System(s). Care should be taken that electronic access to or between each asset is through the Cyber Asset(s) determined by the Responsible Entity to be performing electronic access controls at the centralized location. When permitting the inbound and outbound electronic access permissions using access control lists, the Responsible Entity could restrict communication(s) using source and destination addresses or ranges of addresses. Responsible Entities could also restrict communication(s) using ports or services based on the capability of the electronic access control, the low impact BES Cyber System(s), or the application(s).



Reference Model 3

Reference Model 4 – Uni-directional Gateway

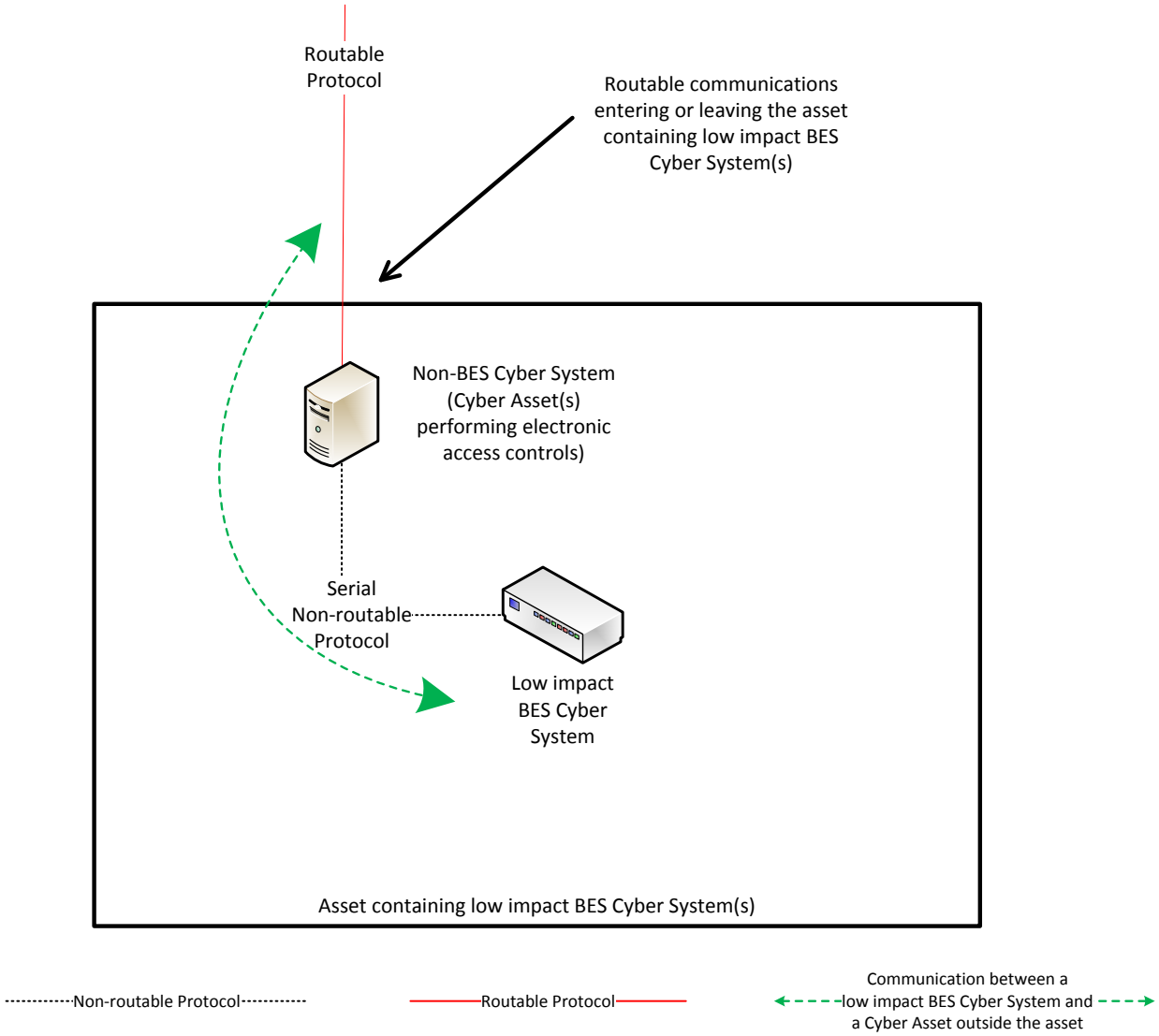
The Responsible Entity may choose to utilize a uni-directional gateway as the electronic access control. The low impact BES Cyber System(s) is not accessible (data cannot flow into the low impact BES Cyber System) using the routable protocol entering the asset due to the implementation of a "one-way" (uni-directional) path for data to flow. The uni-directional gateway is configured to permit only the necessary outbound communications using the routable protocol communication leaving the asset.



Reference Model 4

Reference Model 5 – User Authentication

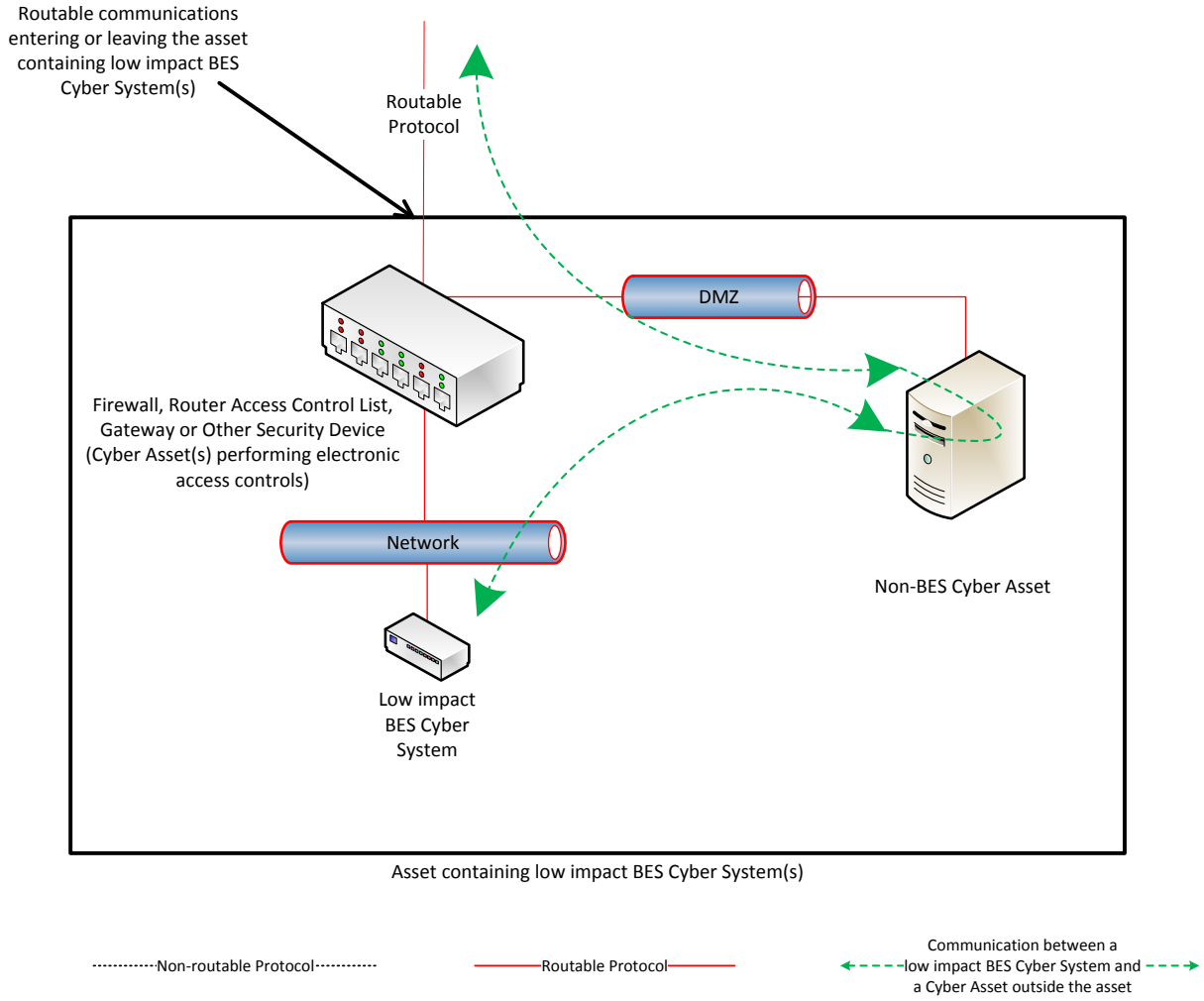
This reference model demonstrates that Responsible Entities have flexibility in choosing electronic access controls so long as the security objective of the requirement is met. The Responsible Entity may choose to utilize a non-BES Cyber Asset located at the asset containing the low impact BES Cyber System that requires authentication for communication from the Cyber Asset(s) outside the asset. This non-BES Cyber System performing the authentication permits only authenticated communication to connect to the low impact BES Cyber System(s), meeting the first half of the security objective to permit only necessary inbound electronic access. Additionally, the non-BES Cyber System performing authentication is configured such that it permits only necessary outbound communication meeting the second half of the security objective. Often, the outbound communications would be controlled in this network architecture by permitting no communication to be initiated from the low impact BES Cyber System. This configuration may be beneficial when the only communication to a device is for user-initiated interactive access.



Reference Model 5

Reference Model 6 – Indirect Access

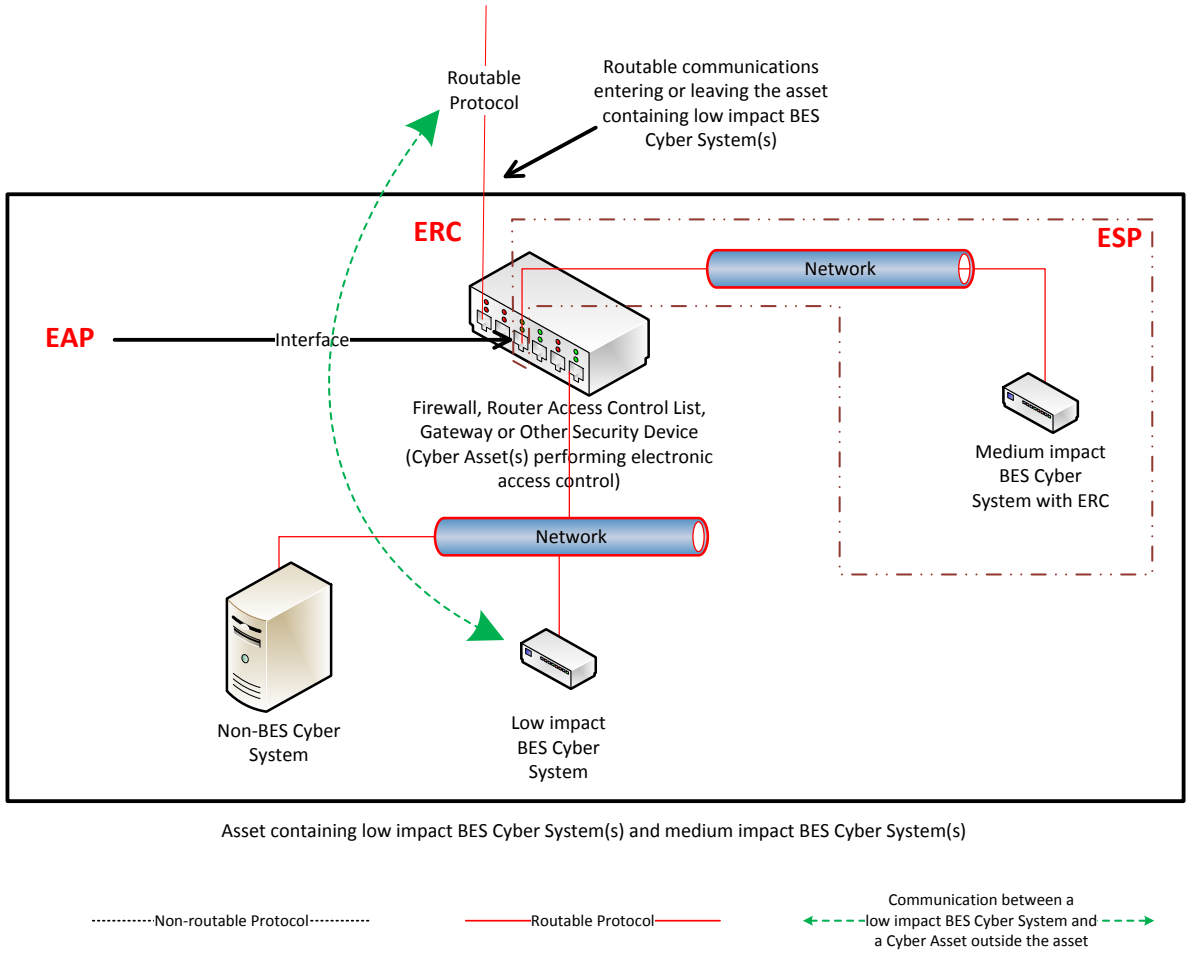
In implementing its electronic access controls, the Responsible Entity may identify that it has indirect access between the low impact BES Cyber System and a Cyber Asset outside the asset containing the low impact BES Cyber System through a non-BES Cyber Asset located within the asset. This indirect access meets the criteria of having communication between the low impact BES Cyber System and a Cyber Asset outside the asset containing the low impact BES Cyber System. In this reference model, it is intended that the Responsible Entity implement electronic access controls that permit only necessary inbound and outbound electronic access to the low impact BES Cyber System. Consistent with the other reference models provided, the electronic access in this reference model is controlled using the security device that is restricting the communication that is entering or leaving the asset.



Reference Model 6

Reference Model 7 – Electronic Access Controls at assets containing low impact BES Cyber Systems and ERC

In this reference model, there is both a routable protocol entering and leaving the asset containing the low impact BES Cyber System(s) that is used by Cyber Asset(s) outside the asset and External Routable Connectivity because there is at least one medium impact BES Cyber System and one low impact BES Cyber System within the asset using the routable protocol communications. The Responsible Entity may choose to leverage an interface on the medium impact Electronic Access Control or Monitoring Systems (EACMS) to provide electronic access controls for purposes of CIP-003. The EACMS is therefore performing multiple functions – as a medium impact EACMS and as implementing electronic access controls for an asset containing low impact BES Cyber Systems.

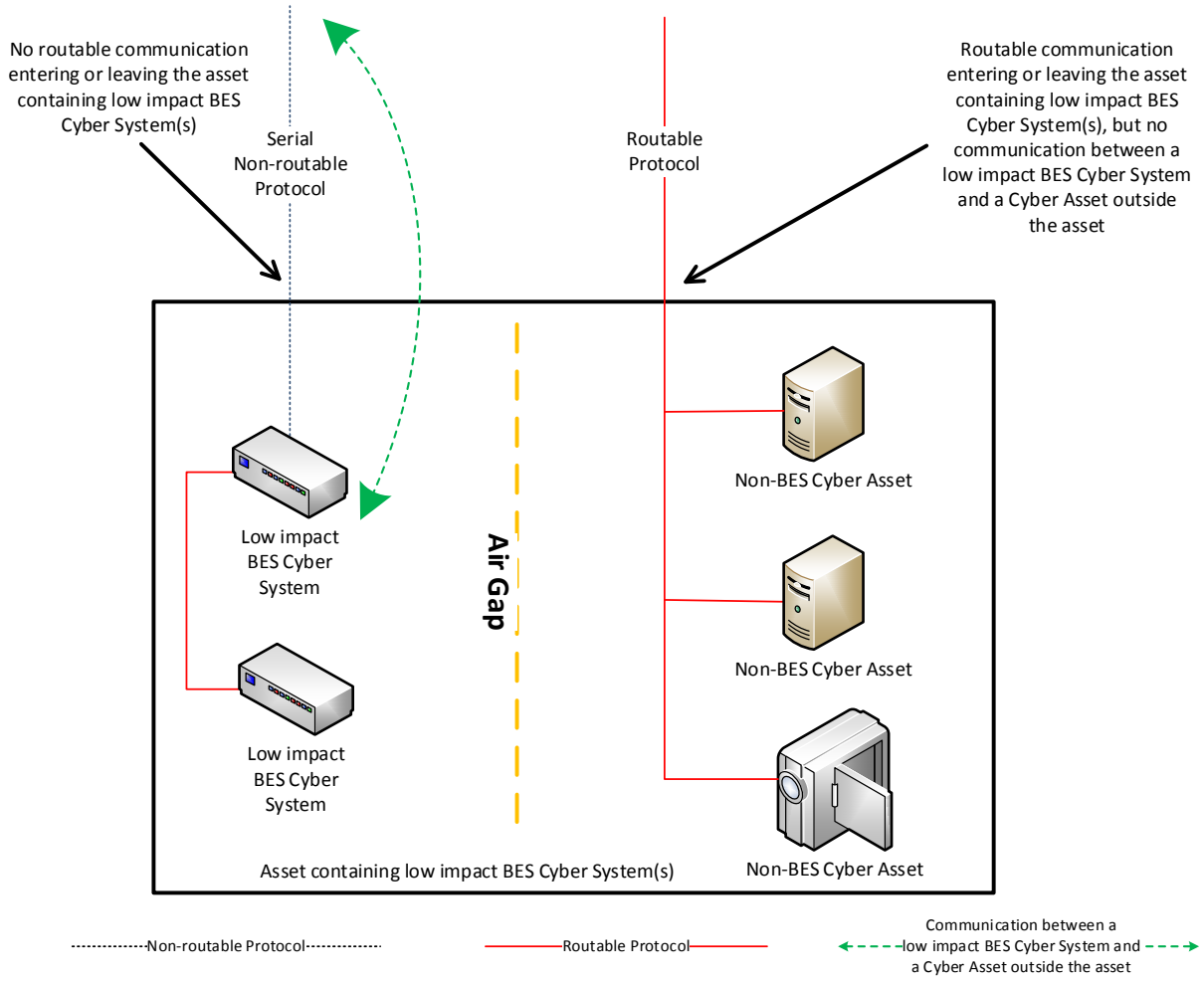


Reference Model 7

Reference Model 8 – Physical Isolation and Serial Non-routable Communications – No Electronic Access Controls Required

In this reference model, the criteria from Attachment 1, Section 3.1 requiring the implementation of electronic access controls are not met. This reference model demonstrates three concepts:

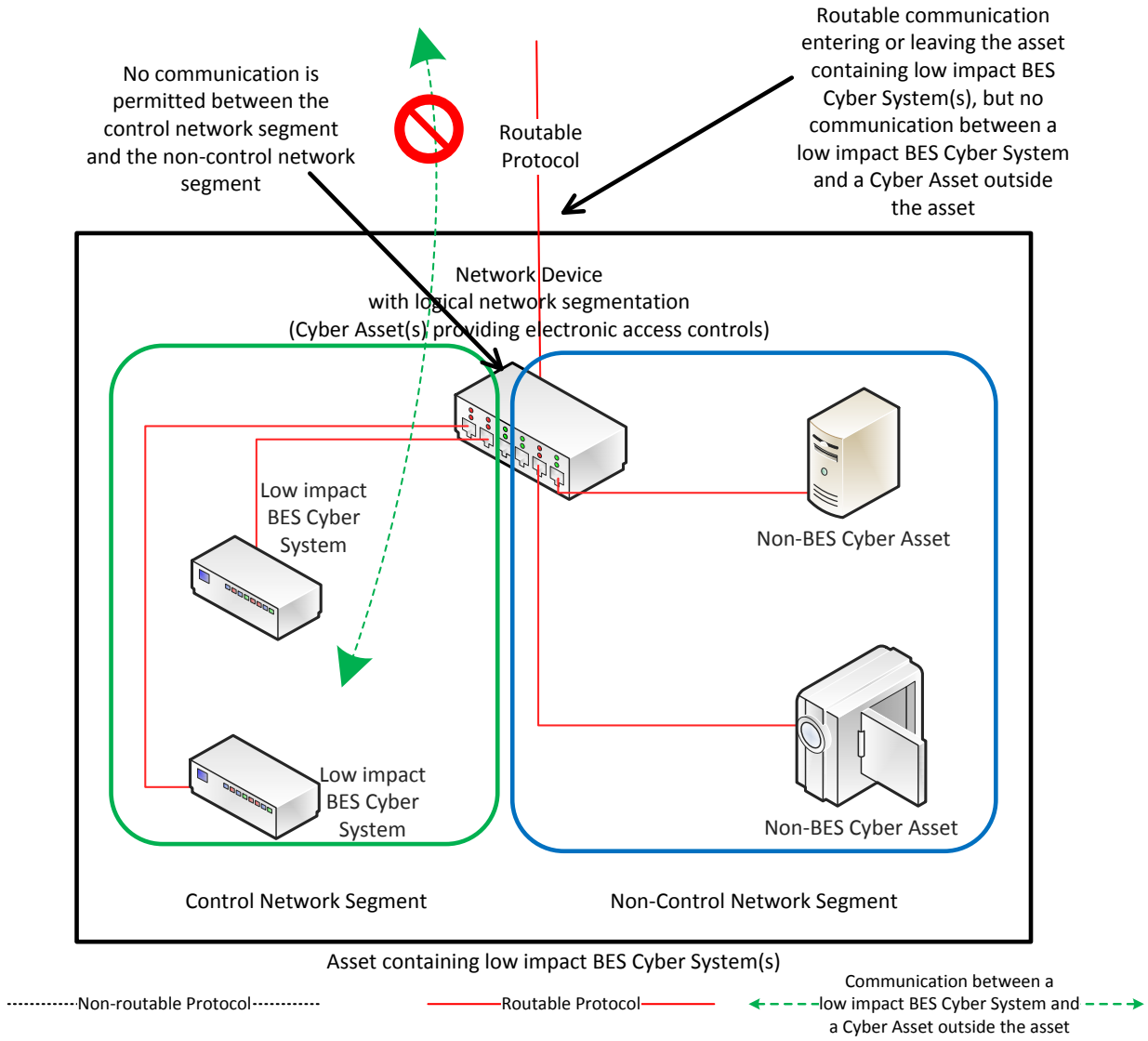
1) The physical isolation of the low impact BES Cyber System(s) from the routable protocol communication entering or leaving the asset containing the low impact BES Cyber System(s), commonly referred to as an 'air gap', mitigates the need to implement the required electronic access controls;
2) The communication to the low impact BES Cyber System from a Cyber Asset outside the asset containing the low impact BES Cyber System(s) using only a serial non-routable protocol where such communication is entering or leaving the asset mitigates the need to implement the required electronic access controls.
3) The routable protocol communication between the low impact BES Cyber System(s) and other Cyber Asset(s), such as the second low impact BES Cyber System depicted, may exist without needing to implement the required electronic access controls so long as the routable protocol communications never leaves the asset containing the low impact BES Cyber System(s).



Reference Model 8

Reference Model 9 – Logical Isolation - No Electronic Access Controls Required

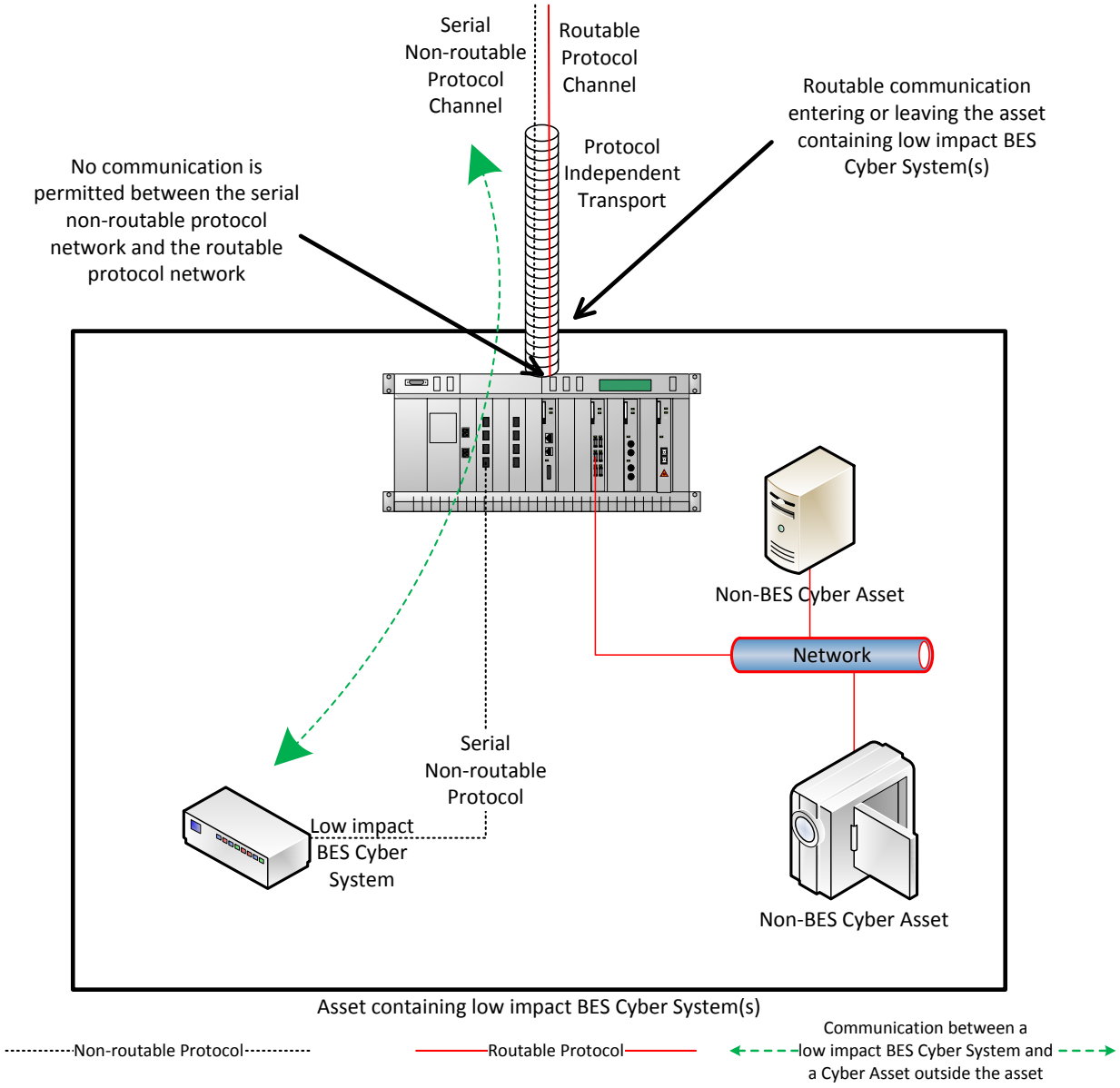
In this reference model, the criteria from Attachment 1, Section 3.1 requiring the implementation of electronic access controls are not met. The Responsible Entity has logically isolated the low impact BES Cyber System(s) from the routable protocol communication entering or leaving the asset containing low impact BES Cyber System(s). The logical network segmentation in this reference model permits no communication between a low impact BES Cyber System and a Cyber Asset outside the asset. Additionally, no indirect access exists because those non-BES Cyber Assets that are able to communicate outside the asset are strictly prohibited from communicating to the low impact BES Cyber System(s). The low impact BES Cyber System(s) is on an isolated network segment with logical controls preventing routable protocol communication into or out of the network containing the low impact BES Cyber System(s) and these communications never leave the asset using a routable protocol.



Reference Model 9

Reference Model 10 - Serial Non-routable Communications Traversing an Isolated Channel on a Non-routable Transport Network – No Electronic Access Controls Required

In this reference model, the criteria from Attachment 1, Section 3.1 requiring the implementation of electronic access controls are not met. This reference model depicts communication between a low impact BES Cyber System and a Cyber Asset outside the asset containing the low impact BES Cyber System over a serial non-routable protocol which is transported across a wide-area network using a protocol independent transport that may carry routable and non-routable communication such as a Time-Division Multiplexing (TDM) network, a Synchronous Optical Network (SONET), or a Multiprotocol Label Switching (MPLS) network. While there is routable protocol communication entering or leaving the asset containing low impact BES Cyber Systems(s) and there is communication between a low impact BES Cyber System and a Cyber Asset outside the asset, the communication between the low impact BES Cyber System and the Cyber Asset outside the asset is not using the routable protocol communication. This model is related to Reference Model 9 in that it relies on logical isolation to prohibit the communication between a low impact BES Cyber System and a Cyber Asset outside the asset from using a routable protocol.



Reference Model 10

Dial-up Connectivity

Dial-up Connectivity to a low impact BES Cyber System is set to dial out only (no auto-answer) to a preprogrammed number to deliver data. Incoming Dial-up Connectivity is to a dialback modem, a modem that must be remotely controlled by the control center or control room, has some form of access control, or the low impact BES Cyber System has access control.

Insufficient Access Controls

Some examples of situations that would lack sufficient access controls to meet the intent of this requirement include:

- An asset has Dial-up Connectivity and a low impact BES Cyber System is reachable via an auto-answer modem that connects any caller to the Cyber Asset that has a default password. There is no practical access control in this instance.
- A low impact BES Cyber System has a wireless card on a public carrier that allows the BES Cyber System to be reachable via a public IP address. In essence, low impact BES Cyber Systems should not be accessible from the Internet and search engines such as Shodan.
- Dual-homing or multiple-network interface cards without disabling IP forwarding in the non-BES Cyber Asset within the DMZ to provide separation between the low impact BES Cyber System(s) and the external network would not meet the intent of "controlling" inbound and outbound electronic access assuming there was no other host-based firewall or other security devices on the non-BES Cyber Asset.

Requirement R2, Attachment 1, Section 4 – Cyber Security Incident Response

The entity should have one or more documented Cyber Security Incident response plan(s) that include each of the topics listed in Section 4. If, in the normal course of business, suspicious activities are noted at an asset containing low impact BES Cyber System(s), the intent is for the entity to implement a Cyber Security Incident response plan that will guide the entity in responding to the incident and reporting the incident if it rises to the level of a Reportable Cyber Security Incident.

Entities are provided the flexibility to develop their Attachment 1, Section 4 Cyber Security Incident response plan(s) by asset or group of assets. The plans do not need to be on a per asset site or per low impact BES Cyber System basis. Entities can choose to use a single enterprise-wide plan to fulfill the obligations for low impact BES Cyber Systems.

The plan(s) must be tested once every 36 months. This is not an exercise per low impact BES Cyber Asset or per type of BES Cyber Asset but rather is an exercise of each incident response plan the entity created to meet this requirement. An actual Reportable Cyber Security Incident counts as an exercise as do other forms of tabletop exercises or drills. NERC-led exercises such as GridEx participation would also count as an exercise provided the entity's response plan is followed. The intent of the requirement is for entities to keep the Cyber Security Incident response plan(s) current, which includes updating the plan(s), if needed, within 180 days following a test or an actual incident.

For low impact BES Cyber Systems, the only portion of the definition of Cyber Security Incident that would apply is, "A malicious act or suspicious event that disrupts, or was an attempt to

disrupt, the operation of a BES Cyber System." The other portion of that definition is not to be used to require ESPs and PSPs for low impact BES Cyber Systems.

Requirement R2, Attachment 1, Section 5 – Transient Cyber Assets and Removable Media Malicious Code Risk Mitigation

Most BES Cyber Assets and BES Cyber Systems are isolated from external public or untrusted networks, and therefore Transient Cyber Assets and Removable Media are needed to transport files to and from secure areas to maintain, monitor, or troubleshoot critical systems. Transient Cyber Assets and Removable Media are a potential means for cyber-attack. To protect the BES Cyber Assets and BES Cyber Systems, CIP-003 Requirement R2, Attachment 1, Section 5 requires Responsible Entities to document and implement a plan for how they will mitigate the risk of malicious code introduction to low impact BES Cyber Systems from Transient Cyber Assets and Removable Media. The approach of defining a plan allows the Responsible Entity to document processes that are supportable within its organization and in alignment with its change management processes.

Transient Cyber Assets can be one of many types of devices from a specially-designed device for maintaining equipment in support of the BES to a platform such as a laptop, desktop, or tablet that may interface with or run applications that support BES Cyber Systems and is capable of transmitting executable code to the BES Cyber Asset(s) or BES Cyber System(s). Note: Cyber Assets connected to a BES Cyber System for less than 30 days due to an unplanned removal, such as premature failure, are not intended to be identified as Transient Cyber Assets. Removable Media subject to this requirement include, among others, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.

Examples of these temporarily connected devices include, but are not limited to:

- Diagnostic test equipment;
- Equipment used for BES Cyber System maintenance; or
- Equipment used for BES Cyber System configuration.

To meet the objective of mitigating risks associated with the introduction of malicious code at low impact BES Cyber Systems, Section 5 specifies the capabilities and possible security methods available to Responsible Entities based upon asset type and ownership.

With the list of options provided in Attachment 1, the entity has the discretion to use the option(s) that is most appropriate. This includes documenting its approach for how and when the entity reviews the Transient Cyber Asset under its control or under the control of parties other than the Responsible Entity. The entity should avoid implementing a security function that jeopardizes reliability by taking actions that would negatively impact the performance or support of the Transient Cyber Asset or BES Cyber Asset.

Malicious Code Risk Mitigation

The terms “mitigate”, “mitigating”, and “mitigation” are used in Section 5 in Attachment 1 to address the risks posed by malicious code when connecting Transient Cyber Assets and Removable Media to BES Cyber Systems. Mitigation is intended to mean that entities reduce security risks presented by connecting the Transient Cyber Asset or Removable Media. When determining the method(s) to mitigate the introduction of malicious code, it is not intended for entities to perform and document a formal risk assessment associated with the introduction of malicious code.

Per Transient Cyber Asset Capability

As with other CIP standards, the requirements are intended for an entity to use the method(s) that the system is capable of performing. The use of “per Transient Cyber Asset capability” is to eliminate the need for a Technical Feasibility Exception when it is understood that the device cannot use a method(s). For example, for malicious code, many types of appliances are not capable of implementing antivirus software; therefore, because it is not a capability of those types of devices, implementation of the antivirus software would not be required for those devices.

Requirement R2, Attachment 1, Section 5.1 - Transient Cyber Asset(s) Managed by the Responsible Entity

For Transient Cyber Assets and Removable Media that are connected to both low impact and medium/high impact BES Cyber Systems, entities must be aware of the differing levels of requirements and manage these assets under the program that matches the highest impact level to which they will connect.

Section 5.1: Entities are to document and implement their plan(s) to mitigate malicious code through the use of one or more of the protective measures listed, based on the capability of the Transient Cyber Asset.

The Responsible Entity has the flexibility to apply the selected method(s) to meet the objective of mitigating the introductions of malicious code either in an on-going or in an on-demand manner. An example of managing a device in an on-going manner is having the antivirus solution for the device managed as part of an end-point security solution with current signature or pattern updates, regularly scheduled systems scans, etc. In contrast, for devices that are used infrequently and the signatures or patterns are not kept current, the entity may manage those devices in an on-demand manner by requiring an update to the signatures or patterns and a scan of the device before the device is connected to ensure that it is free of malicious code.

Selecting management in an on-going or on-demand manner is not intended to imply that the control has to be verified at every single connection. For example, if the device is managed in an on-demand manner, but will be used to perform maintenance on several BES Cyber Asset(s), the Responsible Entity may choose to document that the Transient Cyber Asset has been updated before being connected as a Transient Cyber Asset for the first use of that maintenance work. The intent is not to require a log documenting each connection of a Transient Cyber Asset to a BES Cyber Asset.

The following is additional discussion of the methods to mitigate the introduction of malicious code.

- Antivirus software, including manual or managed updates of signatures or patterns, provides flexibility to manage Transient Cyber Asset(s) by deploying antivirus or endpoint security tools that maintain a scheduled update of the signatures or patterns. Also, for devices that do not regularly connect to receive scheduled updates, entities may choose to update the signatures or patterns and scan the Transient Cyber Asset prior to connection to ensure no malicious software is present.
- Application whitelisting is a method of authorizing only the applications and processes that are necessary on the Transient Cyber Asset. This reduces the risk that malicious software could execute on the Transient Cyber Asset and impact the BES Cyber Asset or BES Cyber System.
- When using methods other than those listed, entities need to document how the other method(s) meet the objective of mitigating the risk of the introduction of malicious code.

If malicious code is discovered on the Transient Cyber Asset, it must be mitigated prior to connection to a BES Cyber System to prevent the malicious code from being introduced into the BES Cyber System. An entity may choose to not connect the Transient Cyber Asset to a BES Cyber System to prevent the malicious code from being introduced into the BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber Security Incident.

Requirement R2, Attachment 1, Section 5.2 - Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity

Section 5 also recognizes the lack of direct control over Transient Cyber Assets that are managed by parties other than the Responsible Entity. This lack of control, however, does not obviate the Responsible Entity's responsibility to ensure that methods have been deployed to mitigate the introduction of malicious code to low impact BES Cyber System(s) from Transient Cyber Assets it does not manage. Section 5 requires entities to review the other party's security practices with respect to Transient Cyber Assets to help meet the objective of the requirement. The use of "prior to connecting the Transient Cyber Assets" is intended to ensure that the Responsible Entity conducts the review before the first connection of the Transient Cyber Asset to help meet the objective to mitigate the introduction of malicious code. The SDT does not intend for the Responsible Entity to conduct a review for every single connection of that Transient Cyber Asset once the Responsible Entity has established the Transient Cyber Asset is meeting the security objective. The intent is to not require a log documenting each connection of a Transient Cyber Asset to a BES Cyber Asset.

To facilitate these controls, Responsible Entities may execute agreements with other parties to provide support services to BES Cyber Systems and BES Cyber Assets that may involve the use of Transient Cyber Assets. Entities may consider using the Department of Energy Cybersecurity Procurement Language for Energy Delivery dated April 2014.[1] Procurement language may unify

[1] http://www.energy.gov/oe/downloads/cybersecurity-procurement-language-energy-delivery-april-2014

the other party and entity actions supporting the BES Cyber Systems and BES Cyber Assets. CIP program attributes may be considered including roles and responsibilities, access controls, monitoring, logging, vulnerability, and patch management along with incident response and back up recovery may be part of the other party's support. Entities may consider the "General Cybersecurity Procurement Language" and "The Supplier's Life Cycle Security Program" when drafting Master Service Agreements, Contracts, and the CIP program processes and controls.

Section 5.2.1: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more of the protective measures listed.

- Review the use of antivirus software and signature or pattern levels to ensure that the level is adequate to the Responsible Entity to mitigate the risk of malicious software being introduced to an applicable system.
- Review the antivirus or endpoint security processes of the other party to ensure that their processes are adequate to the Responsible Entity to mitigate the risk of introducing malicious software to an applicable system.
- Review the use of application whitelisting used by the other party to mitigate the risk of introducing malicious software to an applicable system.
- Review the use of live operating systems or software executable only from read-only media to ensure that the media is free from malicious software itself. Entities should review the processes to build the read-only media as well as the media itself.
- Review system hardening practices used by the other party to ensure that unnecessary ports, services, applications, etc. have been disabled or removed. This method intends to reduce the attack surface on the Transient Cyber Asset and reduce the avenues by which malicious software could be introduced.

Section 5.2.2: The intent of this section is to ensure that after conducting the selected review from Section 5.2.1, if there are deficiencies identified, actions mitigating the risk of the introduction of malicious code to low impact BES Cyber Systems must be completed prior to connecting the device(s) to an applicable system.

Requirement R2, Attachment 1, Section 5.3 - Removable Media

Entities have a high level of control for Removable Media that are going to be connected to their BES Cyber Assets.

Section 5.3: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more method(s) to detect malicious code on the Removable Media before it is connected to a BES Cyber Asset. When using the method(s) to detect malicious code, it is expected to occur from a system that is not part of the BES Cyber System to reduce the risk of propagating malicious code into the BES Cyber System

network or onto one of the BES Cyber Assets. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber Security Incident. Frequency and timing of the methods used to detect malicious code were intentionally excluded from the requirement because there are multiple timing scenarios that can be incorporated into a plan to mitigate the risk of malicious code. The SDT does not intend to obligate a Responsible Entity to conduct a review for every single connection of Removable Media, but rather to implement its plan(s) in a manner that protects all BES Cyber Systems where Removable Media may be used. The intent is to not require a log documenting each connection of Removable Media to a BES Cyber Asset.

As a method to detect malicious code, entities may choose to use Removable Media with on-board malicious code detection tools. For these tools, the Removable Media are still used in conjunction with a Cyber Asset to perform the detection. For Section 5.3.1, the Cyber Asset used to perform the malicious code detection must be outside of the BES Cyber System.

Requirement R3:

The intent of CIP-003-8, Requirement R3 is effectively unchanged since prior versions of the standard. The specific description of the CIP Senior Manager has now been included as a defined term rather than clarified in the Reliability Standard itself to prevent any unnecessary cross-reference to this standard. It is expected that the CIP Senior Manager will play a key role in ensuring proper strategic planning, executive/board-level awareness, and overall program governance.

Requirement R4:

As indicated in the rationale for CIP-003-8, Requirement R4, this requirement is intended to demonstrate a clear line of authority and ownership for security matters. The intent of the SDT was not to impose any particular organizational structure, but, rather, the intent is to afford the Responsible Entity significant flexibility to adapt this requirement to its existing organizational structure. A Responsible Entity may satisfy this requirement through a single delegation document or through multiple delegation documents. The Responsible Entity can make use of the delegation of the delegation authority itself to increase the flexibility in how this applies to its organization. In such a case, delegations may exist in numerous documentation records as long as the collection of these documentation records shows a clear line of authority back to the CIP Senior Manager. In addition, the CIP Senior Manager could also choose not to delegate any authority and meet this requirement without such delegation documentation.

The Responsible Entity must keep its documentation of the CIP Senior Manager and any delegations up-to-date. This is to ensure that individuals do not assume any undocumented authority. However, delegations do not have to be re-instated if the individual who delegated the task changes roles or the individual is replaced. For instance, assume that John Doe is named the CIP Senior Manager and he delegates a specific task to the Substation Maintenance Manager. If John Doe is replaced as the CIP Senior Manager, the CIP Senior Manager documentation must be updated within the specified timeframe, but the existing delegation to

the Substation Maintenance Manager remains in effect as approved by the previous CIP Senior Manager, John Doe.

Rationale:

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for Requirement R1:

One or more security policies enable effective implementation of the requirements of the cyber security Reliability Standards. The purpose of policies is to provide a management and governance foundation for all requirements that apply to a Responsible Entity's BES Cyber Systems. The Responsible Entity can demonstrate through its policies that its management supports the accountability and responsibility necessary for effective implementation of the requirements.

Annual review and approval of the cyber security policies ensures that the policies are kept-up-to-date and periodically reaffirms management's commitment to the protection of its BES Cyber Systems.

Rationale for Requirement R2:

In response to FERC Order No. 791, Requirement R2 requires entities to develop and implement cyber security plans to meet specific security control objectives for assets containing low impact BES Cyber System(s). The cyber security plan(s) covers five subject matter areas: (1) cyber security awareness; (2) physical security controls; (3) electronic access controls; (4) Cyber Security Incident response; and (5) Transient Cyber Asset and Removable Media Malicious Code Risk Mitigation. This plan(s), along with the cyber security policies required under Requirement R1, Part 1.2, provides a framework for operational, procedural, and technical safeguards for low impact BES Cyber Systems.

Considering the varied types of low impact BES Cyber Systems across the BES, Attachment 1 provides Responsible Entities flexibility on how to apply the security controls to meet the security objectives. Additionally, because many Responsible Entities have multiple-impact rated BES Cyber Systems, nothing in the requirement prohibits entities from using their high and medium impact BES Cyber System policies, procedures, and processes to implement security controls required for low impact BES Cyber Systems, as detailed in Requirement R2, Attachment 1.

Responsible Entities will use their identified assets containing low impact BES Cyber System(s) (developed pursuant to CIP-002) to substantiate the sites or locations associated with low impact BES Cyber System(s). However, there is no requirement or compliance expectation for Responsible Entities to maintain a list(s) of individual low impact BES Cyber System(s) and their associated cyber assets or to maintain a list of authorized users.

Rationale for Modifications to Sections 2 and 3 of Attachment 1 (Requirement R2):

Requirement R2 mandates that entities develop and implement one or more cyber security plan(s) to meet specific security objectives for assets containing low impact BES Cyber System(s). In Paragraph 73 of FERC Order No. 822, the Commission directed NERC to modify "…the Low Impact External Routable Connectivity definition to reflect the commentary in the Guidelines and Technical Basis section of CIP-003-6…to provide needed clarity to the definition

and eliminate ambiguity surrounding the term 'direct' as it is used in the proposed definition…within one year of the effective date of this Final Rule."

The revisions to Section 3 incorporate select language from the LERC definition into Attachment 1 and focus the requirement on implementing electronic access controls for asset(s) containing low impact BES Cyber System(s). This change requires the Responsible Entity to permit only necessary inbound and outbound electronic access when using a routable protocol entering or leaving the asset between low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber system(s). When this communication is present, Responsible Entities are required to implement electronic access controls unless that communication meets the following exclusion language (previously in the definition of LERC) contained in romanette (iii): "not used for time-sensitive protection or control functions between intelligent electronic devices (e.g. communications using protocol IEC TR-61850-90-5 R-GOOSE)".

The revisions to Section 2 of Attachment 1 complement the revisions to Section 3; consequently, the requirement now mandates the Responsible Entity control physical access to "the Cyber Asset(s), as specified by the Responsible Entity, that provide electronic access control(s) implemented for Section 3.1, if any." The focus on electronic access controls rather than on the Low Impact BES Cyber System Electronic Access Points (LEAPs) eliminates the need for LEAPs.

Given these revisions to Sections 2 and 3, the NERC Glossary terms: Low Impact External Routable Connectivity (LERC) and Low Impact BES Cyber System Electronic Access Point (LEAP) will be retired.

Rationale for Section 5 of Attachment 1 (Requirement R2):
Requirement R2 mandates that entities develop and implement one or more cyber security plan(s) to meet specific security objectives for assets containing low impact BES Cyber System(s). In Paragraph 32 of FERC Order No. 822, the Commission directed NERC to "…provide mandatory protection for transient devices used at Low Impact BES Cyber Systems based on the risk posed to bulk electric system reliability." Transient devices are potential vehicles for introducing malicious code into low impact BES Cyber Systems. Section 5 of Attachment 1 is intended to mitigate the risk of malware propagation to the BES through low impact BES Cyber Systems by requiring entities to develop and implement one or more plan(s) to address the risk. The cyber security plan(s) along with the cyber security policies required under Requirement R1, Part 1.2, provide a framework for operational, procedural, and technical safeguards for low impact BES Cyber Systems.

Rationale for Requirement R3:

The identification and documentation of the single CIP Senior Manager ensures that there is clear authority and ownership for the CIP program within an organization, as called for in Blackout Report Recommendation 43. The language that identifies CIP Senior Manager responsibilities is included in the Glossary of Terms used in NERC Reliability Standards so that it may be used across the body of CIP standards without an explicit cross-reference.

FERC Order No. 706, Paragraph 296, requests consideration of whether the single senior manager should be a corporate officer or equivalent. As implicated through the defined term, the senior manager has "the overall authority and responsibility for leading and managing implementation of the requirements within this set of standards" which ensures that the senior manager is of sufficient position in the Responsible Entity to ensure that cyber security receives the prominence that is necessary. In addition, given the range of business models for responsible entities, from municipal, cooperative, federal agencies, investor owned utilities, privately owned utilities, and everything in between, the SDT believes that requiring the CIP Senior Manager to be a "corporate officer or equivalent" would be extremely difficult to interpret and enforce on a consistent basis.

Rationale for Requirement R4:

The intent of the requirement is to ensure clear accountability within an organization for certain security matters. It also ensures that delegations are kept up-to-date and that individuals do not assume undocumented authority.

In FERC Order No. 706, Paragraphs 379 and 381, the Commission notes that Recommendation 43 of the 2003 Blackout Report calls for "clear lines of authority and ownership for security matters." With this in mind, the Standard Drafting Team has sought to provide clarity in the requirement for delegations so that this line of authority is clear and apparent from the documented delegations.

Appendix CIP-003-8-QC-1

Specific provisions applicable in Québec for standard
CIP-003-8 – Cyber Security – Security Management Controls

This appendix establishes specific provisions for the application of the standard in Québec. Provisions of the standard and of this appendix must be read jointly for comprehension and interpretation purposes. Where the standard and appendix differ, the appendix shall prevail.

A. Introduction

1. **Title:** No specific provisions.

2. **Number:** No specific provisions.

3. **Purpose:** No specific provisions.

4. **Applicability:**

4.1. Functional entities

No specific provisions.

4.2. Facilities

This standard applies only to main transmission system (RTP) facilities and designated Distribution Provider facilities. When applying this standard, any reference to the terms 'Bulk Electric System' or 'BES' shall be replaced by the terms 'main transmission system' or 'RTP', respectively.

Additional exemptions

The following are exempt from this standard:

- Generation facilities meeting the following conditions: (1) the rated power of the facility is equal to or less than 300 MVA and (2) none of the generation units at the facility can be synchronized with a neighbouring system.
- Step-up substations for the above-mentioned generating facilities.

5. **Effective dates for Quebec:**

5.1. Adoption of the standard by the Régie de l'énergie: September 10, 2020

5.2. Adoption of the appendix by the Régie de l'énergie: September 10, 2020

5.3. Effective date of the standard and attachment for Québec: October 1, 2021

6. **Background:** No specific provisions.

B. Requirements and measures

No specific provisions.

C. Compliance

1. **Compliance Monitoring Process**

1.1. Compliance Enforcement Authority

In Québec, "Compliance Enforcement Authority" means the Régie de l'énergie in its roles of monitoring and enforcing compliance with respect to the Reliability

Standard and to this appendix.

1.2. Evidence Retention

No specific provisions.

1.3. Compliance Monitoring and Assessment Processes

The Régie de l'énergie establishes the monitoring processes used to evaluate data or information for the purpose of determining compliance or non-compliance with the Reliability Standard and with this appendix.

1.4. Additional Compliance Information

No specific provisions.

2. Violation Severity Levels

No specific provisions.

D. Regional variations

No specific provisions.

E. Interpretations

No specific provisions.

F. Associated Documents

No specific provisions.

Attachment 1

No specific provisions.

Attachment 2

No specific provisions.

Guidelines and technical basis

No specific provisions.

Rationale

No specific provisions.

Version history

Version	Date	Action	Change tracking
1	September 10, 2020	New attachment.	New
2	October 16, 2020	Improvements to layout of document.	Revised

A. Introduction

1. **Title:** Cyber Security — Personnel & Training

2. **Number:** CIP-004-7

3. **Purpose:** To minimize the risk against compromise that could lead to misoperation or instability in the Bulk Electric System (BES) from individuals accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training, security awareness, and access management in support of protecting BES Cyber Systems.

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1. Balancing Authority

   4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

   4.1.3. Generator Operator

   4.1.4. Generator Owner

   4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-004-7:

4.2.3.1. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1a identification and categorization processes.

5. **Effective Dates:** See Implementation Plan for CIP-004-7.

6. **Background:** Standard CIP-004 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.

   Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the common subject matter of the requirements.

   The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.

   The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

   Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

   Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

   Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed

as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the BES. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:
Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1a identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1a identification and categorization processes.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-004-7 Table R1 – Security Awareness Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-004-7 Table R1 – Security Awareness Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-7 Table R1 – Security Awareness Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Security awareness that, at least once each calendar quarter, reinforces cyber security practices (which may include associated physical security practices) for the Responsible Entity's personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Systems.	An example of evidence may include, but is not limited to, documentation that the quarterly reinforcement has been provided. Examples of evidence of reinforcement may include, but are not limited to, dated copies of information used to reinforce security awareness, as well as evidence of distribution, such as: • direct communications (for example, e-mails, memos, computer-based training); or • indirect communications (for example, posters, intranet, or brochures); or • management support and reinforcement (for example, presentations or meetings).

R2. Each Responsible Entity shall implement one or more cyber security training program(s) appropriate to individual roles, functions, or responsibilities that collectively includes each of the applicable requirement parts in *CIP-004-7 Table R2 – Cyber Security Training Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M2. Evidence must include the training program that includes each of the applicable requirement parts in *CIP-004-7 Table R2 – Cyber Security Training Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-7 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Training content on: 2.1.1. Cyber security policies; 2.1.2. Physical access controls; 2.1.3. Electronic access controls; 2.1.4. The visitor control program; 2.1.5. Handling of BES Cyber System Information and its storage; 2.1.6. Identification of a Cyber Security Incident and initial notifications in accordance with the entity's incident response plan; 2.1.7. Recovery plans for BES Cyber Systems; 2.1.8. Response to Cyber Security Incidents; and 2.1.9. Cyber security risks associated with a BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets, including	Examples of evidence may include, but are not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials.

CIP-004-7 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
		Transient Cyber Assets, and with Removable Media.	
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Require completion of the training specified in Part 2.1 prior to granting authorized electronic access and authorized unescorted physical access to applicable Cyber Assets, except during CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, training records and documentation of when CIP Exceptional Circumstances were invoked.
2.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Require completion of the training specified in Part 2.1 at least once every 15 calendar months.	Examples of evidence may include, but are not limited to, dated individual training records.

R3. Each Responsible Entity shall implement one or more documented personnel risk assessment program(s) to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that collectively include each of the applicable requirement parts in *CIP-004-7 Table R3 – Personnel Risk Assessment Program*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M3. Evidence must include the documented personnel risk assessment programs that collectively include each of the applicable requirement parts in *CIP-004-7 Table R3 – Personnel Risk Assessment Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-7 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to confirm identity.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to confirm identity.
3.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and	Process to perform a seven year criminal history records check as part of each personnel risk assessment that includes: 3.2.1. current residence, regardless of duration; and 3.2.2. other locations where, during the seven years immediately prior to the date of the criminal history records check, the subject has resided	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to perform a seven year criminal history records check.

CIP-004-7 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
	2. PACS	for six consecutive months or more. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.	
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Criteria or process to evaluate criminal history records checks for authorizing access.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to evaluate criminal history records checks.
3.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and	Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted according to Parts 3.1 through 3.3.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's criteria or process for verifying contractors or service vendors personnel risk assessments.

CIP-004-7 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
	2. PACS		
3.5	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed according to Parts 3.1 to 3.4 within the last seven years.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process for ensuring that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed within the last seven years.

R4. Each Responsible Entity shall implement one or more documented access management program(s) that collectively include each of the applicable requirement parts in *CIP-004-7 Table R4 – Access Management Program. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M4. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-004-7 Table R4 – Access Management Program* and additional evidence to demonstrate that the access management program was implemented as described in the Measures column of the table.

CIP-004-7 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 4.1.1. Electronic access; and 4.1.2. Unescorted physical access into a Physical Security Perimeter	An example of evidence may include, but is not limited to, dated documentation of the process to authorize electronic access, and unescorted physical access in a Physical Security Perimeter.
4.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records.	Examples of evidence may include, but are not limited to: • Dated documentation of the verification between the system generated list of individuals who have been authorized for access (i.e., workflow database) and a system generated list of personnel who have access (i.e., user account listing), or Dated documentation of the

CIP-004-7 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
			verification between a list of individuals who have been authorized for access (i.e., authorization forms) and a list of individuals provisioned for access (i.e., provisioning forms or shared account listing).
4.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For electronic access, verify at least once every 15 calendar months that all user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and are those that the Responsible Entity determines are necessary.	An example of evidence may include, but is not limited to, documentation of the review that includes all of the following: 1. A dated listing of all accounts/account groups or roles within the system; 2. A summary description of privileges associated with each group or role; 3. Accounts assigned to the group or role; and Dated evidence showing verification of the privileges for the group are authorized and appropriate to the work function performed by people assigned to each account.

R5. Each Responsible Entity shall implement one or more documented access revocation program(s) that collectively include each of the applicable requirement parts in *CIP-004-7 Table R5 – Access Revocation*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning].*

M5. Evidence must include each of the applicable documented programs that collectively include each of the applicable requirement parts in *CIP-004-7 Table R5 – Access Revocation* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-7 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	A process to initiate removal of an individual's ability for unescorted physical access and Interactive Remote Access upon a termination action, and complete the removals within 24 hours of the termination action (Removal of the ability for access may be different than deletion, disabling, revocation, or removal of all access rights).	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form verifying access removal associated with the termination action; and Logs or other demonstration showing such persons no longer have access.
5.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For reassignments or transfers, revoke the individual's authorized electronic access to individual accounts and authorized unescorted physical access that the Responsible Entity determines are not necessary by the end of the next calendar day following the date that the Responsible Entity determines that the individual no longer requires retention of that access.	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form showing a review of logical and physical access; and Logs or other demonstration showing such persons no longer have access that the Responsible Entity determines is not necessary.
5.3	High Impact BES Cyber Systems and their associated:	For termination actions, revoke the individual's non-shared user accounts	An example of evidence may include, but is not limited to, workflow or sign-

CIP-004-7 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
	• EACMS	(unless already revoked according to Part 5.1) within 30 calendar days of the effective date of the termination action.	off form showing access removal for any individual BES Cyber Assets and software applications as determined necessary to completing the revocation of access and dated within thirty calendar days of the termination actions.
5.4	High Impact BES Cyber Systems and their associated: • EACMS	For termination actions, change passwords for shared account(s) known to the user within 30 calendar days of the termination action. For reassignments or transfers, change passwords for shared account(s) known to the user within 30 calendar days following the date that the Responsible Entity determines that the individual no longer requires retention of that access. If the Responsible Entity determines and documents that extenuating operating circumstances require a longer time period, change the password(s) within 10 calendar days following the end of the operating circumstances.	Examples of evidence may include, but are not limited to: • Workflow or sign-off form showing password reset within 30 calendar days of the termination; • Workflow or sign-off form showing password reset within 30 calendar days of the reassignments or transfers; or Documentation of the extenuating operating circumstance and workflow or sign-off form showing password reset within 10 calendar days following the end of the operating circumstance.

R6. Each Responsible Entity shall implement one or more documented access management program(s) to authorize, verify, and revoke provisioned access to BCSI pertaining to the "Applicable Systems" identified in *CIP-004-7 Table R6 – Access Management for BES Cyber System Information* that collectively include each of the applicable requirement parts in *CIP-004-7 Table R6 – Access Management for BES Cyber System Information*. To be considered access to BCSI in the context of this requirement, an individual has both the ability to obtain and use BCSI. Provisioned access is to be considered the result of the specific actions taken to provide an individual(s) the means to access BCSI (e.g., may include physical keys or access cards, user accounts and associated rights and privileges, encryption keys). *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning].*

M6. Evidence must include each of the applicable documented programs that collectively include the applicable requirement parts in *CIP-004-7 Table R6 – Access Management for BES Cyber System Information* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-7 Table R6 – Access Management for BES Cyber System Information

Part	Applicable Systems	Requirements	Measures
6.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Prior to provisioning, authorize (unless already authorized according to Part 4.1.) based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 6.1.1. Provisioned electronic access to electronic BCSI; and 6.1.2. Provisioned physical access to physical BCSI.	Examples of evidence may include, but are not limited to, individual records or lists that include who is authorized, the date of the authorization, and the justification of business need for the provisioned access.

CIP-004-7 Table R6 – Access Management for BES Cyber System Information			
Part	**Applicable Systems**	**Requirements**	**Measures**
6.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Verify at least once every 15 calendar months that all individuals with provisioned access to BCSI: 6.2.1. have an authorization record; and 6.2.2. still need the provisioned access to perform their current work functions, as determined by the Responsible Entity.	Examples of evidence may include, but are not limited to, the documentation of the review that includes all of the following: • List of authorized individuals; • List of individuals who have been provisioned access; • Verification that provisioned access is appropriate based on need; and • Documented reconciliation actions, if any.
6.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For termination actions, remove the individual's ability to use provisioned access to BCSI (unless already revoked according to Part 5.1) by the end of the next calendar day following the effective date of the termination action.	Examples of dated evidence may include, but are not limited to, access revocation records associated with the terminations and dated within the next calendar day of the termination action.

C. Compliance

1. **Compliance Monitoring Process:**

1.1. Compliance Enforcement Authority: "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- The applicable entity shall retain evidence of each requirement in this standard for three calendar years.
- The applicable entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Lower**	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so between 10 and 30 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so within the subsequent quarter but beyond 30 calendar days after the start of that calendar quarter. (1.1)	The Responsible Entity did not document or implement any security awareness process(es) to reinforce cyber security practices. (R1) OR The Responsible Entity did not reinforce cyber security practices and associated physical security practices for at least two consecutive calendar quarters. (1.1)
R2	**Operations Planning**	**Lower**	The Responsible Entity implemented a cyber security training program but failed to include one of the training content topics in Requirement Parts	The Responsible Entity implemented a cyber security training program but failed to include two of the training content topics in Requirement Parts	The Responsible Entity implemented a cyber security training program but failed to include three of the training content topics in Requirement Parts	The Responsible Entity did not implement a cyber security training program appropriate to individual roles, functions, or responsibilities. (R2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			2.1.1 through 2.1.9. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train one individual (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train one individual with authorized electronic or authorized unescorted physical access within	2.1.1 through 2.1.9. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train two individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train two individuals with authorized electronic or authorized unescorted physical access within	2.1.1 through 2.1.9. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train three individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train three individuals with authorized electronic or authorized unescorted physical access within	OR The Responsible Entity implemented a cyber security training program but failed to include four or more of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train four or more individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			15 calendar months of the previous training completion date. (2.3)	15 calendar months of the previous training completion date. (2.3)	15 calendar months of the previous training completion date. (2.3)	The Responsible Entity implemented a cyber security training program but failed to train four or more individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)
R3	**Operations Planning**	**Medium**	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for one individual. (R3)	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for two individuals. (R3)	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for three individuals. (R3)	The Responsible Entity did not have all of the required elements as described by 3.1 through 3.4 included within documented program(s) for implementing Personnel Risk Assessments (PRAs), for individuals, including contractors and service vendors, for obtaining and

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for one individual. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did	OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for two individuals. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did	OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for three individuals. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did	retaining authorized cyber or authorized unescorted physical access. (R3) OR The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for four or more individuals. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			not include the required checks described in 3.2.1 and 3.2.2 for one individual. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for one individual. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs)	not include the required checks described in 3.2.1 and 3.2.2 for two individuals. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for two individuals. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs)	not include the required checks described in 3.2.1 and 3.2.2 for three individuals. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for three individuals. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk	and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for four or more individuals. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for four or more individuals. (3.2 & 3.4) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			for one individual with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date. (3.5)	for two individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date. (3.5)	Assessments (PRAs) for three individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date. (3.5)	The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for four or more individuals. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for four or more individuals with authorized electronic or authorized unescorted physical access within 7

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						calendar years of the previous PRA completion date. (3.5)
R4	**Operations Planning and Same Day Operations**	**Medium**	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 10 and 20 calendar days after the start of a subsequent calendar quarter. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 20 and 30 calendar days after the start of a subsequent calendar quarter. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct	The Responsible Entity did not implement any documented program(s) for access management. (R4) OR The Responsible Entity did not implement one or more documented program(s) for access management that includes a process to authorize electronic access or unescorted physical access. (4.1) OR The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			15 calendar months of the previous verification but for 5% or less of its BES Cyber Systems, privileges were incorrect or unnecessary. (4.3)	and necessary within 15 calendar months of the previous verification but for more than 5% but less than (or equal to) 10% of its BES Cyber Systems, privileges were incorrect or unnecessary. (4.3)	and necessary within 15 calendar months of the previous verification but for more than 10% but less than (or equal to) 15% of its BES Cyber Systems, privileges were incorrect or unnecessary. (4.3)	authorization records for at least two consecutive calendar quarters. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for more than 15% of its BES Cyber Systems, privileges were incorrect or unnecessary. (4.3)
R5	**Same Day Operations**	**Medium**	The Responsible Entity has implemented one or more process(es) to revoke the individual's	The Responsible Entity has implemented one or more process(es) to remove the ability for	The Responsible Entity has implemented one or more process(es) to remove the ability for	The Responsible Entity has not implemented any documented program(s) for access

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
	and Operations Planning		user accounts upon termination action but did not do so for within 30 calendar days of the date of termination action for one or more individuals. (5.3) OR The Responsible Entity has implemented one or more process(es) to change passwords for shared accounts known to the user upon termination action, reassignment, or transfer, but did not do so for within 30 calendar days of the date of termination action, reassignment, or transfer for one or more individuals. (5.4) OR	unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for one individual. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for one individual, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of	unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for two individuals. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for two individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of	revocation for electronic access or unescorted physical access. (R5) OR The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for three or more individuals. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			The Responsible Entity has implemented one or more process(es) to determine and document extenuating operating circumstances following a termination action, reassignment, or transfer, but did not change one or more passwords for shared accounts known to the user within 10 calendar days following the end of the extenuating operating circumstances. (5.4)	the next calendar day following the predetermined date. (5.2)	the next calendar day following the predetermined date. (5.2)	access following reassignments or transfers but, for three or more individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (5.2)
R6	**Same Day Operations and Operations Planning**	**Medium**	The Responsible Entity has implemented one or more program(s) as required by Requirement R6 Part 6.1 but, for one individual, did not	The Responsible Entity has implemented one or more program(s) as required by Requirement R6 Part 6.1 but, for two individuals, did not	The Responsible Entity has implemented one or more program(s) as required by Requirement R6 Part 6.1 but, for three individuals, did not	The Responsible Entity did not implement one or more documented access management program(s) for BCSI. (R6)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. (6.1) OR The Responsible Entity performed the verification required by Requirement R6 Part 6.2 more than 15 calendar months but less than or equal to 16 calendar months of the previous verification. (6.2) OR The Responsible Entity has implemented one or more program(s) to remove the individual's ability to use provisioned access to BCSI but, for one individual, did not	authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. (6.1) OR The Responsible Entity performed the verification required by Requirement R6 Part 6.2 more than 16 calendar months but less than or equal to 17 calendar months of the previous verification. (6.2) OR The Responsible Entity has implemented one or more program(s) to remove the individual's ability to use provisioned access to BCSI but, for two individuals, did	authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. (6.1) OR The Responsible Entity performed the verification required by Requirement R6 Part 6.2 more than 17 calendar months but less than or equal to 18 calendar months of the previous verification. (6.2) OR The Responsible Entity has implemented one or more program(s) to remove the individual's ability to use provisioned access to BCSI but, for three individuals, did	OR The Responsible Entity has implemented one or more program(s) as required by Requirement R6 Part 6.1 but, for four or more individuals, did not authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. (6.1) OR The Responsible Entity performed the verification required by Requirement R6 Part 6.2 more than 18 calendar months of the previous verification. (6.2) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			do so by the timeframe required in Requirement R6, Part 6.3.	not do so by the timeframe required in Requirement R6, Part 6.3.	not do so by the timeframe required in Requirement R6, Part 6.3.	The Responsible Entity has implemented one or more program(s) to remove the individual's ability to use provisioned access to BCSI but, for four or more individuals, did not do so by the timeframe required in Requirement R6, Part 6.3.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	

Version	Date	Action	Change Tracking
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-004-5.	
5.1	9/30/13	Modified two VSLs in R4	Errata
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
6	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
6	1/21/16	FERC order issued approving CIP-004-6. Docket No. RM15-14-000	
7	8/12/21	Adopted by the NERC Board of Trustees	Revised to enhance BES reliability for entities to manage their BCSI.
7	12/7/21	FERC Order issued approving CIP-004-7 Docket No. RD21-6-000	
7	12/10/21	Effective Date	1/1/24

Appendix CIP-004-7-QC-1
Specific provisions applicable in Québec for standard
CIP-004-7 – Cyber Security – Personnel & Training

This appendix establishes specific provisions for the application of the standard in Québec. Provisions of the standard and of this appendix must be read jointly for comprehension and interpretation purposes. Where the standard and appendix differ, the appendix shall prevail.

A. Introduction

1. Title: No specific provisions.

2. Number: No specific provisions.

3. Purpose: No specific provisions.

4. Applicability:

4.1. Functional Entities

No specific provisions.

4.2. Facilities

This standard only applies to the facilities of the Main Transmission System (RTP) and to the facilities specified for the Distribution Provider. In the application of this standard, all reference to the terms "Bulk Electric System" or "BES" shall be replaced by the terms "Main Transmission System" or "RTP" respectively.

Additional Exemptions

The following are exempt from this standard:

- Any generating facility that meets the two following conditions: (1) the nameplate capacity of the facility is 300 MVA or less, and (2) no unit of the facility can be synchronized with a neighbouring System.
- Step-up substations of generating facilities identified in the preceding point.

5. Effective Dates:

5.1. Adoption of the standard by the Régie de l'énergie: December 13, 2022

5.2. Adoption of the appendix by the Régie de l'énergie: December 13, 2022

5.3. Effective date of the standard and its appendix in Québec: January 1, 2025

6. Background:

No specific provisions.

B. Requirements and Measures

No specific provisions.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

In Québec, "Compliance Enforcement Authority" means the Régie de l'énergie in its roles of monitoring and enforcing compliance with respect to the Reliability Standard and to this appendix.

1.2. Evidence Retention

No specific provisions.

1.3. Compliance Monitoring and Enforcement Program

The Régie de l'énergie establishes the monitoring processes used to evaluate data or information for the purpose of determining compliance or non-compliance with the Reliability Standard and with this appendix.

2. Table of Compliance Elements

No specific provisions.

D. Regional Variances

No specific provisions.

E. Interpretations

No specific provisions.

F. Associated Documents

No specific provisions.

Version History

Version	Date	Action	Change Tracking
1	December 13, 2022	New appendix as per decision D-2022-150.	New

A. Introduction

1. **Title:** Cyber Security — Electronic Security Perimeter(s)

2. **Number:** CIP-005-7

3. **Purpose:** To manage electronic access to BES Cyber Systems by specifying a controlled Electronic Security Perimeter in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1. Balancing Authority

   4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

   4.1.3. Generator Operator

   4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in Section 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-005-7:

4.2.3.1. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002 identification and categorization processes.

5. Effective Date: See Implementation Plan for Project 2019-03.

6. Background: Standard CIP-005 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans, and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training

program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicability Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002 identification and categorization processes.
- **High Impact BES Cyber Systems with Dial-up Connectivity** – Only applies to high impact BES Cyber Systems with Dial-up Connectivity.
- **High Impact BES Cyber Systems with External Routable Connectivity** – Only applies to high impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002 identification and categorization processes.

- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to medium impact BES Cyber Systems located at a Control Center.
- **Medium Impact BES Cyber Systems with Dial-up Connectivity** – Only applies to medium impact BES Cyber Systems with Dial-up Connectivity.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Electronic Access Points (EAP)** – Applies at Electronic Access Points associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-005-7 Table R1 – Electronic Security Perimeter*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-005-7 Table R1 – Electronic Security Perimeter* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-7 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems and their associated: • PCA	All applicable Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP.	An example of evidence may include, but is not limited to, a list of all ESPs with all uniquely identifiable applicable Cyber Assets connected via a routable protocol within each ESP.
1.2	High Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	All External Routable Connectivity must be through an identified Electronic Access Point (EAP).	An example of evidence may include, but is not limited to, network diagrams showing all external routable communication paths and the identified EAPs.

CIP-005-7 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	Electronic Access Points for High Impact BES Cyber Systems Electronic Access Points for Medium Impact BES Cyber Systems	Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default.	An example of evidence may include, but is not limited to, a list of rules (firewall, access control lists, etc.) that demonstrate that only permitted access is allowed and that each access rule has a documented reason.
1.4	High Impact BES Cyber Systems with Dial-up Connectivity and their associated: • PCA Medium Impact BES Cyber Systems with Dial-up Connectivity and their associated: • PCA	Where technically feasible, perform authentication when establishing Dial-up Connectivity with applicable Cyber Assets.	An example of evidence may include, but is not limited to, a documented process that describes how the Responsible Entity is providing authenticated access through each dial-up connection.
1.5	Electronic Access Points for High Impact BES Cyber Systems Electronic Access Points for Medium Impact BES Cyber Systems at Control Centers	Have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications.	An example of evidence may include, but is not limited to, documentation that malicious communications detection methods (e.g. intrusion detection system, application layer firewall, etc.) are implemented.

R2. Each Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts, where technically feasible, in *CIP-005-7 Table R2 –Remote Access Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M2. Evidence must include the documented processes that collectively address each of the applicable requirement parts in *CIP-005-7 Table R2 –Remote Access Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-7 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	For all Interactive Remote Access, utilize an Intermediate System such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset.	Examples of evidence may include, but are not limited to, network diagrams or architecture documents.
2.2	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	For all Interactive Remote Access sessions, utilize encryption that terminates at an Intermediate System.	An example of evidence may include, but is not limited to, architecture documents detailing where encryption initiates and terminates.

CIP-005-7 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	Require multi-factor authentication for all Interactive Remote Access sessions.	An example of evidence may include, but is not limited to, architecture documents detailing the authentication factors used. Examples of authenticators may include, but are not limited to, • Something the individual knows such as passwords or PINs. This does not include User ID; • Something the individual has such as tokens, digital certificates, or smart cards; or • Something the individual is such as fingerprints, iris scans, or other biometric characteristics.

CIP-005-7 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.4	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	Have one or more methods for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access).	Examples of evidence may include, but are not limited to, documentation of the methods used to determine active vendor remote access (including Interactive Remote Access and system-to-system remote access), such as: • Methods for accessing logged or monitoring information to determine active vendor remote access sessions; • Methods for monitoring activity (e.g. connection tables or rule hit counters in a firewall, or user activity monitoring) or open ports (e.g. netstat or related commands to display currently active ports) to determine active system to system remote access sessions; or • Methods that control vendor initiation of remote access such as vendors calling and requesting a second factor in order to initiate remote access.

CIP-005-7 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.5	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	Have one or more method(s) to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access).	Examples of evidence may include, but are not limited to, documentation of the methods(s) used to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access), such as: • Methods to disable vendor remote access at the applicable Electronic Access Point for system-to-system remote access; or • Methods to disable vendor Interactive Remote Access at the applicable Intermediate System.

R3. Each Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts in *CIP-005-7 Table R3 –Vendor Remote Access Management for EACMS and PACS*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M3. Evidence must include the documented processes that collectively address each of the applicable requirement parts in *CIP-005-7 Table R3 – Vendor Remote Access Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-7 Table R3 – Vendor Remote Access Management for EACMS and PACS			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	EACMS and PACS associated with High Impact BES Cyber Systems EACMS and PACS associated with Medium Impact BES Cyber Systems with External Routable Connectivity	Have one or more method(s) to determine authenticated vendor-initiated remote connections.	Examples of evidence may include, but are not limited to, documentation of the methods used to determine authenticated vendor-initiated remote connections, such as: • Methods for accessing logged or monitoring information to determine authenticated vendor-initiated remote connections.
3.2	EACMS and PACS associated with High Impact BES Cyber Systems EACMS and PACS associated with Medium Impact BES Cyber Systems with External Routable Connectivity	Have one or more method(s) to terminate authenticated vendor-initiated remote connections and control the ability to reconnect.	Examples of evidence may include, but are not limited to, documentation of the methods(s) used to terminate authenticated vendor-initiated remote connections to applicable systems. Examples include terminating an active vendor-initiated shell/process/session or dropping an active vendor-initiated connection in

CIP-005-7 Table R3 – Vendor Remote Access Management for EACMS and PACS			
Part	**Applicable Systems**	**Requirements**	**Measures**
			a firewall. Methods to control the ability to reconnect, if necessary, could be: disabling an Active Directory account; disabling a security token; restricting IP addresses from vendor sources in a firewall; or physically disconnecting a network cable to prevent a reconnection.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation.

- Each applicable entity shall retain evidence of each requirement in this standard for three calendar years.
- If an applicable entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.			The Responsible Entity did not have a method for detecting malicious communications for both inbound and outbound communications. (1.5)	The Responsible Entity did not document one or more processes for *CIP-005-6 Table R1 – Electronic Security Perimeter*. (R1) OR The Responsible Entity did not have all applicable Cyber Assets connected to a network via a routable protocol within a defined Electronic Security Perimeter (ESP). (1.1) OR External Routable Connectivity through the ESP was not through an identified EAP. (1.2) OR The Responsible Entity did not require inbound and outbound access permissions and deny all other access by default. (1.3) OR

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				The Responsible Entity did not perform authentication when establishing dial-up connectivity with the applicable Cyber Assets, where technically feasible. (1.4)
R2.	The Responsible Entity does not have documented processes for one or more of the applicable items for Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for one of the applicable items for Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for two of the applicable items for Requirement Parts 2.1 through 2.3; OR The Responsible Entity did not have either: one or more method(s) for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access) (2.4); or one or more methods to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access) (2.5).	The Responsible Entity did not implement processes for three of the applicable items for Requirement Parts 2.1 through 2.3; OR The Responsible Entity did not have one or more method(s) for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access) (2.4) and one or more methods to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access) (2.5).

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R3.	The Responsible Entity did not document one or more processes for *CIP-005-7 Table R3 – Vendor Remote Access Management for EACMS and PACS*. (R3)	The Responsible Entity had method(s) as required by Part 3.1 for EACMS but did not have a method to determine authenticated vendor-initiated remote connections for PACS (3.1). OR The Responsible Entity had method(s) as required by Part 3.2 for EACMS but did not have a method to terminate authenticated vendor-initiated remote connections for PACS (3.2).	The Responsible Entity did not implement processes for either Part 3.1 or Part 3.2. (R3) OR The Responsible Entity had method(s) as required by Part 3.1 for PACS but did not have a method to determine authenticated vendor-initiated remote connections for EACMS (3.1). OR The Responsible Entity had method(s) as required by Part 3.2 for PACS but did not have a method to terminate authenticated vendor-initiated remote connections or control the ability to reconnect for EACMS (3.2).	The Responsible Entity did not implement any processes for *CIP-005-7 Table R3 – Vendor Remote Access Management for EACMS and PACS*. (R3) OR The Responsible Entity did not have any methods as required by Parts 3.1 and 3.2 (R3).

D. Regional Variances

None.

E. Associated Documents

- Implementation Plan for Project 2019-03
- CIP-005-7 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-005-5.	
6	07/20/17	Modified to address certain directives in FERC Order No. 829.	Revised
6	08/10/17	Adopted by the NERC Board of Trustees.	
6	10/18/2018	FERC Order approving CIP-005-6. Docket No. RM17-13-000.	
7	08/01/2019	Modified to address directives in FERC Order No. 850.	Revised

7	11/05/2020	Adopted by the NERC Board of Trustees.	
7	3/18/2021	FERC Order approving CIP-005-7. Docket No. RD21-2-000	
7	10/1/2022	Effective Date	

Appendix CIP-005-7-QC-1
Specific provisions applicable in Québec for standard CIP-005-7 – Cyber Security – Electronic Security Perimeter(s)

This appendix establishes specific provisions for the application of the standard in Québec. Provisions of the standard and of this appendix must be read jointly for comprehension and interpretation purposes. Where the standard and appendix differ, the appendix shall prevail.

A. Introduction

1. **Title:** No specific provisions.

2. **Number:** No specific provisions.

3. **Purpose:** No specific provisions.

4. **Applicability:**

4.1. Functional Entities

No specific provisions.

4.2. Facilities

This standard only applies to the facilities of the Main Transmission System (RTP) and to the facilities specified for the Distribution Provider. In the application of this standard, all reference to the terms "Bulk Electric System" or "BES" shall be replaced by the terms "Main Transmission System" or "RTP" respectively.

Additional Exemptions

The following are exempt from this standard:

- Any generating facility that meets the two following conditions: (1) the nameplate capacity of the facility is 300 MVA or less, and (2) no unit of the facility can be synchronized with a neighbouring system.
- Step-up substations of generating facilities identified in the preceding point.

5. **Effective Date:**

5.1.	Adoption of the standard by the Régie de l'énergie:	February 11, 2022
5.2.	Adoption of the appendix by the Régie de l'énergie:	February 11, 2022
5.3.	Effective date of the standard and its appendix in Québec:	October 1, 2023

6. **Background:** No specific provisions.

B. Requirements and Measures

No specific provisions.

C. Compliance

1. **Compliance Monitoring Process**

1.1. Compliance Enforcement Authority

In Québec, "Compliance Enforcement Authority" means the Régie de l'énergie in its roles of monitoring and enforcing compliance with respect to the Reliability Standard and to this appendix.

1.2. Evidence Retention

No specific provisions.

1.3. Compliance Monitoring and Enforcement Program

The Régie de l'énergie establishes the monitoring processes used to evaluate data or information for the purpose of determining compliance or non-compliance with the Reliability Standard and with this appendix.

Violation Severity Levels (VSL)

No specific provisions.

D. Regional Variances

No specific provisions.

E. Associated Documents

No specific provisions.

Version History

Version	Date	Action	Change Tracking
1	February 11, 2022	New appendix as per decision D-2022-021.	New

A. Introduction

1. Title: Cyber Security — Physical Security of BES Cyber Systems

2. Number: CIP-006-6

3. Purpose: To manage physical access to Bulk Electric System (BES) Cyber Systems by specifying a physical security plan in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System (SPS) or Remedial Action Scheme (RAS) where the SPS or RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each SPS or RAS where the SPS or RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-006-6:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

5. Effective Dates:

See Implementation Plan for CIP-006-6.

6. Background:

Standard CIP-006 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems without External Routable Connectivity** – Only applies to medium impact BES Cyber Systems without External Routable Connectivity.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Locally mounted hardware or devices at the Physical Security Perimeter –** Applies to the locally mounted hardware or devices (e.g. such as motion sensors, electronic lock control mechanisms, and badge readers) at a Physical Security Perimeter associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity, and that does not contain or store access control information or independently perform access authentication. These hardware and devices are excluded in the definition of Physical Access Control Systems.

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented physical security plan(s) that collectively include all of the applicable requirement parts in *CIP-006-6 Table R1 – Physical Security Plan*. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning and Same Day Operations].*

M1. Evidence must include each of the documented physical security plans that collectively include all of the applicable requirement parts in *CIP-006-6 Table R1 – Physical Security Plan* and additional evidence to demonstrate implementation of the plan or plans as described in the Measures column of the table.

CIP-006-6 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	Medium Impact BES Cyber Systems without External Routable Connectivity Physical Access Control Systems (PACS) associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity	Define operational or procedural controls to restrict physical access.	An example of evidence may include, but is not limited to, documentation that operational or procedural controls exist.

CIP-006-6 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Utilize at least one physical access control to allow unescorted physical access into each applicable Physical Security Perimeter to only those individuals who have authorized unescorted physical access.	An example of evidence may include, but is not limited to, language in the physical security plan that describes each Physical Security Perimeter and how unescorted physical access is controlled by one or more different methods and proof that unescorted physical access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by access logs.

CIP-006-6 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA	Where technically feasible, utilize two or more different physical access controls (this does not require two completely independent physical access control systems) to collectively allow unescorted physical access into Physical Security Perimeters to only those individuals who have authorized unescorted physical access.	An example of evidence may include, but is not limited to, language in the physical security plan that describes the Physical Security Perimeters and how unescorted physical access is controlled by two or more different methods and proof that unescorted physical access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by access logs.

CIP-006-6 Table R1– Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Monitor for unauthorized access through a physical access point into a Physical Security Perimeter.	An example of evidence may include, but is not limited to, documentation of controls that monitor for unauthorized access through a physical access point into a Physical Security Perimeter.

CIP-006-6 Table R1– Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.5	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Issue an alarm or alert in response to detected unauthorized access through a physical access point into a Physical Security Perimeter to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of detection.	An example of evidence may include, but is not limited to, language in the physical security plan that describes the issuance of an alarm or alert in response to unauthorized access through a physical access control into a Physical Security Perimeter and additional evidence that the alarm or alert was issued and communicated as identified in the BES Cyber Security Incident Response Plan, such as manual or electronic alarm or alert logs, cell phone or pager logs, or other evidence that documents that the alarm or alert was generated and communicated.
1.6	Physical Access Control Systems (PACS) associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity	Monitor each Physical Access Control System for unauthorized physical access to a Physical Access Control System.	An example of evidence may include, but is not limited to, documentation of controls that monitor for unauthorized physical access to a PACS.

CIP-006-6 Table R1– Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.7	Physical Access Control Systems (PACS) associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity	Issue an alarm or alert in response to detected unauthorized physical access to a Physical Access Control System to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of the detection.	An example of evidence may include, but is not limited to, language in the physical security plan that describes the issuance of an alarm or alert in response to unauthorized physical access to Physical Access Control Systems and additional evidence that the alarm or alerts was issued and communicated as identified in the BES Cyber Security Incident Response Plan, such as alarm or alert logs, cell phone or pager logs, or other evidence that the alarm or alert was generated and communicated.

CIP-006-6 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.8	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Log (through automated means or by personnel who control entry) entry of each individual with authorized unescorted physical access into each Physical Security Perimeter, with information to identify the individual and date and time of entry.	An example of evidence may include, but is not limited to, language in the physical security plan that describes logging and recording of physical entry into each Physical Security Perimeter and additional evidence to demonstrate that this logging has been implemented, such as logs of physical access into Physical Security Perimeters that show the individual and the date and time of entry into Physical Security Perimeter.

CIP-006-6 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.9	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Retain physical access logs of entry of individuals with authorized unescorted physical access into each Physical Security Perimeter for at least ninety calendar days.	An example of evidence may include, but is not limited to, dated documentation such as logs of physical access into Physical Security Perimeters that show the date and time of entry into Physical Security Perimeter.

CIP-006-6 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.10	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems at Control Centers and their associated: • PCA	Restrict physical access to cabling and other nonprogrammable communication components used for connection between applicable Cyber Assets within the same Electronic Security Perimeter in those instances when such cabling and components are located outside of a Physical Security Perimeter. Where physical access restrictions to such cabling and components are not implemented, the Responsible Entity shall document and implement one or more of the following: • encryption of data that transits such cabling and components; or • monitoring the status of the communication link composed of such cabling and components and issuing an alarm or alert in response to detected communication failures to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of detection; or • an equally effective logical protection.	An example of evidence may include, but is not limited to, records of the Responsible Entity's implementation of the physical access restrictions (e.g., cabling and components secured through conduit or secured cable trays) encryption, monitoring, or equally effective logical protections.

R2. Each Responsible Entity shall implement one or more documented visitor control program(s) that include each of the applicable requirement parts in *CIP-006-6 Table R2 – Visitor Control Program. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations.]*

M2. Evidence must include one or more documented visitor control programs that collectively include each of the applicable requirement parts in *CIP-006-6 Table R2 – Visitor Control Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-6 Table R2 – Visitor Control Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Require continuous escorted access of visitors (individuals who are provided access but are not authorized for unescorted physical access) within each Physical Security Perimeter, except during CIP Exceptional Circumstances.	An example of evidence may include, but is not limited to, language in a visitor control program that requires continuous escorted access of visitors within Physical Security Perimeters and additional evidence to demonstrate that the process was implemented, such as visitor logs.

CIP-006-6 Table R2 – Visitor Control Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Require manual or automated logging of visitor entry into and exit from the Physical Security Perimeter that includes date and time of the initial entry and last exit, the visitor's name, and the name of an individual point of contact responsible for the visitor, except during CIP Exceptional Circumstances.	An example of evidence may include, but is not limited to, language in a visitor control program that requires continuous escorted access of visitors within Physical Security Perimeters and additional evidence to demonstrate that the process was implemented, such as dated visitor logs that include the required information.
2.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Retain visitor logs for at least ninety calendar days.	An example of evidence may include, but is not limited to, documentation showing logs have been retained for at least ninety calendar days.

R3. Each Responsible Entity shall implement one or more documented Physical Access Control System maintenance and testing program(s) that collectively include each of the applicable requirement parts in *CIP-006-6 Table R3 – Maintenance and Testing Program*. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning].*

M3. Evidence must include each of the documented Physical Access Control System maintenance and testing programs that collectively include each of the applicable requirement parts in *CIP-006-6 Table R3 – Maintenance and Testing Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-6 Table R3 – Physical Access Control System Maintenance and Testing Program			
Part	**Applicable Systems**	**Requirement**	**Measures**
3.1	Physical Access Control Systems (PACS) associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity Locally mounted hardware or devices at the Physical Security Perimeter associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity	Maintenance and testing of each Physical Access Control System and locally mounted hardware or devices at the Physical Security Perimeter at least once every 24 calendar months to ensure they function properly.	An example of evidence may include, but is not limited to, a maintenance and testing program that provides for testing each Physical Access Control System and locally mounted hardware or devices associated with each applicable Physical Security Perimeter at least once every 24 calendar months and additional evidence to demonstrate that this testing was done, such as dated maintenance records, or other documentation showing testing and maintenance has been performed on each applicable device or system at least once every 24 calendar months.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Investigations

Self-Reporting

Complaints

1.4. Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Long Term Planning** **Same-Day Operations**	**Medium**	N/A	N/A	N/A	The Responsible Entity did not document or implement physical security plans. (R1) OR The Responsible Entity did not document or implement operational or procedural controls to restrict physical access. (1.1) OR The Responsible Entity has documented and implemented physical access controls, but at least one control does not exist to restrict access to Applicable Systems. (1.2) OR The Responsible Entity has documented and implemented physical

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						access controls, but at least two different controls do not exist to restrict access to Applicable Systems. (1.3) OR The Responsible Entity does not have a process to monitor for unauthorized access through a physical access point into a Physical Security Perimeter. (1.4) OR The Responsible Entity does not have a process to alert for detected unauthorized access through a physical access point into a Physical Security Perimeter or to communicate such alerts within 15 minutes to identified personnel.

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						(1.5) OR The Responsible Entity does not have a process to monitor each Physical Access Control System for unauthorized physical access to a Physical Access Control Systems. (1.6) OR The Responsible Entity does not have a process to alert for unauthorized physical access to Physical Access Control Systems or to communicate such alerts within 15 minutes to identified personnel. (1.7) OR The Responsible Entity does not have a process to log authorized physical entry into each

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						Physical Security Perimeter with sufficient information to identify the individual and date and time of entry. (1.8) OR The Responsible Entity does not have a process to retain physical access logs for 90 calendar days. (1.9) OR The Responsible Entity did not document or implement physical access restrictions, encryption, monitoring or equally effective logical protections for cabling and other nonprogrammable communication components used for connection between applicable Cyber Assets within the same

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						Electronic Security Perimeter in those instances when such cabling and components are located outside of a Physical Security Perimeter. (1.10)
R2	**Same-Day Operations**	**Medium**	N/A	N/A	N/A	The Responsible Entity has failed to include or implement a visitor control program that requires continuous escorted access of visitors within any Physical Security Perimeter. (2.1) OR The Responsible Entity has failed to include or implement a visitor control program that requires logging of the initial entry and last exit dates and times of the visitor, the visitor's name, and the point of

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						contact. (2.2) OR The Responsible Entity failed to include or implement a visitor control program to retain visitor logs for at least ninety days. (2.3)
R3	**Long Term Planning**	**Medium**	The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter, but	The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 25 calendar months but did complete required testing within 26 calendar months. (3.1)	The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 26 calendar months but did complete required testing within 27 calendar months. (3.1)	The Responsible Entity did not document or implement a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter. (3.1) OR The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			did not complete required testing within 24 calendar months but did complete required testing within 25 calendar months. (3.1)			mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 27 calendar months. (3.1)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of	

Version	Date	Action	Change Tracking
		Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-006-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed FERC directives from Order No. 791.
6	1/21/16	FERC order issued approving CIP-006-6. Docket No. RM15-14-000	

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

General:

While the focus of this Reliability Standard has shifted away from the definition and management of a completely enclosed "six-wall" boundary, it is expected that in many instances a six-wall boundary will remain a primary mechanism for controlling, alerting, and logging access to BES Cyber Systems. Taken together, these controls outlined below will effectively constitute the physical security plan to manage physical access to BES Cyber Systems.

Requirement R1:

Methods of physical access control include:

- Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another.
- Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems.
- Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.

- Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access into the Physical Security Perimeter.

Methods to monitor physical access include:

- Alarm Systems: Systems that alarm to indicate interior motion or when a door, gate, or window has been opened without authorization. These alarms must provide for notification within 15 minutes to individuals responsible for response.
- Human Observation of Access Points: Monitoring of physical access points by security personnel who are also controlling physical access.

Methods to log physical access include:

- Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and alerting method.
- Video Recording: Electronic capture of video images of sufficient quality to determine identity.
- Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access.

The FERC Order No. 706, Paragraph 572, directive discussed utilizing two or more different and complementary physical access controls to provide defense in depth. It does not require two or more Physical Security Perimeters, nor does it exclude the use of layered perimeters. Use of two-factor authentication would be acceptable at the same entry points for a non-layered single perimeter. For example, controls for a sole perimeter could include either a combination of card key and pin code (something you know and something you have), or a card key and biometric scanner (something you have and something you are), or a physical key in combination with a guard-monitored remote camera and door release, where the "guard" has adequate information to authenticate the person the guard is observing or talking to prior to permitting access (something you have and something you are). The two-factor authentication could be implemented using a single Physical Access Control System but more than one authentication method must be utilized. For physically layered protection, a locked gate in combination with a locked control-building could be acceptable, provided no single authenticator (e.g., key or card key) would provide access through both.

Entities may choose for certain PACS to reside in a PSP controlling access to applicable BES Cyber Systems. For these PACS, there is no additional obligation to comply with Requirement Parts 1.1, 1.6 and 1.7 beyond what is already required for the PSP.

The new requirement part CIP-006-6, Requirement R1, Part 1.10 responds to the directive found in FERC Order No. 791, Paragraph 150. The requirement intends to protect cabling and nonprogrammable communication components that are within an ESP, but extend outside of a PSP. This protection, similar to the FERC Approved NERC Petition on the interpretation on CIP-006-2 from PacifiCorp, must be accomplished either by physically protecting the cabling and components that leave a PSP (such as by conduit or secured cable trays) or through data encryption, circuit monitoring, or equally effective logical protections. It is intended that the

physical protections reduce the possibility of tampering or allowing direct access to the nonprogrammable devices. Conduit, secured cable trays, and secured communication closets are examples of these types of protections. These physical security measures should be implemented in such a way that they would provide some mechanism to detect or recognize that someone could have tampered with the cabling and non-programmable components. This could be something as simple as a padlock on a communications closet where the entity would recognize if the padlock had been cut off. Alternatively, this protection may also be accomplished through the use of armored cabling or via the stainless steel or aluminum tube protecting the fiber inside an optical ground wire (OPGW) cable. In using any of these methods, care should be taken to protect the entire length of the cabling including any termination points that may be outside of a defined PSP.

This requirement part only covers those portions of cabling and nonprogrammable communications components that are located outside of the PSP, but inside the ESP. Where this cabling and non-programmable communications components exist inside the PSP, this requirement part no longer applies.

The requirement focuses on physical protection of the communications cabling and components as this is a requirement in a physical security standard and the gap in protection identified by FERC in Order 791 is one of physical protections. However, the requirement part recognizes that there is more than one way to provide protection to communication cabling and nonprogrammable components. In particular, the requirement provides a mechanism for entities to select an alternative to physical security protection that may be chosen in a situation where an entity cannot implement physical security or simply chooses not to implement physical security. The entity is under no obligation to justify or explain why it chose logical protections over physical protections identified in the requirement.

The alternative protective measures identified in the CIP-006-6 R1, Part 1.10 (encryption and circuit monitoring) were identified as acceptable alternatives in NERC petition of the PacifiCorp Interpretation of CIP-006-2 which was approved by FERC (RD10-13-000). If an entity chooses to implement an “an equally effective logical protection” in lieu of one of the protection mechanisms identified in the standard, the entity would be expected to document how the protection is equally effective. NERC explained in its petition of the PacifiCorp Interpretation of CIP-006-2 that the measures are relevant to access or physical tampering. Therefore, the entity may choose to discuss how its protection may provide detection of tampering. The entity may also choose to explain how its protection is equivalent to the other logical options identified in the standard in terms of the CIA triad (confidentiality, integrity, and availability). The entity may find value in reviewing their plans prior to implementation with the regional entity, but there is no obligation to do so.

The intent of the requirement is not to require physical protection of third party components, consistent with FERC Order 791-A. The requirement allows flexibility in that the entity has control of how to design its ESP and also has the ability to extend its ESP outside its PSP via the logical mechanisms specified in CIP-006-6 Requirement 1, Part 1.10 such as encryption (which is an option specifically identified in FERC Order 791-A). These mechanisms should provide sufficient protections to an entity’s BES Cyber Systems while not requiring controls to be

implemented on third-party components when entities rely on leased third-party communications.

In addition to the cabling, the components in scope of this requirement part are those components outside of a PSP that could otherwise be considered a BES Cyber Asset or Protected Cyber Asset except that they do not meet the definition of Cyber Asset because they are nonprogrammable. Examples of these nonprogrammable components include, but are not limited to, unmanaged switches, hubs, patch panels, media converters, port savers, and couplers.

Requirement R2:

The logging of visitors should capture each visit of the individual and does not need to capture each entry or exit during that visit. This is meant to allow a visitor to temporarily exit the Physical Security Perimeter to obtain something they left in their vehicle or outside the area without requiring a new log entry for each and every entry during the visit.

The SDT also determined that a point of contact should be documented who can provide additional details about the visit if questions arise in the future. The point of contact could be the escort, but there is no need to document everyone that acted as an escort for the visitor.

Requirement R3:

This includes the testing of locally mounted hardware or devices used in controlling, alerting or logging access to the Physical Security Perimeter. This includes motion sensors, electronic lock control mechanisms, and badge readers which are not deemed to be part of the Physical Access Control System but are required for the protection of the BES Cyber Systems.

Rationale:

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for Requirement R1:

Each Responsible Entity shall ensure that physical access to all BES Cyber Systems is restricted and appropriately managed. Entities may choose for certain Physical Access Control Systems (PACS) to reside in a Physical Security Perimeter (PSP) controlling access to applicable BES Cyber Systems. For these PACS, there is no additional obligation to comply with Requirement R1, Parts 1.1, 1.6 and 1.7 beyond what is already required for the PSP.

Regarding Requirement R1, Part 1.10, when cabling and other nonprogrammable components of a Control Center's communication network cannot be secured in a PSP, steps must be taken to ensure the integrity of the BES Cyber Systems. Exposed communication pathways outside of a PSP necessitate that physical or logical protections be installed to reduce the likelihood that man-in-the-middle attacks could compromise the integrity of their connected BES Cyber Assets or PCAs that are required to reside within PSPs. While it is anticipated that priority consideration will be given to physically securing the cabling and nonprogrammable

communications components, the SDT understands that configurations arise when physical access restrictions are not ideal and Responsible Entities are able to reasonably defend their physically exposed communications components through specific additional logical protections.

Rationale for Requirement R2:

To control when personnel without authorized unescorted physical access can be in any Physical Security Perimeters protecting BES Cyber Systems or Electronic Access Control or Monitoring Systems, as applicable in Table R2.

Rationale for Requirement R3:

To ensure all Physical Access Control Systems and devices continue to function properly.

Appendix QC-CIP-006-6
Provisions specific to the standard CIP-006-6 applicable in Québec

This appendix establishes specific provisions for the application of the standard in Québec. Provisions of the standard and of its appendix must be read together for the purposes of understanding and interpretation. Where the standard and appendix differ, the appendix shall prevail.

A. Introduction

1. Title: Cyber Security — Physical Security of BES Cyber Systems

2. Number: CIP-006-6

3. Purpose: No specific provision

4. Applicability:

4.1. Functional Entities

No specific provision

4.2. Facilities

This standard only applies to the facilities of the Main Transmission System (RTP) and to the facilities specified for the Distribution Provider. In the application of this standard, all reference to the terms "Bulk Electric System" or "BES" shall be replaced by the terms "Main Transmission System" or "RTP" respectively.

Additional Exemptions

The following are exempt from this standard:

- Any generating facility that meets the two following conditions: (1) the nameplate capacity of the facility is 300 MVA or less, and (2) no unit of the facility can be synchronized with a neighbouring system.
- Step-up substations of generating facilities identified in the preceding point.

5. Effective Date:

5.1. Adoption of the standard by the Régie de l'énergie: October 31st, 2017

5.2. Adoption of the appendix by the Régie de l'énergie: October 31st, 2017

5.3. Effective date of the standard and its appendix in Québec: January 1st, 2018

Standard	Implementation date for Québec		
	Entities subject to version 1 of the CIP standards adopted by the Régie	Entities exempted from the application of version 1 of the CIP standards under the specific provisions associated with these standards	Entities that have generation facilities for industrial use
CIP-006-6	January 1st, 2018	October 1st, 2018	April 1st, 2019

6. Background:

No specific provision

B. Requirements and Measures

No specific provision

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

The Régie de l'énergie is responsible, in Québec, for compliance enforcement with respect to the reliability standard and its appendix that it adopts.

1.2. Evidence Retention

No specific provision

1.3. Compliance Monitoring and Assessment Processes

No specific provision

1.4. Additional Compliance Information

No specific provision

2. Table of Compliance Elements

No specific provision

D. Regional Variances

No specific provision

E. Interpretations

No specific provision

F. Associated Documents

No specific provision

Guidelines and Technical Basis

No specific provision

Rationale

No specific provision

Version History

Revision	Date	Action	Change Tracking
0	October 31st, 2017	New appendix	New

A. Introduction

1. Title: Cyber Security — System Security Management

2. Number: CIP-007-6

3. Purpose: To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System (SPS) or Remedial Action Scheme (RAS) where the SPS or RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each SPS or RAS where the SPS or RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-007-6:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

5. Effective Dates:

See Implementation Plan for CIP-007-6.

6. Background:

Standard CIP-007 exists as part of a suite of CIP Standards related to cyber security, which requires the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the BES. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to medium impact BES Cyber Systems located at a Control Center.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System in the applicability column. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-6 Table R1 – Ports and Services*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations.]*

M1. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-007-6 Table R1 – Ports and Services* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-6 Table R1– Ports and Services			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Where technically feasible, enable only logical network accessible ports that have been determined to be needed by the Responsible Entity, including port ranges or services where needed to handle dynamic ports. If a device has no provision for disabling or restricting logical ports on the device then those ports that are open are deemed needed.	Examples of evidence may include, but are not limited to: • Documentation of the need for all enabled ports on all applicable Cyber Assets and Electronic Access Points, individually or by group. • Listings of the listening ports on the Cyber Assets, individually or by group, from either the device configuration files, command output (such as netstat), or network scans of open ports; or • Configuration files of host-based firewalls or other device level mechanisms that only allow needed ports and deny all others.

CIP-007-6 Table R1– Ports and Services			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems and their associated: 1. PCA; and 2. Nonprogrammable communication components located inside both a PSP and an ESP. Medium Impact BES Cyber Systems at Control Centers and their associated: 1. PCA; and 2. Nonprogrammable communication components located inside both a PSP and an ESP.	Protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or Removable Media.	An example of evidence may include, but is not limited to, documentation showing types of protection of physical input/output ports, either logically through system configuration or physically using a port lock or signage.

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-6 Table R2 – Security Patch Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-007-6 Table R2 – Security Patch Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-6 Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	A patch management process for tracking, evaluating, and installing cyber security patches for applicable Cyber Assets. The tracking portion shall include the identification of a source or sources that the Responsible Entity tracks for the release of cyber security patches for applicable Cyber Assets that are updateable and for which a patching source exists.	An example of evidence may include, but is not limited to, documentation of a patch management process and documentation or lists of sources that are monitored, whether on an individual BES Cyber System or Cyber Asset basis.

CIP-007-6 Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	At least once every 35 calendar days, evaluate security patches for applicability that have been released since the last evaluation from the source or sources identified in Part 2.1.	An example of evidence may include, but is not limited to, an evaluation conducted by, referenced by, or on behalf of a Responsible Entity of security-related patches released by the documented sources at least once every 35 calendar days.

CIP-007-6 Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For applicable patches identified in Part 2.2, within 35 calendar days of the evaluation completion, take one of the following actions: • Apply the applicable patches; or • Create a dated mitigation plan; or • Revise an existing mitigation plan. Mitigation plans shall include the Responsible Entity's planned actions to mitigate the vulnerabilities addressed by each security patch and a timeframe to complete these mitigations.	Examples of evidence may include, but are not limited to: • Records of the installation of the patch (e.g., exports from automated patch management tools that provide installation date, verification of BES Cyber System Component software revision, or registry exports that show software has been installed); or • A dated plan showing when and how the vulnerability will be addressed, to include documentation of the actions to be taken by the Responsible Entity to mitigate the vulnerabilities addressed by the security patch and a timeframe for the completion of these mitigations.

CIP-007-6 Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For each mitigation plan created or revised in Part 2.3, implement the plan within the timeframe specified in the plan, unless a revision to the plan or an extension to the timeframe specified in Part 2.3 is approved by the CIP Senior Manager or delegate.	An example of evidence may include, but is not limited to, records of implementation of mitigations.

R3. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-6 Table R3 – Malicious Code Prevention*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations].*

M3. Evidence must include each of the documented processes that collectively include each of the applicable requirement parts in *CIP-007-6 Table R3 – Malicious Code Prevention* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-6 Table R3 – Malicious Code Prevention			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Deploy method(s) to deter, detect, or prevent malicious code.	An example of evidence may include, but is not limited to, records of the Responsible Entity's performance of these processes (e.g., through traditional antivirus, system hardening, policies, etc.).

CIP-007-6 Table R3 – Malicious Code Prevention			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Mitigate the threat of detected malicious code.	Examples of evidence may include, but are not limited to: • Records of response processes for malicious code detection • Records of the performance of these processes when malicious code is detected.
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For those methods identified in Part 3.1 that use signatures or patterns, have a process for the update of the signatures or patterns. The process must address testing and installing the signatures or patterns.	An example of evidence may include, but is not limited to, documentation showing the process used for the update of signatures or patterns.

R4. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-6 Table R4 – Security Event Monitoring*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Assessment.]*

M4. Evidence must include each of the documented processes that collectively include each of the applicable requirement parts in *CIP-007-6 Table R4 – Security Event Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-6 Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Log events at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability) for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: 4.1.1. Detected successful login attempts; 4.1.2. Detected failed access attempts and failed login attempts; 4.1.3. Detected malicious code.	Examples of evidence may include, but are not limited to, a paper or system generated listing of event types for which the BES Cyber System is capable of detecting and, for generated events, is configured to log. This listing must include the required types of events.

CIP-007-6 Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Generate alerts for security events that the Responsible Entity determines necessitates an alert, that includes, as a minimum, each of the following types of events (per Cyber Asset or BES Cyber System capability): 4.2.1. Detected malicious code from Part 4.1; and 4.2.2. Detected failure of Part 4.1 event logging.	Examples of evidence may include, but are not limited to, paper or system-generated listing of security events that the Responsible Entity determined necessitate alerts, including paper or system generated list showing how alerts are configured.

CIP-007-6 Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA	Where technically feasible, retain applicable event logs identified in Part 4.1 for at least the last 90 consecutive calendar days except under CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, documentation of the event log retention process and paper or system generated reports showing log retention configuration set at 90 days or greater.
4.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA	Review a summarization or sampling of logged events as determined by the Responsible Entity at intervals no greater than 15 calendar days to identify undetected Cyber Security Incidents.	Examples of evidence may include, but are not limited to, documentation describing the review, any findings from the review (if any), and dated documentation showing the review occurred.

R5. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-6 Table R5 – System Access Controls*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M5. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-007-6 Table 5 – System Access Controls* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-6 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Have a method(s) to enforce authentication of interactive user access, where technically feasible.	An example of evidence may include, but is not limited to, documentation describing how access is authenticated.

CIP-007-6 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Identify and inventory all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s).	An example of evidence may include, but is not limited to, a listing of accounts by account types showing the enabled or generic account types in use for the BES Cyber System.

CIP-007-6 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Identify individuals who have authorized access to shared accounts.	An example of evidence may include, but is not limited to, listing of shared accounts and the individuals who have authorized access to each shared account.

CIP-007-6 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Change known default passwords, per Cyber Asset capability	Examples of evidence may include, but are not limited to: • Records of a procedure that passwords are changed when new devices are in production; or • Documentation in system manuals or other vendor documents showing default vendor passwords were generated pseudo-randomly and are thereby unique to the device.

CIP-007-6 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.5	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For password-only authentication for interactive user access, either technically or procedurally enforce the following password parameters: 5.5.1. Password length that is, at least, the lesser of eight characters or the maximum length supported by the Cyber Asset; and 5.5.2. Minimum password complexity that is the lesser of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the Cyber Asset.	Examples of evidence may include, but are not limited to: • System-generated reports or screen-shots of the system-enforced password parameters, including length and complexity; or • Attestations that include a reference to the documented procedures that were followed.

CIP-007-6 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.6	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Where technically feasible, for password-only authentication for interactive user access, either technically or procedurally enforce password changes or an obligation to change the password at least once every 15 calendar months.	Examples of evidence may include, but are not limited to: • System-generated reports or screen-shots of the system-enforced periodicity of changing passwords; or • Attestations that include a reference to the documented procedures that were followed.

CIP-007-6 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.7	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA	Where technically feasible, either: • Limit the number of unsuccessful authentication attempts; or • Generate alerts after a threshold of unsuccessful authentication attempts.	Examples of evidence may include, but are not limited to: • Documentation of the account-lockout parameters; or • Rules in the alerting configuration showing how the system notified individuals after a determined number of unsuccessful login attempts.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Same Day Operations**	**Medium**	N/A	The Responsible Entity has implemented and documented processes for Ports and Services but had no methods to protect against unnecessary physical input/output ports used for network connectivity, console commands, or Removable Media. (1.2)	The Responsible Entity has implemented and documented processes for determining necessary Ports and Services but, where technically feasible, had one or more unneeded logical network accessible ports enabled. (1.1)	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-6 Table R1. (R1)
R2	**Operations Planning**	**Medium**	The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for	The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes,	The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes for	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			applicability but did not evaluate the security patches for applicability within 35 calendar days but less than 50 calendar days of the last evaluation for the source or sources identified. (2.2) OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an	including the identification of sources, for tracking or evaluating cyber security patches for applicable Cyber Assets. (2.1) OR The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within 50 calendar days but less than 65 calendar days of the last evaluation for the source or	installing cyber security patches for applicable Cyber Assets. (2.1) OR The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within 65 calendar days of the last evaluation for the source or sources identified. (2.2) OR The Responsible Entity has one or more documented	CIP-007-6 Table R2. (R2) OR The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes for tracking, evaluating, or installing cyber security patches for applicable Cyber Assets. (2.1) OR The Responsible Entity documented a mitigation plan for an applicable cyber security patch and documented a revision or extension to the timeframe but did

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			existing mitigation plan within 35 calendar days but less than 50 calendar days of the evaluation completion. (2.3)	sources identified. (2.2) OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 50 calendar days but less than 65 calendar days of the evaluation completion. (2.3)	process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 65 calendar days of the evaluation completion. (2.3)	not obtain approval by the CIP Senior Manager or delegate. (2.4) OR The Responsible Entity documented a mitigation plan for an applicable cyber security patch but did not implement the plan as created or revised within the timeframe specified in the plan. (2.4)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R3	**Same Day Operations**	**Medium**	N/A	The Responsible Entity has implemented one or more documented process(es), but, where signatures or patterns are used, the Responsible Entity did not address testing the signatures or patterns. (3.3)	The Responsible Entity has implemented one or more documented process(es) for malicious code prevention but did not mitigate the threat of detected malicious code. (3.2) OR The Responsible Entity has implemented one or more documented process(es) for malicious code prevention, but where signatures or patterns are used, the Responsible Entity did not update malicious code protections. (3.3).	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-6 Table R3. (R3). OR The Responsible Entity has implemented one or more documented process(es) for malicious code prevention but did not deploy method(s) to deter, detect, or prevent malicious code. (3.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R4	**Same Day Operations and Operations Assessment**	**Medium**	The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged events at least every 15 calendar days but missed an interval and completed the review within 22 calendar days of the prior review. (4.4)	The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged events at least every 15 calendar days but missed an interval and completed the review within 30 calendar days of the prior review. (4.4)	The Responsible Entity has documented and implemented one or more process(es) to generate alerts for necessary security events (as determined by the responsible entity) for the Applicable Systems (per device or system capability) but did not generate alerts for all of the required types of events described in 4.2.1 through 4.2.2. (4.2) OR The Responsible Entity has documented and implemented one or more process(es) to log applicable events identified in	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-6 Table R4. (R4) OR The Responsible Entity has documented and implemented one or more process(es) to log events for the Applicable Systems (per device or system capability) but did not detect and log all of the required types of events described in 4.1.1 through 4.1.3. (4.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					4.1 (where technically feasible and except during CIP Exceptional Circumstances) but did not retain applicable event logs for at least the last 90 consecutive days. (4.3) OR The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged events at least every 15 calendar days but	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					missed two or more intervals. (4.4)	
R5	**Operations Planning**	**Medium**	The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 15 calendar months but less than or equal to 16 calendar months of the last password change. (5.6)	The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 16 calendar months but less than or equal to 17 calendar months of the last password change. (5.6)	The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, did not include the identification or inventory of all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s). (5.2) OR The Responsible Entity has implemented one or more documented process(es) for	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-6 Table R5. (R5) OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, where technically feasible, does not have a method(s) to enforce authentication of interactive user access. (5.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					System Access Controls but, did not include the identification of the individuals with authorized access to shared accounts. (5.3) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access that did not technically or procedurally enforce one of the two password parameters as described in 5.5.1 and 5.5.2. (5.5) OR	OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, where technically feasible, does not have a method(s) to enforce authentication of interactive user access. (5.1) OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but did not, per device capability, change

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access that did not technically or procedurally enforce one of the two password parameters as described in 5.5.1 and 5.5.2. (5.5) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or	known default passwords. (5.4) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but the Responsible Entity did not technically or procedurally enforce all of the password parameters described in 5.5.1 and 5.5.2. (5.5) OR The Responsible Entity has implemented one or more documented process(es) for

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					procedurally enforce password changes or an obligation to change the password within 17 calendar months but less than or equal to 18 calendar months of the last password change. (5.6)	password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 18 calendar months of the last password change. (5.6) OR The Responsible Entity has implemented one or more documented process(es) for System Access Control but, where technically feasible, did not either limit the number of unsuccessful authentication attempts or

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						generate alerts after a threshold of unsuccessful authentication attempts. (5.7)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	

Version	Date	Action	Change Tracking
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-007-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
6	2/15/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
6	1/21/16	FERC order issued approving CIP-007-6. Docket No. RM15-14-000	

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

Requirement R1 exists to reduce the attack surface of Cyber Assets by requiring entities to disable known unnecessary ports. The SDT intends for the entity to know what network accessible ("listening") ports and associated services are accessible on their assets and systems, whether they are needed for that Cyber Asset's function, and disable or restrict access to all other ports.

1.1. This requirement is most often accomplished by disabling the corresponding service or program that is listening on the port or configuration settings within the Cyber Asset. It can also be accomplished through using host-based firewalls, TCP_Wrappers, or other means on the Cyber Asset to restrict access. Note that the requirement is applicable at the Cyber Asset level. The Cyber Assets are those which comprise the applicable BES Cyber Systems and their associated Cyber Assets. This control is another layer in the defense against network-based attacks, therefore the SDT intends that the control be on the device itself, or positioned inline in a non-bypassable manner. Blocking ports at the ESP border does not substitute for this device level requirement. If a device has no provision for disabling or restricting logical ports on the device (example - purpose built devices that run from firmware with no port configuration available) then those ports that are open are deemed 'needed.'

1.2. Examples of physical I/O ports include network, serial and USB ports external to the device casing. BES Cyber Systems should exist within a Physical Security Perimeter in which case the physical I/O ports have protection from unauthorized access, but it may still be possible for accidental use such as connecting a modem, connecting a network cable that bridges networks, or inserting a USB drive. Ports used for 'console commands' primarily means serial ports on Cyber Assets that provide an administrative interface.

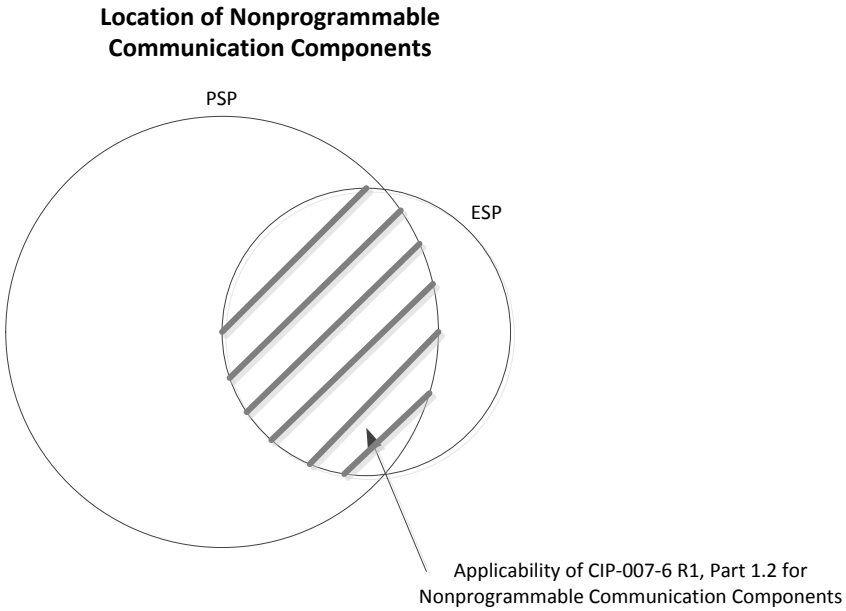
The protection of these ports can be accomplished in several ways including, but not limited to:

- Disabling all unneeded physical ports within the Cyber Asset's configuration
- Prominent signage, tamper tape, or other means of conveying that the ports should not be used without proper authorization
- Physical port obstruction through removable locks

The network ports included in the scope of this requirement part are not limited to those on the BES Cyber System itself. The scope of physical network ports includes those ports that may exist on nonprogrammable devices such as unmanaged switches, hubs, or patch panels.

This is a 'defense in depth' type control and it is acknowledged that there are other layers of control (the PSP for one) that prevent unauthorized personnel from gaining physical access to these ports. Even with physical access, it has been pointed out there are other ways to circumvent the control. This control, with its inclusion of means such as signage, is not meant to be a preventative control against intruders. Signage is indeed a directive control, not a preventative one. However, with a defense-in-depth posture, different layers and types of controls are required throughout the standard with this providing another layer for depth in Control Center environments. Once physical access has been achieved through the other preventative and detective measures by authorized personnel, a directive control that outlines proper behavior as a last line of defense is appropriate in these highest risk areas. In essence, signage would be used to remind authorized users to "think before you plug anything into one of these systems" which is the intent. This control is not designed primarily for intruders, but for example the authorized employee who intends to plug his possibly infected smartphone into an operator console USB port to charge the battery.

The Applicable Systems column was updated on CIP-007-6 Requirement 1, Part 1.2 to include "Nonprogrammable communication components located inside both a PSP and an ESP." This should be interpreted to apply to only those nonprogrammable communication components that are inside both an ESP and a PSP in combination, not those components that are in only one perimeter as can be illustrated in the following diagram:



Requirement R2:

The SDT's intent of Requirement R2 is to require entities to know, track, and mitigate the known software vulnerabilities associated with their BES Cyber Assets. It is not strictly an "install every security patch" requirement; the main intention is to "be aware of in a timely manner and manage all known vulnerabilities" requirement.

Patch management is required for BES Cyber Systems that are accessible remotely as well as standalone systems. Standalone systems are vulnerable to intentional or unintentional introduction of malicious code. A sound defense-in-depth security strategy employs additional measures such as physical security, malware prevention software, and software patch management to reduce the introduction of malicious code or the exploit of known vulnerabilities.

One or multiple processes could be utilized. An overall assessment process may exist in a top tier document with lower tier documents establishing the more detailed process followed for individual systems. Lower tier documents could be used to cover BES Cyber System nuances that may occur at the system level.

2.1. The Responsible Entity is to have a patch management program that covers tracking, evaluating, and installing cyber security patches. The requirement applies to patches only, which are fixes released to handle a specific vulnerability in a hardware or software product. The requirement covers only patches that involve cyber security fixes and does not cover patches that are purely functionality related with no cyber security impact. Tracking involves processes for notification of the availability of new cyber security patches for the Cyber Assets. Documenting the patch source in the tracking portion of the process is required to determine when the assessment timeframe clock starts. This requirement handles the situation where security patches can come from an original source (such as an operating system vendor), but must be approved or certified by another source (such as a control system vendor) before they

can be assessed and applied in order to not jeopardize the availability or integrity of the control system. The source can take many forms. The National Vulnerability Database, Operating System vendors, or Control System vendors could all be sources to monitor for release of security related patches, hotfixes, and/or updates. A patch source is not required for Cyber Assets that have no updateable software or firmware (there is no user accessible way to update the internal software or firmware executing on the Cyber Asset), or those Cyber Assets that have no existing source of patches such as vendors that no longer exist. The identification of these sources is intended to be performed once unless software is changed or added to the Cyber Asset's baseline.

2.2. Responsible Entities are to perform an assessment of security related patches within 35 days of release from their monitored source. An assessment should consist of determination of the applicability of each patch to the entity's specific environment and systems. Applicability determination is based primarily on whether the patch applies to a specific software or hardware component that the entity does have installed in an applicable Cyber Asset. A patch that applies to a service or component that is not installed in the entity's environment is not applicable. If the patch is determined to be non-applicable, that is documented with the reasons why and the entity is compliant. If the patch is applicable, the assessment can include a determination of the risk involved, how the vulnerability can be remediated, the urgency and timeframe of the remediation, and the steps the entity has previously taken or will take. Considerable care must be taken in applying security related patches, hotfixes, and/or updates or applying compensating measures to BES Cyber System or BES Cyber Assets that are no longer supported by vendors. It is possible security patches, hotfixes, and updates may reduce the reliability of the system, and entities should take this into account when determining the type of mitigation to apply. The Responsible Entities can use the information provided in the Department of Homeland Security "Quarterly Report on Cyber Vulnerabilities of Potential Risk to Control Systems" as a source. The DHS document "Recommended Practice for Patch Management of Control Systems" provides guidance on an evaluative process. It uses severity levels determined using the Common Vulnerability Scoring System Version 2. Determination that a security related patch, hotfix, and/or update poses too great a risk to install on a system or is not applicable due to the system configuration should not require a TFE.

When documenting the remediation plan measures it may not be necessary to document them on a one to one basis. The remediation plan measures may be cumulative. A measure to address a software vulnerability may involve disabling a particular service. That same service may be exploited through other software vulnerabilities. Therefore disabling the single service has addressed multiple patched vulnerabilities.

2.3. The requirement handles the situations where it is more of a reliability risk to patch a running system than the vulnerability presents. In all cases, the entity either installs the patch or documents (either through the creation of a new or update of an existing mitigation plan) what they are going to do to mitigate the vulnerability and when they are going to do so. There are times when it is in the best interest of reliability to not install a patch, and the entity can document what they have done to mitigate the vulnerability. For those security related patches that are determined to be applicable, the Responsible Entity must within 35 days either install the patch, create a dated mitigation plan which will outline the actions to be taken or

those that have already been taken by the Responsible Entity to mitigate the vulnerabilities addressed by the security patch, or revise an existing mitigation plan. Timeframes do not have to be designated as a particular calendar day but can have event designations such as “at next scheduled outage of at least two days duration.” “Mitigation plans” in the standard refers to internal documents and are not to be confused with plans that are submitted to Regional Entities in response to violations.

2.4. The entity has been notified of, has assessed, and has developed a plan to remediate the known risk and that plan must be implemented. Remediation plans that only include steps that have been previously taken are considered implemented upon completion of the documentation. Remediation plans that have steps to be taken to remediate the vulnerability must be implemented by the timeframe the entity documented in their plan. There is no maximum timeframe in this requirement as patching and other system changes carries its own risk to the availability and integrity of the systems and may require waiting until a planned outage. In periods of high demand or threatening weather, changes to systems may be curtailed or denied due to the risk to reliability.

Requirement R3:

3.1. Due to the wide range of equipment comprising the BES Cyber Systems and the wide variety of vulnerability and capability of that equipment to malware as well as the constantly evolving threat and resultant tools and controls, it is not practical within the standard to prescribe how malware is to be addressed on each Cyber Asset. Rather, the Responsible Entity determines on a BES Cyber System basis which Cyber Assets have susceptibility to malware intrusions and documents their plans and processes for addressing those risks and provides evidence that they follow those plans and processes. There are numerous options available including traditional antivirus solutions for common operating systems, white-listing solutions, network isolation techniques, Intrusion Detection/Prevention (IDS/IPS) solutions, etc. If an entity has numerous BES Cyber Systems or Cyber Assets that are of identical architecture, they may provide one process that describes how all the like Cyber Assets are covered. If a specific Cyber Asset has no updateable software and its executing code cannot be altered, then that Cyber Asset is considered to have its own internal method of deterring malicious code.

3.2. When malicious code is detected on a Cyber Asset within the applicability of this requirement, the threat posed by that code must be mitigated. In situations where traditional antivirus products are used, they may be configured to automatically remove or quarantine the malicious code. In white-listing situations, the white-listing tool itself can mitigate the threat as it will not allow the code to execute, however steps should still be taken to remove the malicious code from the Cyber Asset. In some instances, it may be in the best interest of reliability to not immediately remove or quarantine the malicious code, such as when availability of the system may be jeopardized by removal while operating and a rebuild of the system needs to be scheduled. In that case, monitoring may be increased and steps taken to insure the malicious code cannot communicate with other systems. In some instances the entity may be working with law enforcement or other governmental entities to closely monitor the code and track the perpetrator(s). For these reasons, there is no maximum timeframe or

method prescribed for the removal of the malicious code, but the requirement is to mitigate the threat posed by the now identified malicious code.

Entities should also have awareness of malware protection requirements for Transient Cyber Assets and Removable Media ("transient devices") in CIP-010-2. The protections required here in CIP-007-6, Requirement R3 complement, but do not meet, the additional obligations for transient devices.

3.3. In instances where malware detection technologies depend on signatures or patterns of known attacks, the effectiveness of these tools against evolving threats is tied to the ability to keep these signatures and patterns updated in a timely manner. The entity is to have a documented process that includes the testing and installation of signature or pattern updates. In a BES Cyber System, there may be some Cyber Assets that would benefit from the more timely installation of the updates where availability of that Cyber Asset would not jeopardize the availability of the BES Cyber System's ability to perform its function. For example, some HMI workstations where portable media is utilized may benefit from having the very latest updates at all times with minimal testing. Other Cyber Assets should have any updates thoroughly tested before implementation where the result of a 'false positive' could harm the availability of the BES Cyber System. The testing should not negatively impact the reliability of the BES. The testing should be focused on the update itself and if it will have an adverse impact on the BES Cyber System. Testing in no way implies that the entity is testing to ensure that malware is indeed detected by introducing malware into the environment. It is strictly focused on ensuring that the update does not negatively impact the BES Cyber System before those updates are placed into production.

Requirement R4:

Refer to NIST 800-92 and 800-137 for additional guidance in security event monitoring.

4.1. In a complex computing environment and faced with dynamic threats and vulnerabilities, it is not practical within the standard to enumerate all security-related events necessary to support the activities for alerting and incident response. Rather, the Responsible Entity determines which computer generated events are necessary to log, provide alerts and monitor for their particular BES Cyber System environment.

Specific security events already required in Version 4 of the CIP Standards carry forward in this version. This includes access attempts at the Electronic Access Points, if any have been identified for a BES Cyber Systems. Examples of access attempts include: (i) blocked network access attempts, (ii) successful and unsuccessful remote user access attempts, (iii) blocked network access attempts from a remote VPN, and (iv) successful network access attempts or network flow information.

User access and activity events include those events generated by Cyber Assets within the Electronic Security Perimeter that have access control capability. These types of events include: (i) successful and unsuccessful authentication, (ii) account management, (iii) object access, and (iv) processes started and stopped.

It is not the intent of the SDT that if a device cannot log a particular event that a TFE must be generated. The SDT's intent is that if any of the items in the bulleted list (for example, user logouts) can be logged by the device then the entity must log that item. If the device does not have the capability of logging that event, the entity remains compliant.

4.2. Real-time alerting allows the cyber system to automatically communicate events of significance to designated responders. This involves configuration of a communication mechanism and log analysis rules. Alerts can be configured in the form of an email, text message, or system display and alarming. The log analysis rules can exist as part of the operating system, specific application or a centralized security event monitoring system. On one end, a real-time alert could consist of a set point on an RTU for a login failure, and on the other end, a security event monitoring system could provide multiple alerting communications options triggered on any number of complex log correlation rules.

The events triggering a real-time alert may change from day to day as system administrators and incident responders better understand the types of events that might be indications of a cyber-security incident. Configuration of alerts also must balance the need for responders to know an event occurred with the potential inundation of insignificant alerts. The following list includes examples of events a Responsible Entity should consider in configuring real-time alerts:

- Detected known or potential malware or malicious activity
- Failure of security event logging mechanisms
- Login failures for critical accounts
- Interactive login of system accounts
- Enabling of accounts
- Newly provisioned accounts
- System administration or change tasks by an unauthorized user
- Authentication attempts on certain accounts during non-business hours
- Unauthorized configuration changes
- Insertion of Removable Media in violation of a policy

4.3 Logs that are created under Part 4.1 are to be retained on the applicable Cyber Assets or BES Cyber Systems for at least 90 days. This is different than the evidence retention period called for in the CIP standards used to prove historical compliance. For such audit purposes, the entity should maintain evidence that shows that 90 days were kept historically. One example would be records of disposition of event logs beyond 90 days up to the evidence retention period.

4.4. Reviewing logs at least every 15 days (approximately every two weeks) can consist of analyzing a summarization or sampling of logged events. NIST SP800-92 provides a lot of guidance in periodic log analysis. If a centralized security event monitoring system is used, log analysis can be performed top-down starting with a review of trends from summary reports. The log review can also be an extension of the exercise in identifying those events needing real-

time alerts by analyzing events that are not fully understood or could possibly inundate the real-time alerting.

Requirement R5:

Account types referenced in this guidance typically include:

- Shared user account: An account used by multiple users for normal business functions by employees or contractors. Usually on a device that does not support Individual User Accounts.
- Individual user account: An account used by a single user.
- Administrative account: An account with elevated privileges for performing administrative or other specialized functions. These can be individual or shared accounts.
- System account: Accounts used to run services on a system (web, DNS, mail etc.). No users have access to these accounts.
- Application account: A specific system account, with rights granted at the application level often used for access into a Database.
- Guest account: An individual user account not typically used for normal business functions by employees or contractors and not associated with a specific user. May or may not be shared by multiple users.
- Remote access account: An individual user account only used for obtaining Interactive Remote Access to the BES Cyber System.
- Generic account: A group account set up by the operating system or application to perform specific operations. This differs from a shared user account in that individual users do not receive authorization for access to this account type.

5.1 Reference the Requirement's rationale.

5.2 Where possible, default and other generic accounts provided by a vendor should be removed, renamed, or disabled prior to production use of the Cyber Asset or BES Cyber System. If this is not possible, the passwords must be changed from the default provided by the vendor. Default and other generic accounts remaining enabled must be documented. For common configurations, this documentation can be performed at a BES Cyber System or more general level.

5.3 Entities may choose to identify individuals with access to shared accounts through the access authorization and provisioning process, in which case the individual authorization records suffice to meet this Requirement Part. Alternatively, entities may choose to maintain a separate listing for shared accounts. Either form of evidence achieves the end result of maintaining control of shared accounts.

5.4. Default passwords can be commonly published in vendor documentation that is readily available to all customers using that type of equipment and possibly published online.

The requirement option to have unique password addresses cases where the Cyber Asset generates or has assigned pseudo-random default passwords at the time of production or installation. In these cases, the default password does not have to change because the system or manufacturer created it specific to the Cyber Asset.

5.5. Interactive user access does not include read-only information access in which the configuration of the Cyber Asset cannot change (e.g. front panel displays, web-based reports, etc.). For devices that cannot technically or for operational reasons perform authentication, an entity may demonstrate all interactive user access paths, both remote and local, are configured for authentication. Physical security suffices for local access configuration if the physical security can record who is in the Physical Security Perimeter and at what time.

Technical or procedural enforcement of password parameters are required where passwords are the only credential used to authenticate individuals. Technical enforcement of the password parameters means a Cyber Asset verifies an individually selected password meets the required parameters before allowing the account to authenticate with the selected password. Technical enforcement should be used in most cases when the authenticating Cyber Asset supports enforcing password parameters. Likewise, procedural enforcement means requiring the password parameters through procedures. Individuals choosing the passwords have the obligation of ensuring the password meets the required parameters.

Password complexity refers to the policy set by a Cyber Asset to require passwords to have one or more of the following types of characters: (1) lowercase alphabetic, (2) uppercase alphabetic, (3) numeric, and (4) non-alphanumeric or “special” characters (e.g. #, $, @, &), in various combinations.

5.6 Technical or procedural enforcement of password change obligations are required where passwords are the only credential used to authenticate individuals. Technical enforcement of password change obligations means the Cyber Asset requires a password change after a specified timeframe prior to allowing access. In this case, the password is not required to change by the specified time as long as the Cyber Asset enforces the password change after the next successful authentication of the account. Procedural enforcement means manually changing passwords used for interactive user access after a specified timeframe.

5.7 Configuring an account lockout policy or alerting after a certain number of failed authentication attempts serves to prevent unauthorized access through an online password guessing attack. The threshold of failed authentication attempts should be set high enough to avoid false-positives from authorized users failing to authenticate. It should also be set low enough to account for online password attacks occurring over an extended period of time. This threshold may be tailored to the operating environment over time to avoid unnecessary account lockouts.

Entities should take caution when configuring account lockout to avoid locking out accounts necessary for the BES Cyber System to perform a BES reliability task. In such cases, entities should configure authentication failure alerting.

Rationale:

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for Requirement R1:

The requirement is intended to minimize the attack surface of BES Cyber Systems through disabling or limiting access to unnecessary network accessible logical ports and services and physical I/O ports.

In response to FERC Order No. 791, specifically FERC's reference to NIST 800-53 rev. 3 security control PE-4 in paragraph 149, Part 1.2 has been expanded to include PCAs and nonprogrammable communications components. This increase in applicability expands the scope of devices that receive the protection afforded by the defense-in-depth control included in Requirement R1, Part 1.2.

The applicability is limited to those nonprogrammable communications components located both inside a PSP and an ESP in order to allow for a scenario in which a Responsible Entity may implement an extended ESP (with corresponding logical protections identified in CIP-006, Requirement R1, Part 1.10). In this scenario, nonprogrammable components of the communication network may exist out of the Responsible Entity's control (i.e. as part of the telecommunication carrier's network).

Rationale for Requirement R2:

Security patch management is a proactive way of monitoring and addressing known security vulnerabilities in software before those vulnerabilities can be exploited in a malicious manner to gain control of or render a BES Cyber Asset or BES Cyber System inoperable.

Rationale for Requirement R3:

Malicious code prevention has the purpose of limiting and detecting the addition of malicious code onto the applicable Cyber Assets of a BES Cyber System. Malicious code (viruses, worms, botnets, targeted code such as Stuxnet, etc.) may compromise the availability or integrity of the BES Cyber System.

Rationale for Requirement R4:

Security event monitoring has the purpose of detecting unauthorized access, reconnaissance and other malicious activity on BES Cyber Systems, and comprises of the activities involved with the collection, processing, alerting and retention of security-related computer logs. These logs can provide both (1) the detection of an incident and (2) useful evidence in the investigation of an incident. The retention of security-related logs is intended to support post-event data analysis.

Audit processing failures are not penalized in this requirement. Instead, the requirement specifies processes which must be in place to monitor for and notify personnel of audit processing failures.

Rationale for Requirement R5:

To help ensure that no authorized individual can gain electronic access to a BES Cyber System until the individual has been authenticated, i.e., until the individual's logon credentials have been validated. Requirement R5 also seeks to reduce the risk that static passwords, where used as authenticators, may be compromised.

Requirement Part 5.1 ensures the BES Cyber System or Cyber Asset authenticates individuals that can modify configuration information. This requirement addresses the configuration of authentication. The authorization of individuals is addressed elsewhere in the CIP Cyber Security Standards. Interactive user access does not include read-only information access in which the configuration of the Cyber Asset cannot change (e.g. front panel displays, web-based reports, etc.). For devices that cannot technically or for operational reasons perform authentication, an entity may demonstrate all interactive user access paths, both remote and local, are configured for authentication. Physical security suffices for local access configuration if the physical security can record who is in the Physical Security Perimeter and at what time.

Requirement Part 5.2 addresses default and other generic account types. Identifying the use of default or generic account types that could introduce vulnerabilities has the benefit ensuring entities understand the possible risk these accounts pose to the BES Cyber System. The Requirement Part avoids prescribing an action to address these accounts because the most effective solution is situation specific, and in some cases, removing or disabling the account could have reliability consequences.

Requirement Part 5.3 addresses identification of individuals with access to shared accounts. This Requirement Part has the objective of mitigating the risk of unauthorized access through shared accounts. This differs from other CIP Cyber Security Standards Requirements to authorize access. An entity can authorize access and still not know who has access to a shared account. Failure to identify individuals with access to shared accounts would make it difficult to revoke access when it is no longer needed. The term “authorized” is used in the requirement to make clear that individuals storing, losing, or inappropriately sharing a password is not a violation of this requirement.

Requirement 5.4 addresses default passwords. Changing default passwords closes an easily exploitable vulnerability in many systems and applications. Pseudo-randomly system generated passwords are not considered default passwords.

For password-based user authentication, using strong passwords and changing them periodically helps mitigate the risk of successful password cracking attacks and the risk of accidental password disclosure to unauthorized individuals. In these requirements, the drafting team considered multiple approaches to ensuring this requirement was both effective and flexible enough to allow Responsible Entities to make good security decisions. One of the approaches considered involved requiring minimum password entropy, but the calculation for true information entropy is more highly complex and makes several assumptions in the passwords users choose. Users can pick poor passwords well below the calculated minimum entropy.

The drafting team also chose to not require technical feasibility exceptions for devices that cannot meet the length and complexity requirements in password parameters. The objective of this requirement is to apply a measurable password policy to deter password cracking attempts, and replacing devices to achieve a specified password policy does not meet this objective. At the same time, this requirement has been strengthened to require account lockout or alerting for failed login attempts, which in many instances better meets the requirement objective.

The requirement to change passwords exists to address password cracking attempts if an encrypted password were somehow attained and also to refresh passwords which may have been accidentally disclosed over time. The requirement permits the entity to specify the periodicity of change to accomplish this objective. Specifically, the drafting team felt determining the appropriate periodicity based on a number of factors is more effective than specifying the period for every BES Cyber System in the Standard. In general, passwords for user authentication should be changed at least annually. The periodicity may increase in some cases. For example, application passwords that are long and pseudo-randomly generated could have a very long periodicity. Also, passwords used only as a weak form of application authentication, such as accessing the configuration of a relay may only need to be changed as part of regularly scheduled maintenance.

The Cyber Asset should automatically enforce the password policy for individual user accounts. However, for shared accounts in which no mechanism exists to enforce password policies, the Responsible Entity can enforce the password policy procedurally and through internal assessment and audit.

Requirement Part 5.7 assists in preventing online password attacks by limiting the number of guesses an attacker can make. This requirement allows either limiting the number of failed authentication attempts or alerting after a defined number of failed authentication attempts. Entities should take caution in choosing to limit the number of failed authentication attempts for all accounts because this would allow the possibility for a denial of service attack on the BES Cyber System.

Appendix QC-CIP-007-6
Provisions specific to the standard CIP-007-6 applicable in Québec

This appendix establishes specific provisions for the application of the standard in Québec. Provisions of the standard and of its appendix must be read together for the purposes of understanding and interpretation. Where the standard and appendix differ, the appendix shall prevail.

A. Introduction

1. **Title:** Cyber Security — System Security Management

2. **Number:** CIP-007-6

3. **Purpose:** No specific provision

4. **Applicability:**

   4.1. Functional Entities

   No specific provision

   4.2. Facilities

   This standard only applies to the facilities of the Main Transmission System (RTP) and to the facilities specified for the Distribution Provider. In the application of this standard, all reference to the terms "Bulk Electric System" or "BES" shall be replaced by the terms "Main Transmission System" or "RTP" respectively.

   Additional Exemptions

   The following are exempt from this standard:

   - Any generating facility that meets the two following conditions: (1) the nameplate capacity of the facility is 300 MVA or less, and (2) no unit of the facility can be synchronized with a neighbouring system.
   - Step-up substations of generating facilities identified in the preceding point.

5. **Effective Date:**

   5.1. Adoption of the standard by the Régie de l'énergie: October 31st, 2017

   5.2. Adoption of the appendix by the Régie de l'énergie: October 31st, 2017

   5.3. Effective date of the standard and its appendix in Québec: January 1st, 2018

Standard	Implementation date for Québec		
	Entities subject to version 1 of the CIP standards adopted by the Régie	Entities exempted from the application of version 1 of the CIP standards under the specific provisions associated with these standards	Entities that have generation facilities for industrial use
CIP-007-6	January 1st, 2018	October 1st, 2018	April 1st, 2019

6. Background:

No specific provision

B. Requirements and Measures

No specific provision

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

The Régie de l'énergie is responsible, in Québec, for compliance enforcement with respect to the reliability standard and its appendix that it adopts.

1.2. Evidence Retention

No specific provision

1.3. Compliance Monitoring and Assessment Processes

No specific provision

1.4. Additional Compliance Information

No specific provision

2. Table of Compliance Elements

No specific provision

D. Regional Variances

No specific provision

E. Interpretations

No specific provision

F. Associated Documents

No specific provision

Guidelines and Technical Basis

No specific provision

Rationale

No specific provision

Version History

Revision	Date	Action	Change Tracking
0	October 31st, 2017	New appendix	New

A. Introduction

1. Title: Cyber Security — Incident Reporting and Response Planning

2. Number: CIP-008-6

3. Purpose: To mitigate the risk to the reliable operation of the BES as the result of a Cyber Security Incident by specifying incident response requirements.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Remedial Action Scheme where the Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Reliability Coordinator

4.1.6 Transmission Operator

4.1.7 Transmission Owner

4.2. **Facilities:** For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Remedial Action Scheme where the Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-008-6:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002 identification and categorization processes.

5. Effective Dates:
See Implementation Plan for CIP-008-6.

6. Background:
Standard CIP-008 exists as part of a suite of CIP Standards related to cyber security. CIP-002 requires the initial identification and categorization of BES Cyber Systems. CIP-003, CIP-004, CIP-005, CIP-006, CIP-007, CIP-008, CIP-009, CIP-010, and CIP-011 require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a particular subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:
Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems –** Applies to BES Cyber Systems categorized as high impact according to the CIP-002 identification and categorization processes.
- **Medium Impact BES Cyber Systems –** Applies to BES Cyber Systems categorized as medium impact according to the CIP-002 identification and categorization processes.

B. Requirements and Measures

R1. Each Responsible Entity shall document one or more Cyber Security Incident response plan(s) that collectively include each of the applicable requirement parts in *CIP-008-6 Table R1 – Cyber Security Incident Response Plan Specifications*. *[Violation Risk Factor: Lower] [Time Horizon: Long Term Planning].*

M1. Evidence must include each of the documented plan(s) that collectively include each of the applicable requirement parts in *CIP-008-6 Table R1 – Cyber Security Incident Response Plan Specifications*.

CIP-008-6 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	One or more processes to identify, classify, and respond to Cyber Security Incidents.	An example of evidence may include, but is not limited to, dated documentation of Cyber Security Incident response plan(s) that include the process(es) to identify, classify, and respond to Cyber Security Incidents.

CIP-008-6 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	One or more processes: 1.2.1 That include criteria to evaluate and define attempts to compromise; 1.2.2 To determine if an identified Cyber Security Incident is: • A Reportable Cyber Security Incident; or • An attempt to compromise, as determined by applying the criteria from Part 1.2.1, one or more systems identified in the "Applicable Systems" column for this Part; and 1.2.3 To provide notification per Requirement R4.	Examples of evidence may include, but are not limited to, dated documentation of Cyber Security Incident response plan(s) that provide guidance or thresholds for determining which Cyber Security Incidents are also Reportable Cyber Security Incidents or a Cyber Security Incident that is determined to be an attempt to compromise a system identified in the "Applicable Systems" column including justification for attempt determination criteria and documented processes for notification.

CIP-008-6 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	The roles and responsibilities of Cyber Security Incident response groups or individuals.	An example of evidence may include, but is not limited to, dated Cyber Security Incident response process(es) or procedure(s) that define roles and responsibilities (e.g., monitoring, reporting, initiating, documenting, etc.) of Cyber Security Incident response groups or individuals.
1.4	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	Incident handling procedures for Cyber Security Incidents.	An example of evidence may include, but is not limited to, dated Cyber Security Incident response process(es) or procedure(s) that address incident handling (e.g., containment, eradication, recovery/incident resolution).

R2. Each Responsible Entity shall implement each of its documented Cyber Security Incident response plans to collectively include each of the applicable requirement parts in *CIP-008-6 Table R2 – Cyber Security Incident Response Plan Implementation and Testing. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Real-Time Operations].*

M2. Evidence must include, but is not limited to, documentation that collectively demonstrates implementation of each of the applicable requirement parts in *CIP-008-6 Table R2 – Cyber Security Incident Response Plan Implementation and Testing*.

CIP-008-6 Table R2 – Cyber Security Incident Response Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	Test each Cyber Security Incident response plan(s) at least once every 15 calendar months: • By responding to an actual Reportable Cyber Security Incident; • With a paper drill or tabletop exercise of a Reportable Cyber Security Incident; or • With an operational exercise of a Reportable Cyber Security Incident.	Examples of evidence may include, but are not limited to, dated evidence of a lessons-learned report that includes a summary of the test or a compilation of notes, logs, and communication resulting from the test. Types of exercises may include discussion or operations based exercises.

CIP-008-6 Table R2 – Cyber Security Incident Response Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	Use the Cyber Security Incident response plan(s) under Requirement R1 when responding to a Reportable Cyber Security Incident, responding to a Cyber Security Incident that attempted to compromise a system identified in the "Applicable Systems" column for this Part, or performing an exercise of a Reportable Cyber Security Incident. Document deviations from the plan(s) taken during the response to the incident or exercise.	Examples of evidence may include, but are not limited to, incident reports, logs, and notes that were kept during the incident response process, and follow-up documentation that describes deviations taken from the plan during the incident response or exercise.
2.3	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	Retain records related to Reportable Cyber Security Incidents and Cyber Security Incidents that attempted to compromise a system identified in the "Applicable Systems" column for this Part as per the Cyber Security Incident response plan(s) under Requirement R1.	An example of evidence may include, but is not limited to, dated documentation, such as security logs, police reports, emails, response forms or checklists, forensic analysis results, restoration records, and post-incident review notes related to Reportable Cyber Security Incidents and a Cyber Security Incident that is determined to be an attempt to compromise a system identified in the "Applicable Systems" column.

R3. Each Responsible Entity shall maintain each of its Cyber Security Incident response plans according to each of the applicable requirement parts in *CIP-008-6 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].*

M3. Evidence must include, but is not limited to, documentation that collectively demonstrates maintenance of each Cyber Security Incident response plan according to the applicable requirement parts in *CIP-008-6 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication.*

CIP-008-6 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	No later than 90 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response: 3.1.1. Document any lessons learned or document the absence of any lessons learned; 3.1.2. Update the Cyber Security Incident response plan based on any documented lessons learned associated with the plan; and 3.1.3. Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates to the Cyber Security Incident response plan based on any documented lessons learned.	An example of evidence may include, but is not limited to, all of the following: 1. Dated documentation of post incident(s) review meeting notes or follow-up report showing lessons learned associated with the Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response or dated documentation stating there were no lessons learned; 2. Dated and revised Cyber Security Incident response plan showing any changes based on the lessons learned; and 3. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

CIP-008-6 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	No later than 60 calendar days after a change to the roles or responsibilities, Cyber Security Incident response groups or individuals, or technology that the Responsible Entity determines would impact the ability to execute the plan: 3.2.1. Update the Cyber Security Incident response plan(s); and 3.2.2. Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates.	An example of evidence may include, but is not limited to: 1. Dated and revised Cyber Security Incident response plan with changes to the roles or responsibilities, responders or technology; and 2. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

R4. Each Responsible Entity shall notify the Electricity Information Sharing and Analysis Center (E-ISAC) and, if subject to the jurisdiction of the United States, the United States National Cybersecurity and Communications Integration Center (NCCIC),[1] or their successors, of a Reportable Cyber Security Incident and a Cyber Security Incident that was an attempt to compromise, as determined by applying the criteria from Requirement R1, Part 1.2.1, a system identified in the "Applicable Systems" column, unless prohibited by law, in accordance with each of the applicable requirement parts in *CIP-008-6 Table R4 – Notifications and Reporting for Cyber Security Incidents*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].*

M4. Evidence must include, but is not limited to, documentation that collectively demonstrates notification of each determined Reportable Cyber Security Incident and a Cyber Security Incident that was an attempt to compromise a system identified in the "Applicable Systems" column according to the applicable requirement parts in *CIP-008-6 Table R4 – Notifications and Reporting for Cyber Security Incidents.*

CIP-008-6 Table R4 – Notifications and Reporting for Cyber Security Incidents			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	Initial notifications and updates shall include the following attributes, at a minimum, to the extent known: 4.1.1 The functional impact; 4.1.2 The attack vector used; and 4.1.3 The level of intrusion that was achieved or attempted.	Examples of evidence may include, but are not limited to, dated documentation of initial notifications and updates to the E-ISAC and NCCIC.

[1] The National Cybersecurity and Communications Integration Center (NCCIC) is the successor organization of the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). In 2017, NCCIC realigned its organizational structure and integrated like functions previously performed independently by the ICS-CERT and the United States Computer Emergency Readiness Team (US-CERT).

CIP-008-6 Table R4 – Notifications and Reporting for Cyber Security Incidents			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.2	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	After the Responsible Entity's determination made pursuant to documented process(es) in Requirement R1, Part 1.2, provide initial notification within the following timelines: • One hour after the determination of a Reportable Cyber Security Incident. • By the end of the next calendar day after determination that a Cyber Security Incident was an attempt to compromise a system identified in the "Applicable Systems" column for this Part.	Examples of evidence may include, but are not limited to, dated documentation of notices to the E-ISAC and NCCIC.
4.3	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	Provide updates, if any, within 7 calendar days of determination of new or changed attribute information required in Part 4.1.	Examples of evidence may include, but are not limited to, dated documentation of submissions to the E-ISAC and NCCIC.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:
The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:
The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information:
None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Long Term Planning**	**Lower**	N/A	N/A	The Responsible Entity has developed the Cyber Security Incident response plan(s), but the plan does not include the roles and responsibilities of Cyber Security Incident response groups or individuals. (1.3) OR The Responsible Entity has developed the Cyber Security Incident response plan(s), but the plan does not include incident handling procedures for Cyber Security Incidents. (1.4) OR The Responsible Entity has developed a Cyber	The Responsible Entity has not developed a Cyber Security Incident response plan with one or more processes to identify, classify, and respond to Cyber Security Incidents. (1.1) OR The Responsible Entity has developed a Cyber Security Incident response plan, but the plan does not include one or more processes to identify Reportable Cyber Security Incidents or a Cyber Security Incident that was an attempt to compromise, as determined by applying the criteria from Part 1.2.1, a system identified in

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					Security Incident response plan, but the plan does not include one or more processes to provide notification per Requirement R4. (1.2) OR The Responsible Entity has developed a Cyber Security Incident response plan, but the plan does not include one or more processes that include criteria to evaluate and define attempts to compromise. (1.2)	the "Applicable Systems" column for Part 1.2. (1.2)
R2	**Operations Planning** **Real-time Operations**	**Lower**	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 15 calendar months, not exceeding 16 calendar months between tests of the plan(s). (2.1)	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 16 calendar months, not exceeding 17 calendar months between tests of the plan(s). (2.1)	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 17 calendar months, not exceeding 18 calendar months between tests of the plan(s). (2.1)	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 18 calendar months between tests of the plan(s). (2.1) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					OR The Responsible Entity did not document deviations, if any, from the plan during a test or when a Reportable Cyber Security Incident or a Cyber Security Incident that was an attempt to compromise a system identified in the "Applicable Systems" column for Part 2.2 occurs. (2.2)	The Responsible Entity did not retain relevant records related to Reportable Cyber Security Incidents or Cyber Security Incidents that were an attempt to compromise a system identified in the "Applicable Systems" column for Part 2.3. (2.3)
R3	**Operations Assessment**	**Lower**	The Responsible Entity has not notified each person or group with a defined role in the Cyber Security Incident response plan of updates to the Cyber Security Incident response plan within greater than 90 but less than 120 calendar days of a test or actual incident	The Responsible Entity has not updated the Cyber Security Incident response plan based on any documented lessons learned within 90 and less than 120 calendar days of a test or actual incident response to a Reportable Cyber	The Responsible Entity has neither documented lessons learned nor documented the absence of any lessons learned within 90 and less than 120 calendar days of a test or actual incident response to a Reportable Cyber	The Responsible Entity has neither documented lessons learned nor documented the absence of any lessons learned within 120 calendar days of a test or actual incident response to a Reportable Cyber

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			response to a Reportable Cyber Security Incident. (3.1.3)	Security Incident. (3.1.2) OR The Responsible Entity has not notified each person or group with a defined role in the Cyber Security Incident response plan of updates to the Cyber Security Incident response plan within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.3) OR The Responsible Entity has not updated the Cyber Security Incident response plan(s) or notified each person or group with a defined role within 60 and less than 90 calendar days	Security Incident. (3.1.1) OR The Responsible Entity has not updated the Cyber Security Incident response plan based on any documented lessons learned within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.2) OR The Responsible Entity has not updated the Cyber Security Incident response plan(s) or notified each person or group with a defined role within 90 calendar days of any of the following changes that the responsible entity	Security Incident. (3.1.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (3.2) • Roles or responsibilities, or • Cyber Security Incident response groups or individuals, or • Technology changes.	determines would impact the ability to execute the plan: (3.2) • Roles or responsibilities, or • Cyber Security Incident response groups or individuals, or • Technology changes.	
R4	**Operations Assessment**	**Lower**	The Responsible Entity notified E-ISAC and NCCIC, or their successors, of a Cyber Security Incident that was an attempt to compromise a system identified in the "Applicable Systems" column for Part 4.2 but failed to notify or update E-ISAC or NCCIC, or their successors, within the	The Responsible Entity failed to notify E-ISAC or NCCIC, or their successors, of a Cyber Security Incident that was an attempt to compromise, as determined by applying the criteria from Requirement R1, Part 1.2.1, a system identified in the "Applicable Systems" column. (R4)	The Responsible Entity notified E-ISAC and NCCIC, or their successors, of a Reportable Cyber Security Incident but failed to notify or update E-ISAC or NCCIC, or their successors, within the timelines pursuant to Part 4.2. (4.2) OR	The Responsible Entity failed to notify E-ISAC and NCCIC, or their successors, of a Reportable Cyber Security Incident. (R4)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			timelines pursuant to Part 4.2. (4.2) OR The Responsible Entity notified E-ISAC and NCCIC, or their successors, of a Reportable Cyber Security Incident or a Cyber Security Incident that was an attempt to compromise a system identified in the "Applicable Systems" column for Part 4.3 but failed to report on one or more of the attributes within 7 days after determination of the attribute(s) not reported pursuant to Part 4.1. (4.3) OR The Responsible Entity notified E-ISAC and NCCIC, or their successors, of a		The Responsible Entity failed to notify E-ISAC or NCCIC, or their successors, of a Reportable Cyber Security Incident. (R4)	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Reportable Cyber Security Incident or a Cyber Security Incident that was an attempt to compromise a system identified in the "Applicable Systems" column for Part 4.1 but failed to report on one or more of the attributes after determination pursuant to Part 4.1. (4.1)			

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a Responsible Entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	Update
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-008-5.	
5	7/9/14	FERC Letter Order issued approving VRFs and VSLs revisions to certain CIP standards.	CIP-008-5 Requirement R2, VSL table under Severe, changed

Version	Date	Action	Change Tracking
			from 19 to 18 calendar months.
6	2/6/2019	Adopted by the NERC Board of Trustees.	Modified to address directives in FERC Order No. 848

Appendix CIP-008-6-QC-1

Specific provisions applicable in Québec for standard
CIP-008-6 — Cyber Security — Incident Reporting and Response Planning

This appendix establishes specific provisions for the application of the standard in Québec. Provisions of the standard and of this appendix must be read jointly for comprehension and interpretation purposes. Where the standard and appendix differ, the appendix shall prevail.

A. Introduction

1. Title: No specific provisions.

2. Number: No specific provisions.

3. Purpose: No specific provisions.

4. Applicability:

4.1. Functional Entities

No specific provisions.

4.2. Facilities

This standard only applies to the facilities of the Main Transmission System (RTP) and to the facilities specified for the Distribution Provider. In the application of this standard, all reference to the terms "Bulk Electric System" or "BES" shall be replaced by the terms "Main Transmission System" or "RTP" respectively.

Additional Exemptions

The following are exempt from this standard:

- Any generating facility that meets the two following conditions: (1) the nameplate capacity of the facility is 300 MVA or less, and (2) no unit of the facility can be synchronized with a neighbouring system.
- Step-up substations of generating facilities identified in the preceding point.

5. Effective Date:

5.1. Adoption of the standard by the Régie de l'énergie: Setpember 10, 2020

5.2. Adoption of the appendix by the Régie de l'énergie: September 10, 2020

5.3. Effective date of the standard and its appendix in Québec: October 1, 2022

6. Background: No specific provisions.

B. Requirements and Measures

No specific provisions.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

In Québec, "Compliance Enforcement Authority" means the Régie de l'énergie in its roles of monitoring and enforcing compliance with respect to the Reliability Standard and to this appendix.

1.2. Evidence Retention

No specific provisions.

1.3. Compliance Monitoring and Assessment Processes

The Régie de l'énergie establishes the monitoring processes used to evaluate data or information for the purpose of determining compliance or non-compliance with the Reliability Standard and with this appendix.

1.4. Additional Compliance Information

No specific provisions.

2. Table of Compliance Elements

No specific provisions.

D. Regional Variances

No specific provisions.

E. Interpretations

No specific provisions.

F. Associated Documents

No specific provisions.

Version History

Version	Date	Action	Change Tracking
1	September 10, 2020	New appendix	New
2	October 16, 2020	Improvements to layout of document.	Revised

A. Introduction

1. Title: Cyber Security — Recovery Plans for BES Cyber Systems

2. Number: CIP-009-6

3. Purpose: To recover reliability functions performed by BES Cyber Systems by specifying recovery plan requirements in support of the continued stability, operability, and reliability of the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-009-6:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

5. Effective Dates:

See Implementation Plan for CIP-009-6.

6. Background:

Standard CIP-009 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in their documented processes, but they must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show

documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to BES Cyber Systems located at a Control Center and categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.

B. Requirements and Measures

R1. Each Responsible Entity shall have one or more documented recovery plan(s) that collectively include each of the applicable requirement parts in *CIP-009-6 Table R1 – Recovery Plan Specifications*. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning].*

M1. Evidence must include the documented recovery plan(s) that collectively include the applicable requirement parts in *CIP-009-6 Table R1 – Recovery Plan Specifications*.

CIP-009-6 Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	Conditions for activation of the recovery plan(s).	An example of evidence may include, but is not limited to, one or more plans that include language identifying conditions for activation of the recovery plan(s).

CIP-009-6 Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	Roles and responsibilities of responders.	An example of evidence may include, but is not limited to, one or more recovery plans that include language identifying the roles and responsibilities of responders.
1.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	One or more processes for the backup and storage of information required to recover BES Cyber System functionality.	An example of evidence may include, but is not limited to, documentation of specific processes for the backup and storage of information required to recover BES Cyber System functionality.

CIP-009-6 Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; and 2. PACS	One or more processes to verify the successful completion of the backup processes in Part 1.3 and to address any backup failures.	An example of evidence may include, but is not limited to, logs, workflow or other documentation confirming that the backup process completed successfully and backup failures, if any, were addressed.
1.5	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	One or more processes to preserve data, per Cyber Asset capability, for determining the cause of a Cyber Security Incident that triggers activation of the recovery plan(s). Data preservation should not impede or restrict recovery.	An example of evidence may include, but is not limited to, procedures to preserve data, such as preserving a corrupted drive or making a data mirror of the system before proceeding with recovery.

R2. Each Responsible Entity shall implement its documented recovery plan(s) to collectively include each of the applicable requirement parts in *CIP-009-6 Table R2 – Recovery Plan Implementation and Testing. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Real-time Operations.]*

M2. Evidence must include, but is not limited to, documentation that collectively demonstrates implementation of each of the applicable requirement parts in *CIP-009-6 Table R2 – Recovery Plan Implementation and Testing.*

CIP-009-6 Table R2 – Recovery Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; and 2. PACS	Test each of the recovery plans referenced in Requirement R1 at least once every 15 calendar months: • By recovering from an actual incident; • With a paper drill or tabletop exercise; or • With an operational exercise.	An example of evidence may include, but is not limited to, dated evidence of a test (by recovering from an actual incident, with a paper drill or tabletop exercise, or with an operational exercise) of the recovery plan at least once every 15 calendar months. For the paper drill or full operational exercise, evidence may include meeting notices, minutes, or other records of exercise findings.

CIP-009-6 Table R2 – Recovery Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; and 2. PACS	Test a representative sample of information used to recover BES Cyber System functionality at least once every 15 calendar months to ensure that the information is useable and is compatible with current configurations. An actual recovery that incorporates the information used to recover BES Cyber System functionality substitutes for this test.	An example of evidence may include, but is not limited to, operational logs or test results with criteria for testing the usability (e.g. sample tape load, browsing tape contents) and compatibility with current system configurations (e.g. manual or automated comparison checkpoints between backup media contents and current configuration).
2.3	High Impact BES Cyber Systems	Test each of the recovery plans referenced in Requirement R1 at least once every 36 calendar months through an operational exercise of the recovery plans in an environment representative of the production environment. An actual recovery response may substitute for an operational exercise.	Examples of evidence may include, but are not limited to, dated documentation of: • An operational exercise at least once every 36 calendar months between exercises, that demonstrates recovery in a representative environment; or • An actual recovery response that occurred within the 36 calendar month timeframe that exercised the recovery plans.

R3. Each Responsible Entity shall maintain each of its recovery plan(s) in accordance with each of the applicable requirement parts in *CIP-009-6 Table R3 – Recovery Plan Review, Update and Communication*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].*

M3. Acceptable evidence includes, but is not limited to, each of the applicable requirement parts in *CIP-009-6 Table R3 – Recovery Plan Review, Update and Communication.*

CIP-009-6 Table R3 – Recovery Plan Review, Update and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; and 2. PACS	No later than 90 calendar days after completion of a recovery plan test or actual recovery: 3.1.1. Document any lessons learned associated with a recovery plan test or actual recovery or document the absence of any lessons learned; 3.1.2. Update the recovery plan based on any documented lessons learned associated with the plan; and 3.1.3. Notify each person or group with a defined role in the recovery plan of the updates to the recovery plan based on any documented lessons learned.	An example of evidence may include, but is not limited to, all of the following: 1. Dated documentation of identified deficiencies or lessons learned for each recovery plan test or actual incident recovery or dated documentation stating there were no lessons learned; 2. Dated and revised recovery plan showing any changes based on the lessons learned; and 3. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

CIP-009-6 Table R3 – Recovery Plan Review, Update and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; and 2. PACS	No later than 60 calendar days after a change to the roles or responsibilities, responders, or technology that the Responsible Entity determines would impact the ability to execute the recovery plan: 3.2.1. Update the recovery plan; and 3.2.2. Notify each person or group with a defined role in the recovery plan of the updates.	An example of evidence may include, but is not limited to, all of the following: 1. Dated and revised recovery plan with changes to the roles or responsibilities, responders, or technology; and 2. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Investigations

Self-Reporting

Complaints

1.4. Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Long-term Planning**	**Medium**	N/A	The Responsible Entity has developed recovery plan(s), but the plan(s) do not address one of the requirements included in Parts 1.2 through 1.5.	The Responsible Entity has developed recovery plan(s), but the plan(s) do not address two of the requirements included in Parts 1.2 through 1.5.	The Responsible Entity has not created recovery plan(s) for BES Cyber Systems. OR The Responsible Entity has created recovery plan(s) for BES Cyber Systems, but the plan(s) does not address the conditions for activation in Part 1.1. OR The Responsible Entity has created recovery plan(s) for BES Cyber Systems, but the plan(s) does not address three or more of the requirements in Parts 1.2 through 1.5.

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R2	**Operations Planning** **Real-time Operations**	**Lower**	The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 15 calendar months, not exceeding 16 calendar months between tests of the plan. (2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 15 calendar months, not exceeding 16 calendar months between tests. (2.2) OR The Responsible Entity has not tested	The Responsible Entity has not tested the recovery plan(s) within 16 calendar months, not exceeding 17 calendar months between tests of the plan. (2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 16 calendar months, not exceeding 17 calendar months between tests. (2.2) OR The Responsible Entity has not tested the recovery plan	The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 17 calendar months, not exceeding 18 calendar months between tests of the plan. (2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 17 calendar months, not exceeding 18 calendar months between tests. (2.2) OR The Responsible Entity has not tested	The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 18 calendar months between tests of the plan. (2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 18 calendar months between tests. (2.2) OR The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.3 within 39 calendar months

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			the recovery plan according to R2 Part 2.3 within 36 calendar months, not exceeding 37 calendar months between tests. (2.3)	according to R2 Part 2.3 within 37 calendar months, not exceeding 38 calendar months between tests. (2.3)	the recovery plan according to R2 Part 2.3 within 38 calendar months, not exceeding 39 calendar months between tests. (2.3)	between tests of the plan. (2.3)
R3	**Operations Assessment**	**Lower**	The Responsible Entity has not notified each person or group with a defined role in the recovery plan(s) of updates within 90 and less than 120 calendar days of the update being completed. (3.1.3)	The Responsible Entity has not updated the recovery plan(s) based on any documented lessons learned within 90 and less than 120 calendar days of each recovery plan test or actual recovery. (3.1.2) OR The Responsible Entity has not notified each person or group with a defined role in the recovery plan(s) of updates within 120 calendar days of the	The Responsible Entity has neither documented lessons learned nor documented the absence of any lessons learned within 90 and less than 120 calendar days of each recovery plan test or actual recovery. (3.1.1) OR The Responsible Entity has not updated the recovery plan(s) based on any documented lessons learned within 120 calendar days of each	The Responsible Entity has neither documented lessons learned nor documented the absence of any lessons learned within 120 calendar days of each recovery plan test or actual recovery. (3.1.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				update being completed. (3.1.3) OR The Responsible Entity has not updated the recovery plan(s) or notified each person or group with a defined role within 60 and less than 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (3.2) • Roles or responsibilities, or • Responders, or • Technology changes.	recovery plan test or actual recovery. (3.1.2) OR The Responsible Entity has not updated the recovery plan(s) or notified each person or group with a defined role within 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (3.2) • Roles or responsibilities, or • Responders, or • Technology changes.	

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	

Version	Date	Action	Change Tracking
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-009-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed FERC directives from Order No. 791
6	1/21/16	FERC Order issued approving CIP-009-6. Docket No. RM15-14-000	

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

The following guidelines are available to assist in addressing the required components of a recovery plan:

- NERC, Security Guideline for the Electricity Sector: Continuity of Business Processes and Operations Operational Functions, September 2011, online at http://www.nerc.com/docs/cip/sgwg/Continuity%20of%20Business%20and%20Operational%20Functions%20FINAL%20102511.pdf
- National Institute of Standards and Technology, Contingency Planning Guide for Federal Information Systems, Special Publication 800-34 revision 1, May 2010, online at http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf

The term recovery plan is used throughout this Reliability Standard to refer to a documented set of instructions and resources needed to recover reliability functions performed by BES Cyber Systems. The recovery plan may exist as part of a larger business continuity or disaster recovery plan, but the term does not imply any additional obligations associated with those disciplines outside of the Requirements.

A documented recovery plan may not be necessary for each applicable BES Cyber System. For example, the short-term recovery plan for a BES Cyber System in a specific substation may be managed on a daily basis by advanced power system applications such as state estimation, contingency and remedial action, and outage scheduling. One recovery plan for BES Cyber Systems should suffice for several similar facilities such as those found in substations or power plants.

For Part 1.1, the conditions for activation of the recovery plan should consider viable threats to the BES Cyber System such as natural disasters, computing equipment failures, computing environment failures, and Cyber Security Incidents. A business impact analysis for the BES Cyber System may be useful in determining these conditions.

For Part 1.2, entities should identify the individuals required for responding to a recovery operation of the applicable BES Cyber System.

For Part 1.3, entities should consider the following types of information to recover BES Cyber System functionality:

1. Installation files and media;
2. Current backup tapes and any additional documented configuration settings;
3. Documented build or restoration procedures; and
4. Cross site replication storage.

For Part 1.4, the processes to verify the successful completion of backup processes should include checking for: (1) usability of backup media, (2) logs or inspection showing that information from current, production system could be read, and (3) logs or inspection showing that information was written to the backup media. Test restorations are not required for this Requirement Part. The following backup scenarios provide examples of effective processes to verify successful completion and detect any backup failures:

- Periodic (e.g. daily or weekly) backup process – Review generated logs or job status reports and set up notifications for backup failures.
- Non-periodic backup process– If a single backup is provided during the commissioning of the system, then only the initial and periodic (every 15 months) testing must be done. Additional testing should be done as necessary and can be a part of the configuration change management program.
- Data mirroring – Configure alerts on the failure of data transfer for an amount of time specified by the entity (e.g. 15 minutes) in which the information on the mirrored disk may no longer be useful for recovery.
- Manual configuration information – Inspect the information used for recovery prior to storing initially and periodically (every 15 months). Additional inspection should be done as necessary and can be a part of the configuration change management program.

The plan must also include processes to address backup failures. These processes should specify the response to failure notifications or other forms of identification.

For Part 1.5, the recovery plan must include considerations for preservation of data to determine the cause of a Cyber Security Incident. Because it is not always possible to initially know if a Cyber Security Incident caused the recovery activation, the data preservation procedures should be followed until such point a Cyber Security Incident can be ruled out. CIP-008 addresses the retention of data associated with a Cyber Security Incident.

Requirement R2:

A Responsible Entity must exercise each BES Cyber System recovery plan every 15 months. However, this does not necessarily mean that the entity must test each plan individually. BES Cyber Systems that are numerous and distributed, such as those found at substations, may not require an individual recovery plan and the associated redundant facilities since reengineering and reconstruction may be the generic response to a severe event. Conversely, there is typically one control center per bulk transmission service area that requires a redundant or backup facility. Because of these differences, the recovery plans associated with control centers differ a great deal from those associated with power plants and substations.

A recovery plan test does not necessarily cover all aspects of a recovery plan and failure scenarios, but the test should be sufficient to ensure the plan is up to date and at least one restoration process of the applicable cyber systems is covered.

Entities may use an actual recovery as a substitute for exercising the plan every 15 months. Otherwise, entities must exercise the plan with a paper drill, tabletop exercise, or operational exercise. For more specific types of exercises, refer to the FEMA Homeland Security Exercise and Evaluation Program (HSEEP). It lists the following four types of discussion-based exercises: seminar, workshop, tabletop, and games. In particular, it defines that, “A tabletop exercise involves key personnel discussing simulated scenarios in an informal setting. [Table top exercises (TTX)] can be used to assess plans, policies, and procedures.”

The HSEEP lists the following three types of operations-based exercises: Drill, functional exercise, and full-scale exercise. It defines that, “[A] full-scale exercise is a multi-agency, multi-jurisdictional, multi-discipline exercise involving functional (e.g., joint field office, Emergency operation centers, etc.) and ‘boots on the ground’ response (e.g., firefighters decontaminating mock victims).”

For Part 2.2, entities should refer to the backup and storage of information required to recover BES Cyber System functionality in Requirement Part 1.3. This provides additional assurance that the information will actually recover the BES Cyber System as necessary. For most complex computing equipment, a full test of the information is not feasible. Entities should determine the representative sample of information that provides assurance in the processes for Requirement Part 1.3. The test must include steps for ensuring the information is useable and current. For backup media, this can include testing a representative sample to make sure the information can be loaded, and checking the content to make sure the information reflects the current configuration of the applicable Cyber Assets.

Requirement R3:

This requirement ensures entities maintain recovery plans. There are two requirement parts that trigger plan updates: (1) lessons learned and (2) organizational or technology changes.

The documentation of lessons learned is associated with each recovery activation, and it involves the activities as illustrated in Figure 1, below. The deadline to document lessons learned starts after the completion of the recovery operation in recognition that complex recovery activities can take a few days or weeks to complete. The process of conducting lessons learned can involve the recovery team discussing the incident to determine gaps or areas of improvement within the plan. It is possible to have a recovery activation without any documented lessons learned. In such cases, the entity must retain documentation of the absence of any lessons learned associated with the recovery activation.

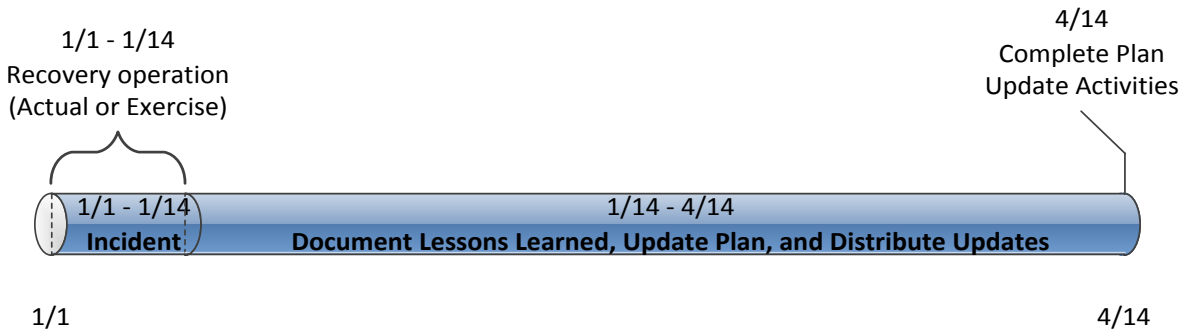


Figure 1: CIP-009-6 R3 Timeline

The activities necessary to complete the lessons learned include updating the plan and distributing those updates. Entities should consider meeting with all of the individuals involved in the recovery and documenting the lessons learned as soon after the recovery activation as possible. This allows more time for making effective updates to the plan, obtaining any necessary approvals, and distributing those updates to the recovery team.

The plan change requirement is associated with organization and technology changes referenced in the plan and involves the activities illustrated in Figure 2, below. Organizational changes include changes to the roles and responsibilities people have in the plan or changes to the response groups or individuals. This may include changes to the names or contact information listed in the plan. Technology changes affecting the plan may include referenced information sources, communication systems, or ticketing systems.

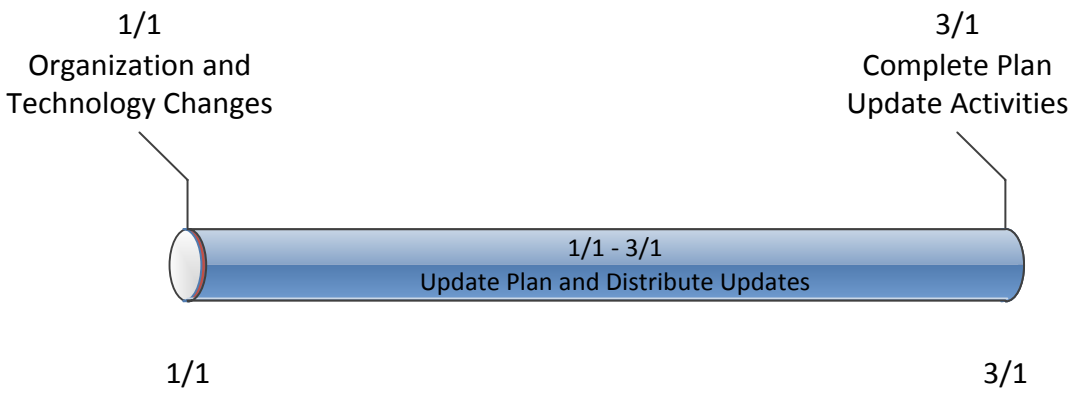


Figure 2: Timeline for Plan Changes in 3.2

When notifying individuals of response plan changes, entities should keep in mind that recovery plans may be considered BES Cyber System Information, and they should take the appropriate measures to prevent unauthorized disclosure of recovery plan information. For example, the recovery plan itself, or other sensitive information about the recovery plan, should be redacted from Email or other unencrypted transmission.

Rationale:

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for Requirement R1:

Preventative activities can lower the number of incidents, but not all incidents can be prevented. A preplanned recovery capability is, therefore, necessary for rapidly recovering from incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services so that planned and consistent recovery action to restore BES Cyber System functionality occurs.

Rationale for Requirement R2:

The implementation of an effective recovery plan mitigates the risk to the reliable operation of the BES by reducing the time to recover from various hazards affecting BES Cyber Systems. This requirement ensures continued implementation of the response plans.

Requirement Part 2.2 provides further assurance in the information (e.g. backup tapes, mirrored hot-sites, etc.) necessary to recover BES Cyber Systems. A full test is not feasible in most instances due to the amount of recovery information, and the Responsible Entity must determine a sampling that provides assurance in the usability of the information.

Rationale for Requirement R3:

To improve the effectiveness of BES Cyber System recovery plan(s) following a test, and to ensure the maintenance and distribution of the recovery plan(s). Responsible Entities achieve this by (i) performing a lessons learned review in 3.1 and (ii) revising the plan in 3.2 based on specific changes in the organization or technology that would impact plan execution. In both instances when the plan needs to change, the Responsible Entity updates and distributes the plan.

Appendix QC-CIP-009-6
Provisions specific to the standard CIP-009-6 applicable in Québec

This appendix establishes specific provisions for the application of the standard in Québec. Provisions of the standard and of its appendix must be read together for the purposes of understanding and interpretation. Where the standard and appendix differ, the appendix shall prevail.

A. Introduction

1. **Title:** Cyber Security — Recovery Plans for BES Cyber Systems

2. **Number:** CIP-009-6

3. **Purpose:** No specific provision

4. **Applicability:**

   4.1. Functional Entities

   No specific provision

   4.2. Facilities

   This standard only applies to the facilities of the Main Transmission System (RTP) and to the facilities specified for the Distribution Provider. In the application of this standard, all reference to the terms "Bulk Electric System" or "BES" shall be replaced by the terms "Main Transmission System" or "RTP" respectively.

   Additional Exemptions

   The following are exempt from this standard:

   - Any generating facility that meets the two following conditions: (1) the nameplate capacity of the facility is 300 MVA or less, and (2) no unit of the facility can be synchronized with a neighbouring system.
   - Step-up substations of generating facilities identified in the preceding point.

5. **Effective Date:**

   5.1. Adoption of the standard by the Régie de l'énergie: October 31st , 2017

   5.2. Adoption of the appendix by the Régie de l'énergie: October 31st, 2017

   5.3. Effective date of the standard and its appendix in Québec: January 1st, 2018

Standard	Implementation date for Québec		
	Entities subject to version 1 of the CIP standards adopted by the Régie	Entities exempted from the application of version 1 of the CIP standards under the specific provisions associated with these standards	Entities that have generation facilities for industrial use
CIP-009-6	January 1st, 2018	October 1st, 2018	April 1st, 2019

6. Background:

No specific provision

B. Requirements and Measures

No specific provision

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

The Régie de l'énergie is responsible, in Québec, for compliance enforcement with respect to the reliability standard and its appendix that it adopts.

1.2. Evidence Retention

No specific provision

1.3. Compliance Monitoring and Assessment Processes

No specific provision

1.4. Additional Compliance Information

No specific provision

1.5. Table of Compliance Elements

No specific provision

D. Regional Variances

No specific provision

E. Interpretations

No specific provision

F. Associated Documents

No specific provision

Guidelines and Technical Basis

No specific provision

Rationale

No specific provision

Version History

Revision	Date	Action	Change Tracking
0	October 31st, 2017	New appendix	New

A. Introduction

1. **Title:** Cyber Security — Configuration Change Management and Vulnerability Assessments

2. **Number:** CIP-010-4

3. **Purpose:** To prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1. Balancing Authority

   4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

   4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in Section 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-010-4:

4.2.3.1. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002 identification and categorization processes.

5. Effective Date: See Implementation Plan for Project 2019-03.

6. Background: Standard CIP-010 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans, and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the BES. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the applicability column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002 identification and categorization processes.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.

- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-4 Table R1 – Configuration Change Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*.

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-4 Table R1 – Configuration Change Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-4 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Develop a baseline configuration, individually or by group, which shall include the following items: 1.1.1. Operating system(s) (including version) or firmware where no independent operating system exists; 1.1.2. Any commercially available or open-source application software (including version) intentionally installed; 1.1.3. Any custom software installed; 1.1.4. Any logical network accessible ports; and 1.1.5. Any security patches applied.	Examples of evidence may include, but are not limited to: • A spreadsheet identifying the required items of the baseline configuration for each Cyber Asset, individually or by group; or • A record in an asset management system that identifies the required items of the baseline configuration for each Cyber Asset, individually or by group.
1.2	High Impact BES Cyber Systems and their associated: 1. EACMS;	Authorize and document changes that deviate from the existing baseline configuration.	Examples of evidence may include, but are not limited to:

CIP-010-4 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
	2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA		• A change request record and associated electronic authorization (performed by the individual or group with the authority to authorize the change) in a change management system for each change; or • Documentation that the change was performed in accordance with the requirement.
1.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For a change that deviates from the existing baseline configuration, update the baseline configuration as necessary within 30 calendar days of completing the change.	An example of evidence may include, but is not limited to, updated baseline documentation with a date that is within 30 calendar days of the date of the completion of the change.
1.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated:	For a change that deviates from the existing baseline configuration: 1.4.1. Prior to the change, determine required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change; 1.4.2. Following the change, verify that	An example of evidence may include, but is not limited to, a list of cyber security controls verified or tested along with the dated test results.

CIP-010-4 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
	1. EACMS; 2. PACS; and 3. PCA	required cyber security controls determined in 1.4.1 are not adversely affected; and 1.4.3. Document the results of the verification.	
1.5	High Impact BES Cyber Systems	Where technically feasible, for each change that deviates from the existing baseline configuration: 1.5.1. Prior to implementing any change in the production environment, test the changes in a test environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely affected; and 1.5.2. Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures	An example of evidence may include, but is not limited to, a list of cyber security controls tested along with successful test results and a list of differences between the production and test environments with descriptions of how any differences were accounted for, including the date of the test.

CIP-010-4 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
		used to account for any differences in operation between the test and production environments.	
1.6	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Note: Implementation does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders). Additionally, the following issues are beyond the scope of Part 1.6: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.	Prior to a change that deviates from the existing baseline configuration associated with baseline items in Parts 1.1.1, 1.1.2, and 1.1.5, and when the method to do so is available to the Responsible Entity from the software source: 1.6.1. Verify the identity of the software source; and 1.6.2. Verify the integrity of the software obtained from the software source.	An example of evidence may include, but is not limited to a change request record that demonstrates the verification of identity of the software source and integrity of the software was performed prior to the baseline change or a process which documents the mechanisms in place that would automatically ensure the identity of the software source and integrity of the software.

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-4 Table R2 – Configuration Monitoring. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-4 Table R2 – Configuration Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-4 Table R2 – Configuration Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA	Monitor at least once every 35 calendar days for changes to the baseline configuration (as described in Requirement R1, Part 1.1). Document and investigate detected unauthorized changes.	An example of evidence may include, but is not limited to, logs from a system that is monitoring the configuration along with records of investigation for any unauthorized changes that were detected.

R3. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-3 Table R3– Vulnerability Assessments*. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M3. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-3 Table R3 – Vulnerability Assessments* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-4 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	At least once every 15 calendar months, conduct a paper or active vulnerability assessment.	Examples of evidence may include, but are not limited to: • A document listing the date of the assessment (performed at least once every 15 calendar months), the controls assessed for each BES Cyber System along with the method of assessment; or • A document listing the date of the assessment and the output of any tools used to perform the assessment.

CIP-010-4 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems	Where technically feasible, at least once every 36 calendar months: 3.2.1 Perform an active vulnerability assessment in a test environment, or perform an active vulnerability assessment in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration of the BES Cyber System in a production environment; and 3.2.2 Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed at least once every 36 calendar months), the output of the tools used to perform the assessment, and a list of differences between the production and test environments with descriptions of how any differences were accounted for in conducting the assessment.

CIP-010-4 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA	Prior to adding a new applicable Cyber Asset to a production environment, perform an active vulnerability assessment of the new Cyber Asset, except for CIP Exceptional Circumstances and like replacements of the same type of Cyber Asset with a baseline configuration that models an existing baseline configuration of the previous or other existing Cyber Asset.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed prior to the commissioning of the new Cyber Asset) and the output of any tools used to perform the assessment.
3.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Document the results of the assessments conducted according to Parts 3.1, 3.2, and 3.3 and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of any remediation or mitigation action items.	An example of evidence may include, but is not limited to, a document listing the results or the review or assessment, a list of action items, documented proposed dates of completion for the action plan, and records of the status of the action items (such as minutes of a status meeting, updates in a work order system, or a spreadsheet tracking the action items).

R4. Each Responsible Entity, for its high impact and medium impact BES Cyber Systems and associated Protected Cyber Assets, shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) for Transient Cyber Assets and Removable Media that include the sections in Attachment 1. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M4. Evidence shall include each of the documented plan(s) for Transient Cyber Assets and Removable Media that collectively include each of the applicable sections in Attachment 1 and additional evidence to demonstrate implementation of plan(s) for Transient Cyber Assets and Removable Media. Additional examples of evidence per section are located in Attachment 2. If a Responsible Entity does not use Transient Cyber Asset(s) or Removable Media, examples of evidence include, but are not limited to, a statement, policy, or other document that states the Responsible Entity does not use Transient Cyber Asset(s) or Removable Media.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation.

- Each applicable entity shall retain evidence of each requirement in this standard for three calendar years.
- If an applicable entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only four of the required baseline items listed in 1.1.1 through 1.1.5. (1.1)	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only three of the required baseline items listed in 1.1.1 through 1.1.5. (1.1)	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only two of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) OR The Responsible Entity has a process as specified in Part 1.6 to verify the identity of the software source (1.6.1) but does not have a process as specified in Part 1.6 to verify the integrity of the software provided by the software source when the method to do so is available to the Responsible Entity from the software source. (1.6.2)	The Responsible Entity has not documented or implemented any configuration change management process(es). (R1) OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes only one of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) OR The Responsible Entity does not have a process(es) that requires authorization and documentation of changes that deviate from the existing baseline configuration. (1.2) OR

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				The Responsible Entity does not have a process(es) to update baseline configurations within 30 calendar days of completing a change(s) that deviates from the existing baseline configuration.(1.3) OR The Responsible Entity does not have a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline configuration. (1.4.1) OR The Responsible Entity has a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline configuration but did not verify and document that the required controls were

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				not adversely affected following the change. (1.4.2 & 1.4.3) OR The Responsible Entity does not have a process for testing changes in an environment that models the baseline configuration prior to implementing a change that deviates from baseline configuration. (1.5.1) OR The Responsible Entity does not have a process to document the test results and, if using a test environment, document the differences between the test and production environments. (1.5.2) OR The Responsible Entity does not have a process as specified in Part 1.6 to verify the identity of the software

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				source and the integrity of the software provided by the software source when the method to do so is available to the Responsible Entity from the software source. (1.6)
R2.	N/A	N/A	N/A	The Responsible Entity has not documented or implemented a process(es) to monitor for, investigate, and document detected unauthorized changes to the baseline at least once every 35 calendar days. (2.1)
R3.	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 15 months, but less than 18 months, since the last assessment on one of its	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 18 months, but less than 21 months, since the last assessment on one of its	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 21 months, but less than 24 months, since the last assessment on one of its	The Responsible Entity has not implemented any vulnerability assessment processes for one of its applicable BES Cyber Systems. (R3) OR The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 36 months, but less than 39 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 39 months, but less than 42 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 42 months, but less than 45 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	Cyber Systems, but has performed a vulnerability assessment more than 24 months since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 45 months since the last active assessment on one of its applicable BES Cyber Systems.(3.2) OR The Responsible Entity has implemented and documented one or more vulnerability assessment processes for each of its applicable BES Cyber Systems, but did not

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				perform the active vulnerability assessment in a manner that models an existing baseline configuration of its applicable BES Cyber Systems. (3.3) OR The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has not documented the results of the vulnerability assessments, the action plans to remediate or mitigate vulnerabilities identified in the assessments, the planned date of completion of the action plan, and the execution status of the mitigation plans. (3.4)
R4.	The Responsible Entity documented its plan(s) for Transient Cyber Assets and	The Responsible Entity documented its plan(s) for Transient Cyber Assets and	The Responsible Entity documented its plan(s) for Transient Cyber Assets and	The Responsible Entity failed to document or implement one or more

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	Removable Media, but failed to manage its Transient Cyber Asset(s) according to CIP-010-3, Requirement R4, Attachment 1, Section 1.1. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document the Removable Media sections according to CIP-010-3, Requirement R4, Attachment 1, Section 3. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document authorization for Transient Cyber Assets managed by the Responsible Entity according to CIP-010-3,	Removable Media, but failed to implement the Removable Media sections according to CIP-010-3, Requirement R4, Attachment 1, Section 3. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media plan, but failed to document mitigation of software vulnerabilities, mitigation for the introduction of malicious code, or mitigation of the risk of unauthorized use for Transient Cyber Assets managed by the Responsible Entity according to CIP-010-3, Requirement R4, Attachment 1, Sections 1.3, 1.4, and 1.5. (R4) OR The Responsible Entity documented its plan(s) for	Removable Media, but failed to authorize its Transient Cyber Asset(s) according to CIP-010-3, Requirement R4, Attachment 1, Section 1.2. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation of software vulnerabilities, mitigation for the introduction of malicious code, or mitigation of the risk of unauthorized use for Transient Cyber Assets managed by the Responsible Entity according to CIP-010-3, Requirement R4, Attachment 1, Sections 1.3, 1.4, and 1.5. (R4) OR The Responsible Entity documented its plan(s) for	plan(s) for Transient Cyber Assets and Removable Media according to CIP-010-3, Requirement R4. (R4)

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	Requirement R4, Attachment 1, Section 1.2. (R4)	Transient Cyber Assets and Removable Media, but failed to document mitigation of software vulnerabilities or mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to CIP-010-3, Requirement R4, Attachment 1, Sections 2.1, 2.2, and 2.3. (R4)	Transient Cyber Assets and Removable Media, but failed to implement mitigation of software vulnerabilities or mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to CIP-010-3, Requirement R4, Attachment 1, Sections 2.1, 2.2, and 2.3. (R4)	

D. Regional Variances

None.

E. Associated Documents

- Implementation Plan for Project 2019-03.
- CIP-010-4 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	11/26/12	Adopted by the NERC Board of Trustees.	Developed to define the configuration change management and vulnerability assessment requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.
1	11/22/13	FERC Order issued approving CIP-010-1. (Order becomes effective on 2/3/14.)	
2	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
2	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
2	1/21/16	FERC Order issued approving CIP-010-3. Docket No. RM15-14-000	
3	07/20/17	Modified to address certain directives in FERC Order No. 829.	Revised
3	08/10/17	Adopted by the NERC Board of Trustees.	
3	10/18/2018	FERC Order approving CIP-010-3. Docket No. RM17-13-000.	
4	08/01/2019	Modified to address directives in FERC Order No. 850.	Revised
4	11/05/2020	Adopted by the NERC Board of Trustees.	

Version	Date	Action	Change Tracking
4	3/18/2021	FERC Order approving CIP-010-4.Docket No. RD21-2-000	
4	10/1/2022	Effective Date	

CIP-010-4 - Attachment 1

Required Sections for Plans for Transient Cyber Assets and Removable Media

Responsible Entities shall include each of the sections provided below in their plan(s) for Transient Cyber Assets and Removable Media as required under Requirement R4.

Section 1. Transient Cyber Asset(s) Managed by the Responsible Entity.

1.1. Transient Cyber Asset Management: Responsible Entities shall manage Transient Cyber Asset(s), individually or by group: (1) in an ongoing manner to ensure compliance with applicable requirements at all times, (2) in an on-demand manner applying the applicable requirements before connection to a BES Cyber System, or (3) a combination of both (1) and (2) above.

1.2. Transient Cyber Asset Authorization: For each individual or group of Transient Cyber Asset(s), each Responsible Entity shall authorize:

1.2.1. Users, either individually or by group or role;

1.2.2. Locations, either individually or by group; and

1.2.3. Uses, which shall be limited to what is necessary to perform business functions.

1.3. Software Vulnerability Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of vulnerabilities posed by unpatched software on the Transient Cyber Asset (per Transient Cyber Asset capability):

- Security patching, including manual or managed updates;
- Live operating system and software executable only from read-only media;
- System hardening; or
- Other method(s) to mitigate software vulnerabilities.

1.4. Introduction of Malicious Code Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the introduction of malicious code (per Transient Cyber Asset capability):

- Antivirus software, including manual or managed updates of signatures or patterns;
- Application whitelisting; or
- Other method(s) to mitigate the introduction of malicious code.

1.5. Unauthorized Use Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of unauthorized use of Transient Cyber Asset(s):

- Restrict physical access;
- Full-disk encryption with authentication;
- Multi-factor authentication; or
- Other method(s) to mitigate the risk of unauthorized use.

Section 2. Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity.

2.1. Software Vulnerabilities Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of vulnerabilities posed by unpatched software on the Transient Cyber Asset (per Transient Cyber Asset capability):

- Review of installed security patch(es);
- Review of security patching process used by the party;
- Review of other vulnerability mitigation performed by the party; or
- Other method(s) to mitigate software vulnerabilities.

2.2. Introduction of malicious code mitigation: Use one or a combination of the following methods to achieve the objective of mitigating malicious code (per Transient Cyber Asset capability):

- Review of antivirus update level;
- Review of antivirus update process used by the party;
- Review of application whitelisting used by the party;
- Review use of live operating system and software executable only from read-only media;
- Review of system hardening used by the party; or
- Other method(s) to mitigate malicious code.

2.3. For any method used to mitigate software vulnerabilities or malicious code as specified in 2.1 and 2.2, Responsible Entities shall determine whether any additional mitigation actions are necessary and implement such actions prior to connecting the Transient Cyber Asset.

Section 3. Removable Media

3.1. Removable Media Authorization: For each individual or group of Removable Media, each Responsible Entity shall authorize:

3.1.1. Users, either individually or by group or role; and

3.1.2. Locations, either individually or by group.

3.2. Malicious Code Mitigation: To achieve the objective of mitigating the threat of introducing malicious code to high impact or medium impact BES Cyber

Systems and their associated Protected Cyber Assets, each Responsible Entity shall:

3.2.1. Use method(s) to detect malicious code on Removable Media using a Cyber Asset other than a BES Cyber System or Protected Cyber Assets; and

3.2.2. Mitigate the threat of detected malicious code on Removable Media prior to connecting the Removable Media to a high impact or medium impact BES Cyber System or associated Protected Cyber Assets.

CIP-010-4 - Attachment 2

Examples of Evidence for Plans for Transient Cyber Assets and Removable Media

Section 1.1: Examples of evidence for Section 1.1 may include, but are not limited to, the method(s) of management for the Transient Cyber Asset(s). This can be included as part of the Transient Cyber Asset plan(s), part of the documentation related to authorization of Transient Cyber Asset(s) managed by the Responsible Entity or part of a security policy.

Section 1.2: Examples of evidence for Section 1.2 may include, but are not limited to, documentation from asset management systems, human resource management systems, or forms or spreadsheets that show authorization of Transient Cyber Asset(s) managed by the Responsible Entity. Alternatively, this can be documented in the overarching plan document.

Section 1.3: Examples of evidence for Section 1.3 may include, but are not limited to, documentation of the method(s) used to mitigate software vulnerabilities posed by unpatched software such as security patch management implementation, the use of live operating systems from read-only media, system hardening practices or other method(s) to mitigate the software vulnerability posed by unpatched software. Evidence can be from change management systems, automated patch management solutions, procedures or processes associated with using live operating systems, or procedures or processes associated with system hardening practices. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the risk from unpatched software, evidence may include documentation by the vendor or Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 1.4: Examples of evidence for Section 1.4 may include, but are not limited to, documentation of the method(s) used to mitigate the introduction of malicious code such as antivirus software and processes for managing signature or pattern updates, application whitelisting practices, processes to restrict communication, or other method(s) to mitigate the introduction of malicious code. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the vendor or Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 1.5: Examples of evidence for Section 1.5 may include, but are not limited to, documentation through policies or procedures of the method(s) to restrict physical access; method(s) of the full-disk encryption solution along with the authentication protocol; method(s) of the multi-factor authentication solution; or documentation of other method(s) to mitigate the risk of unauthorized use.

Section 2.1: Examples of evidence for Section 2.1 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of installed security patch(es); memoranda, electronic

mail, policies or contracts from parties other than the Responsible Entity that identify the security patching process or vulnerability mitigation performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail, system documentation or contracts that identifies acceptance by the Responsible Entity that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate software vulnerabilities for Transient Cyber Asset(s) managed by a party other than the Responsible Entity. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the risk from unpatched software, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 2.2: Examples of evidence for Section 2.2 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of the installed antivirus update level; memoranda, electronic mail, system documentation, policies or contracts from the party other than the Responsible Entity that identify the antivirus update process, the use of application whitelisting, use of live of operating systems or system hardening performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail or contracts that identifies the Responsible Entity's acceptance that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate malicious code for Transient Cyber Asset(s) managed by a party other than the Responsible Entity. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 2.3: Examples of evidence for Section 2.3 may include, but are not limited to, documentation from change management systems, electronic mail, or contracts that identifies a review to determine whether additional mitigations are necessary and that they have been implemented prior to connecting the Transient Cyber Asset managed by a party other than the Responsible Entity.

Section 3.1: Examples of evidence for Section 3.1 may include, but are not limited to, documentation from asset management systems, human resource management systems, forms or spreadsheets that shows authorization of Removable Media. The documentation must identify Removable Media, individually or by group of Removable Media, along with the authorized users, either individually or by group or role, and the authorized locations, either individually or by group.

Section 3.2: Examples of evidence for Section 3.2 may include, but are not limited to, documented process(es) of the method(s) used to mitigate malicious code such as results of scan settings for Removable Media, or implementation of on-demand scanning. Documented process(es) for the method(s) used for mitigating

the threat of detected malicious code on Removable Media, such as logs from the method(s) used to detect malicious code that show the results of scanning and that show mitigation of detected malicious code on Removable Media or documented confirmation by the entity that the Removable Media was deemed to be free of malicious code.

Appendix CIP-010-4-QC-1
Specific provisions applicable in Québec for standard CIP-010-4 – Cyber Security — Configuration Change Management and Vulnerability Assessments

This appendix establishes specific provisions for the application of the standard in Québec. Provisions of the standard and of this appendix must be read jointly for comprehension and interpretation purposes. Where the standard and appendix differ, the appendix shall prevail.

A. Introduction

1. Title: No specific provisions.

2. Number: No specific provisions.

3. Purpose: No specific provisions.

4. Applicability:

4.1. Functional Entities

No specific provisions.

4.2. Facilities

This standard only applies to the facilities of the Main Transmission System (RTP) and to the facilities specified for the Distribution Provider. In the application of this standard, all reference to the terms "Bulk Electric System" or "BES" shall be replaced by the terms "Main Transmission System" or "RTP" respectively.

Additional Exemptions

The following are exempt from this standard:

- Any generating facility that meets the two following conditions: (1) the nameplate capacity of the facility is 300 MVA or less, and (2) no unit of the facility can be synchronized with a neighbouring system.
- Step-up substations of generating facilities identified in the preceding point.

5. Effective Date:

5.1. Adoption of the standard by the Régie de l'énergie: February 11, 2022

5.2. Adoption of the appendix by the Régie de l'énergie: February 11, 2022

5.3. Effective date of the standard and its appendix in Québec: October 1, 2023

6. Background: No specific provisions.

B. Requirements and Measures

For Requirement R3 and Measure M3, replace any reference to Reliability Standard CIP-010-3 by CIP-010-4 Reliability Standard.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

In Québec, "Compliance Enforcement Authority" means the Régie de l'énergie in its roles of monitoring and enforcing compliance with respect to the Reliability Standard and to this appendix.

1.2. Evidence Retention

No specific provisions.

1.3. Compliance Monitoring and Enforcement Program

The Régie de l'énergie establishes the monitoring processes used to evaluate data or information for the purpose of determining compliance or non-compliance with the Reliability Standard and with this appendix.

Violation Severity Levels (VSL)

For all Violation Severity Levels of Requirement R4, replace any reference to Reliability Standard CIP-010-3 by CIP-010-4 Reliability Standard.

D. Regional Variances

No specific provisions.

E. Associated Documents

No specific provisions.

CIP-010-4 - Attachment 1

No specific provisions.

CIP-010-4 - Attachment 2

No specific provisions.

Version History

Version	Date	Action	Change Tracking
1	February 11, 2022	New appendix as per decision D-2022-021.	New

A. Introduction

1. **Title:** Cyber Security — Information Protection

2. **Number:** CIP-011-3

3. **Purpose:** To prevent unauthorized access to BES Cyber System Information (BCSI) by specifying information protection requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1 Balancing Authority

   4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2 Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

   4.1.3 Generator Operator

   4.1.4 Generator Owner

   4.1.5 Reliability Coordinator

4.1.6 Transmission Operator

4.1.7 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-011-3:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1a identification and categorization processes.

5. **Effective Dates:** See Implementation Plan for CIP-011-3.

6. **Background:** Standard CIP-011 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.

   Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

   The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.

   The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

   Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

   Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

   Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and

implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the BES. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1a identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1a identification and categorization processes.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented information protection program(s) for BES Cyber System Information (BCSI) pertaining to "Applicable Systems" identified in *CIP-011-3 Table R1 – Information Protection Program* that collectively includes each of the applicable requirement parts in *CIP-011-3 Table R1 – Information Protection Program*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1. Evidence for the information protection program must include the applicable requirement parts in *CIP-011-3 Table R1 – Information Protection Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-3 Table R1 – Information Protection Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	Method(s) to identify BCSI.	Examples of acceptable evidence may include, but are not limited to, the following: • Documented method(s) to identify BCSI from the entity's information protection program; or • Indications on information (e.g., labels or classification) that identify BCSI as designated in the entity's information protection program; or • Training materials that provide personnel with sufficient knowledge to identify BCSI; or • Storage locations identified for housing BCSI in the entity's information protection program.

CIP-011-3 Table R1 – Information Protection Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	Method(s) to protect and securely handle BCSI to mitigate risks of compromising confidentiality.	Examples of evidence for on-premise BCSI may include, but are not limited to, the following: • Procedures for protecting and securely handling, which include topics such as storage, security during transit, and use of BCSI; or • Records indicating that BCSI is handled in a manner consistent with the entity's documented procedure(s). Examples of evidence for off-premise BCSI may include, but are not limited to, the following: • Implementation of electronic technical method(s) to protect electronic BCSI (e.g., data masking, encryption, hashing, tokenization, cipher, electronic key management); or • Implementation of physical technical method(s) to protect physical BCSI (e.g., physical lock and key management, physical badge management, biometrics, alarm system); or

CIP-011-3 Table R1 – Information Protection Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
			• Implementation of administrative method(s) to protect BCSI (e.g., vendor service risk assessments, business agreements).

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include the applicable requirement parts in *CIP-011-3 Table R2 – BES Cyber Asset Reuse and Disposal*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-011-3 Table R2 – BES Cyber Asset Reuse and Disposal* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-3 Table R2 – BES Cyber Asset Reuse and Disposal			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Prior to the release for reuse of applicable Cyber Assets that contain BCSI (except for reuse within other systems identified in the "Applicable Systems" column), the Responsible Entity shall take action to prevent the unauthorized retrieval of BCSI from the Cyber Asset data storage media.	Examples of acceptable evidence may include, but are not limited to, the following: • Records tracking sanitization actions taken to prevent unauthorized retrieval of BCSI such as clearing, purging, or destroying; or • Records tracking actions such as encrypting, retaining in the Physical Security Perimeter or other methods used to prevent unauthorized retrieval of BCSI.

CIP-011-3 Table R2 – BES Cyber Asset Reuse and Disposal			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Prior to the disposal of applicable Cyber Assets that contain BCSI, the Responsible Entity shall take action to prevent the unauthorized retrieval of BCSI from the Cyber Asset or destroy the data storage media.	Examples of acceptable evidence may include, but are not limited to, the following: • Records that indicate that data storage media was destroyed prior to the disposal of an applicable Cyber Asset; or • Records of actions taken to prevent unauthorized retrieval of BCSI prior to the disposal of an applicable Cyber Asset.

B. Compliance

1. **Compliance Monitoring Process:**

1.1. Compliance Enforcement Authority: "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- The applicable entity shall retain evidence of each requirement in this standard for three calendar years.
- If an applicable entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Time Horizon	VRF	Violation Severity Levels (CIP-011-3)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	N/A	N/A	The Responsible Entity documented, but did not, implement one or more BCSI protection program(s). (R1) OR The Responsible Entity documented but did not implement at least one method to identify BCSI. (1.1) OR The Responsible Entity documented but did not implement at least one method to protect and securely handle BCSI. (1.2)	The Responsible Entity neither documented nor implemented one or more BCSI protection program(s). (R1)
R2	**Operations Planning**	**Lower**	N/A	The Responsible Entity implemented one or more documented	The Responsible Entity implemented one or more documented	The Responsible Entity has not documented or implemented any

R #	Time Horizon	VRF	Violation Severity Levels (CIP-011-3)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				processes but did not include processes for reuse as to prevent the unauthorized retrieval of BCSI from the BES Cyber Asset. (2.1)	processes but did not include disposal or media destruction processes to prevent the unauthorized retrieval of BCSI from the BES Cyber Asset. (2.2)	processes for applicable requirement parts in CIP-011-3 Table R3 – BES Cyber Asset Reuse and Disposal. (R2)

C. Regional Variances

None.

D. Interpretations

None.

E. Associated Documents

Version History

Version	Date	Action	Change Tracking
1	11/26/12	Adopted by the NERC Board of Trustees.	Developed to define the information protection requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.
1	11/22/13	FERC Order issued approving CIP-011-1. (Order becomes effective on 2/3/14.)	
2	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
2	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
2	1/21/16	FERC Order issued approving CIP-011-2. Docket No. RM15-14-000	
3	8/12/21	Adopted by the NERC Board of Trustees	Revised to enhance BES reliability for entities to manage their BCSI.

3	12/7/21	FERC Order issued approving CIP-011-3 Docket No. RD21-6-000	"A Responsible Entity may elect to comply with the requirements in CIP-004-7 and CIP-011-3 following their approval by the applicable governmental authority, but prior to their Effective Date. In such a case, the Responsible Entity shall notify the applicable Regional Entities of the date of compliance with the CIP-004-7 and CIP-011-3 Reliability Standards. Responsible Entities must comply with CIP-004-6 and CIP-011-2 until that date."
3	12/10/21	Effective Date	1/1/2024

Appendix CIP-011-3-QC-1
Specific provisions applicable in Québec for standard
CIP-011-3 – Cyber Security – Information Protection

This appendix establishes specific provisions for the application of the standard in Québec. Provisions of the standard and of this appendix must be read jointly for comprehension and interpretation purposes. Where the standard and appendix differ, the appendix shall prevail.

A. Introduction

1. Title: No specific provisions.

2. Number: No specific provisions.

3. Purpose: No specific provisions.

4. Applicability:

4.1. Functional Entities

No specific provisions.

4.2. Facilities

This standard only applies to the facilities of the Main Transmission System (RTP) and to the facilities specified for the Distribution Provider. In the application of this standard, all reference to the terms "Bulk Electric System" or "BES" shall be replaced by the terms "Main Transmission System" or "RTP" respectively.

Additional Exemptions

The following are exempt from this standard:

- Any generating facility that meets the two following conditions: (1) the nameplate capacity of the facility is 300 MVA or less, and (2) no unit of the facility can be synchronized with a neighbouring System.
- Step-up substations of generating facilities identified in the preceding point.

5. Effective Dates:

5.1. Adoption of the standard by the Régie de l'énergie: December 13, 2022

5.2. Adoption of the appendix by the Régie de l'énergie: December 13, 2022

5.3. Effective date of the standard and its appendix in Québec: January 1, 2025

6. Background:

No specific provisions.

B. Requirements and Measures

No specific provisions.

B. Compliance

Replace the title « B. Compliance » by the title « C. Compliance ».

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

In Québec, "Compliance Enforcement Authority" means the Régie de l'énergie in its roles of monitoring and enforcing compliance with respect to the Reliability Standard and to this appendix.

1.2. Evidence Retention

No specific provisions.

1.3. Compliance Monitoring and Enforcement Program

The Régie de l'énergie establishes the monitoring processes used to evaluate data or information for the purpose of determining compliance or non-compliance with the Reliability Standard and with this appendix.

Violation Severity Levels (VSL)

For Requirement R2 severe Violation Severity Level, replace any reference to Table R3 by Table R2.

C. Regional Variances

Replace the title « C. Regional Variances » by the title « D. Regional Variances ».

D. Interpretations

Replace the title « D. Interpretations » by the title « E. Interpretations ».

E. Associated Documents

Replace the title « E. Associated Documents » by the title « F. Associated Documents ».

Version History

Version	Date	Action	Change Tracking
1	December 13, 2022	New appendix as per decision D-2022-150.	New

A. Introduction

1. **Title:** Cyber Security – Communications between Control Centers
2. **Number:** CIP-012-1
3. **Purpose:** To protect the confidentiality and integrity of Real-time Assessment and Real-time monitoring data transmitted between Control Centers.
4. **Applicability:**
   - **4.1. Functional Entities:** The requirements in this standard apply to the following functional entities, referred to as "Responsible Entities," that own or operate a Control Center.
     - **4.1.1. Balancing Authority**
     - **4.1.2. Generator Operator**
     - **4.1.3. Generator Owner**
     - **4.1.4. Reliability Coordinator**
     - **4.1.5. Transmission Operator**
     - **4.1.6. Transmission Owner**
   - **4.2. Exemptions:** The following are exempt from Reliability Standard CIP-012-1:
     - **4.2.1.** Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.
     - **4.2.2.** The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.
     - **4.2.3.** A Control Center that transmits to another Control Center Real-time Assessment or Real-time monitoring data pertaining only to the generation resource or Transmission station or substation co-located with the transmitting Control Center.
5. **Effective Date:** See Implementation Plan for CIP-012-1.

B. Requirements and Measures

R1. The Responsible Entity shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) to mitigate the risks posed by unauthorized disclosure and unauthorized modification of Real-time Assessment and Real-time monitoring data while being transmitted between any applicable Control Centers. The Responsible Entity is not required to include oral communications in its plan. The plan shall include: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1. Identification of security protection used to mitigate the risks posed by unauthorized disclosure and unauthorized modification of Real-time Assessment and Real-time monitoring data while being transmitted between Control Centers;

1.2. Identification of where the Responsible Entity applied security protection for transmitting Real-time Assessment and Real-time monitoring data between Control Centers; and

1.3. If the Control Centers are owned or operated by different Responsible Entities, identification of the responsibilities of each Responsible Entity for applying security protection to the transmission of Real-time Assessment and Real-time monitoring data between those Control Centers.

M1. Evidence may include, but is not limited to, documented plan(s) that meet the security objective of Requirement R1 and documentation demonstrating the implementation of the plan(s).

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: "Compliance Enforcement Authority" (CEA) means NERC, the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation.

- The Responsible Entities shall keep data or evidence of each Requirement in this Reliability Standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	N/A	The Responsible Entity documented its plan(s) but failed to include one of the applicable Parts of the plan as specified in Requirement R1.	The Responsible Entity documented its plan(s) but failed to include two of the applicable Parts of the plan as specified in Requirement R1.	The Responsible Entity failed to document plan(s) for Requirement R1; Or The Responsible Entity failed to implement any Part of its plan(s) for Requirement R1, except under CIP Exceptional Circumstances.

D. Regional Variances

None.

E. Associated Documents

Implementation Plan.

Technical Rationale for CIP-012-1.

Implementation Guidance.

Version History

Version	Date	Action	Change Tracking
1		Respond to FERC Order No. 822	New
1	August 16, 2018	Adopted by NERC Board of Trustees	
1	January 23, 2020	FERC Order issued approving CIP-012-1. Docket No. RM18-20-000;	

Appendix CIP-012-1-QC-1
Specific provisions applicable in Québec for standard
CIP-012-1 – Cyber Security – Communications between Control Centers

This appendix establishes specific provisions for the application of the standard in Québec. Provisions of the standard and of this appendix must be read jointly for comprehension and interpretation purposes. Where the standard and appendix differ, the appendix shall prevail.

A. Introduction

1. Title: No specific provisions.

2. Number: No specific provisions.

3. Purpose: No specific provisions.

4. Applicability:

4.1. Functional Entities

No specific provisions.

Facilities

When applying the CIP-012-1 standard, the definition of Control Center reads as follows: One or more facilities operating personnel that monitor and control the Main Transmission System (RTP) in real-time to perform the reliability tasks, including their associated data centers, of: 1) a Reliability Coordinator, 2) a Balancing Authority, 3) a Transmission Operator for transmission Facilities at two or more locations, or 4) a Generator Operator for generation Facilities at two or more locations.

4.2. Exemptions

No specific provisions.

5. Effective date:

5.1. Adoption of the standard by the Régie de l'énergie: April 8th, 2022

5.2. Adoption of this appendix by the Régie de l'énergie: April 8th, 2022

5.3. Effective date of the standard and of its appendix in Québec: July 1st, 2024

B. Requirements and Measures

No specific provisions.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

In Québec, "Compliance Enforcement Authority" means the Régie de l'énergie in its roles of monitoring and enforcing compliance with respect to the Reliability Standard and to this appendix.

1.2. Evidence Retention

No specific provisions.

1.3. Compliance Monitoring and Enforcement Program

The Régie de l'énergie establishes the monitoring processes used to evaluate data or information for the purpose of determining compliance or non-compliance with the Reliability Standard and with this appendix.

Violation Severity Levels

No specific provisions

D. Regional Variances

No specific provisions.

E. Associated Documents

No specific provisions.

Version History

Version	Date	Action	Change tracking
1	April 8, 2022	New appendix as per decision D-2022-048	New

A. Introduction

1. **Title:** **Cyber Security - Supply Chain Risk Management**

2. **Number:** **CIP-013-2**

3. **Purpose:** To mitigate cyber security risks to the reliable operation of the Bulk Electric System (BES) by implementing security controls for supply chain risk management of BES Cyber Systems.

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1. Balancing Authority

   4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1. Is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2. Performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.3. Generator Operator

   4.1.4. Generator Owner

   4.1.5. Reliability Coordinator

   4.1.6. Transmission Operator

   4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. Is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. Performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-013-2:

4.2.3.1. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESPs).

4.2.3.3. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the identification and categorization process required by CIP-002 or any subsequent version of that Reliability Standard.

5. Effective Date: See Implementation Plan for Project 2019-03.

B. Requirements and Measures

R1. Each Responsible Entity shall develop one or more documented supply chain cyber security risk management plan(s) for high and medium impact BES Cyber Systems and their associated Electronic Access Control or Monitoring Systems (EACMS) and Physical Access Control Systems (PACS). The plan(s) shall include: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1. One or more process(es) used in planning for the procurement of BES Cyber Systems and their associated EACMS and PACS to identify and assess cyber security risk(s) to the Bulk Electric System from vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s).

1.2. One or more process(es) used in procuring BES Cyber Systems, and their associated EACMS and PACS, that address the following, as applicable:

1.2.1. Notification by the vendor of vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;

1.2.2. Coordination of responses to vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;

1.2.3. Notification by vendors when remote or onsite access should no longer be granted to vendor representatives;

1.2.4. Disclosure by vendors of known vulnerabilities related to the products or services provided to the Responsible Entity;

1.2.5. Verification of software integrity and authenticity of all software and patches provided by the vendor for use in the BES Cyber System and their associated EACMS and PACS; and

1.2.6. Coordination of controls for vendor-initiated remote access.

M1. Evidence shall include one or more documented supply chain cyber security risk management plan(s) as specified in the Requirement.

R2. Each Responsible Entity shall implement its supply chain cyber security risk management plan(s) specified in Requirement R1. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

Note: Implementation of the plan does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders). Additionally, the following issues are beyond the scope of Requirement R2: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.

M2. Evidence shall include documentation to demonstrate implementation of the supply chain cyber security risk management plan(s), which could include, but is not limited to, correspondence, policy documents, or working documents that demonstrate use of the supply chain cyber security risk management plan.

R3. Each Responsible Entity shall review and obtain CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) specified in Requirement R1 at least once every 15 calendar months. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. Evidence shall include the dated supply chain cyber security risk management plan(s) approved by the CIP Senior Manager or delegate(s) and additional evidence to demonstrate review of the supply chain cyber security risk management plan(s). Evidence may include, but is not limited to, policy documents, revision history, records of review, or workflow evidence from a document management system that indicate review of supply chain risk management plan(s) at least once every 15 calendar months; and documented approval by the CIP Senior Manager or delegate.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority:

"Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention:

The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation.

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program

As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s) which include the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, and include the use of process(es) for procuring BES Cyber Systems and their associated EACMS and PACS, as specified in Part 1.2, but the plans do not include one of the parts in Part 1.2.1 through Part 1.2.6.	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s) which include the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, and include the use of process(es) for procuring BES Cyber Systems and their associated EACMS and PACS, as specified in Part 1.2, but the plans do not include two or more of the parts in Part 1.2.1 through Part 1.2.6.	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s), but the plan(s) did not include the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, or the plan(s) did not include the use of process(es) for procuring BES Cyber Systems and their associated EACMS and PACS, as specified in Part 1.2.	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s), but the plan(s) did not include the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, and the plan(s) did not include the use of process(es) for procuring BES Cyber Systems and their associated EACMS and PACS, as specified in Part 1.2. OR The Responsible Entity did not develop one or more documented supply chain cyber security risk

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				management plan(s) as specified in the Requirement.
R2.	The Responsible Entity implemented its supply chain cyber security risk management plan(s) including the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, and including the use of process(es) for procuring BES Cyber Systems and their associated EACMS and PACS, as specified in Requirement R1 Part 1.2, but did not implement one of the parts in Requirement R1 Part 1.2.1 through Part 1.2.6.	The Responsible Entity implemented its supply chain cyber security risk management plan(s) including the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, and including the use of process(es) for procuring BES Cyber Systems and their associated EACMS and PACS, as specified in Requirement R1 Part 1.2, but did not implement two or more of the parts in Requirement R1 Part 1.2.1 through Part 1.2.6.	The Responsible Entity implemented its supply chain cyber security risk management plan(s), but did not implement the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, or did not implement the use of process(es) for procuring BES Cyber Systems and their associated EACMS and PACS, as specified in Requirement R1 Part 1.2.	The Responsible Entity implemented its supply chain cyber security risk management plan(s), but did not implement the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, and did not implement the use of process(es) for procuring BES Cyber Systems and their associated EACMS and PACS, as specified in Requirement R1 Part 1.2; OR The Responsible Entity did not implement its supply

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				chain cyber security risk management plan(s) specified in the requirement.
R3.	The Responsible Entity reviewed and obtained CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) but did so more than 15 calendar months but less than or equal to 16 calendar months since the previous review as specified in the Requirement.	The Responsible Entity reviewed and obtained CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) but did so more than 16 calendar months but less than or equal to 17 calendar months since the previous review as specified in the Requirement.	The Responsible Entity reviewed and obtained CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) but did so more than 17 calendar months but less than or equal to 18 calendar months since the previous review as specified in the Requirement.	The Responsible Entity did not review and obtain CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) within 18 calendar months of the previous review as specified in the Requirement.

D. Regional Variances

None.

E. Associated Documents

- Implementation Plan for Project 2019-03
- CIP-013-2 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	07/20/17	Respond to FERC Order No. 829.	
1	08/10/17	Approved by the NERC Board of Trustees.	
1	10/18/18	FERC Order approving CIP-013-1. Docket No. RM17-13-000.	
2	08/01/2019	Modified to address directive in FERC Order No. 850.	Revised
2	11/05/2020	Approved by the NERC Board of Trustees.	
2	3/18/2021	FERC Order approving CIP-013-2.Docket No. RD21-2-000.	
2	10/1/2022	Effective Date	

Appendix CIP-013-2-QC-1
Specific provisions applicable in Québec for standard
CIP-013-2 – Cyber Security — Supply Chain Risk Management

This appendix establishes specific provisions for the application of the standard in Québec. Provisions of the standard and of this appendix must be read jointly for comprehension and interpretation purposes. Where the standard and appendix differ, the appendix shall prevail.

A. Introduction

1. Title: No specific provisions.

2. Number: No specific provisions.

3. Purpose: No specific provisions.

4. Applicability:

4.1. Functional Entities

No specific provision.

4.2. Facilities

This standard only applies to the facilities of the Main Transmission System (RTP) and to the facilities specified for the Distribution Provider. In the application of this standard, all reference to the terms "Bulk Electric System" or "BES" shall be replaced by the terms "Main Transmission System" or "RTP" respectively.

Additional Exemptions

The following are exempt from this standard:

- Any generating facility that meets the two following conditions: (1) the nameplate capacity of the facility is 300 MVA or less, and (2) no unit of the facility can be synchronized with a neighbouring system.
- Step-up substations of generating facilities identified in the preceding point.

5. Effective Date:

5.1. Adoption of the standard by the Régie de l'énergie: February 11, 2022

5.2. Adoption of the appendix by the Régie de l'énergie: February 11, 2022

5.3. Effective date of the standard and its appendix in Québec: October 1, 2023

B. Requirements and Measures

No specific provisions.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

In Québec, "Compliance Enforcement Authority" means the Régie de l'énergie in its roles of monitoring and enforcing compliance with respect to the Reliability Standard and to this appendix.

1.2. Evidence Retention

No specific provisions.

1.3. Compliance Monitoring and Enforcement Program

The Régie de l'énergie establishes the monitoring processes used to evaluate data or information for the purpose of determining compliance or non-compliance with the Reliability Standard and with this appendix.

Violation Severity Levels (VSL)

No specific provisions.

D. Regional Variances

No specific provisions.

E. Associated Documents

No specific provisions.

Version History

Version	Date	Action	Change Tracking
1	February 11, 2022	New appendix as per decision D-2022-021.	New

A. Introduction

1. Title: Physical Security

2. Number: CIP-014-3

3. Purpose: To identify and protect Transmission stations and Transmission substations, and their associated primary control centers, that if rendered inoperable or damaged as a result of a physical attack could result in instability, uncontrolled separation, or Cascading within an Interconnection.

4. Applicability:

4.1. Functional Entities:

4.1.1 Transmission Owner that owns a Transmission station or Transmission substation that meets any of the following criteria:

4.1.1.1 Transmission Facilities operated at 500 kV or higher. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.

4.1.1.2 Transmission Facilities that are operating between 200 kV and 499 kV at a single station or substation, where the station or substation is connected at 200 kV or higher voltages to three or more other Transmission stations or substations and has an "aggregate weighted value" exceeding 3000 according to the table below. The "aggregate weighted value" for a single station or substation is determined by summing the "weight value per line" shown in the table below for each incoming and each outgoing BES Transmission Line that is connected to another Transmission station or substation. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.

Voltage Value of a Line	Weight Value per Line
less than 200 kV (not applicable)	(not applicable)
200 kV to 299 kV	700
300 kV to 499 kV	1300
500 kV and above	0

4.1.1.3 Transmission Facilities at a single station or substation location that are identified by its Reliability Coordinator, Planning Coordinator, or

Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.

4.1.1.4 Transmission Facilities identified as essential to meeting Nuclear Plant Interface Requirements.

4.1.2 Transmission Operator.

Exemption: Facilities in a "protected area," as defined in 10 C.F.R. § 73.2, within the scope of a security plan approved or accepted by the Nuclear Regulatory Commission are not subject to this Standard; or, Facilities within the scope of a security plan approved or accepted by the Canadian Nuclear Safety Commission are not subject to this Standard.

5. Effective Dates:

See Implementation Plan for CIP-014-2.

6. Background:

This Reliability Standard addresses the directives from the FERC order issued March 7, 2014, *Reliability Standards for Physical Security Measures*, 146 FERC ¶ 61,166 (2014), which required NERC to develop a physical security reliability standard(s) to identify and protect facilities that if rendered inoperable or damaged could result in instability, uncontrolled separation, or Cascading within an Interconnection.

B. Requirements and Measures

R1. Each Transmission Owner shall perform an initial risk assessment and subsequent risk assessments of its Transmission stations and Transmission substations (existing and planned to be in service within 24 months) that meet the criteria specified in Applicability Section 4.1.1. The initial and subsequent risk assessments shall consist of a transmission analysis or transmission analyses designed to identify the Transmission station(s) and Transmission substation(s) that if rendered inoperable or damaged could result in instability, uncontrolled separation, or Cascading within an Interconnection. *[VRF: High; Time-Horizon: Long-term Planning]*

1.1. Subsequent risk assessments shall be performed:

- At least once every 30 calendar months for a Transmission Owner that has identified in its previous risk assessment (as verified according to Requirement R2) one or more Transmission stations or Transmission substations that if rendered inoperable or damaged could result in instability, uncontrolled separation, or Cascading within an Interconnection; or

- At least once every 60 calendar months for a Transmission Owner that has not identified in its previous risk assessment (as verified according to Requirement R2) any Transmission stations or Transmission substations that if rendered inoperable or damaged could result in instability, uncontrolled separation, or Cascading within an Interconnection.

1.2. The Transmission Owner shall identify the primary control center that operationally controls each Transmission station or Transmission substation identified in the Requirement R1 risk assessment.

M1. Examples of acceptable evidence may include, but are not limited to, dated written or electronic documentation of the risk assessment of its Transmission stations and Transmission substations (existing and planned to be in service within 24 months) that meet the criteria in Applicability Section 4.1.1 as specified in Requirement R1. Additionally, examples of acceptable evidence may include, but are not limited to, dated written or electronic documentation of the identification of the primary control center that operationally controls each Transmission station or Transmission substation identified in the Requirement R1 risk assessment as specified in Requirement R1, Part 1.2.

R2. Each Transmission Owner shall have an unaffiliated third party verify the risk assessment performed under Requirement R1. The verification may occur concurrent with or after the risk assessment performed under Requirement R1. *[VRF: Medium; Time-Horizon: Long-term Planning]*

2.1. Each Transmission Owner shall select an unaffiliated verifying entity that is either:

- A registered Planning Coordinator, Transmission Planner, or Reliability Coordinator; or
- An entity that has transmission planning or analysis experience.

2.2. The unaffiliated third party verification shall verify the Transmission Owner's risk assessment performed under Requirement R1, which may include recommendations for the addition or deletion of a Transmission station(s) or Transmission substation(s). The Transmission Owner shall ensure the verification is completed within 90 calendar days following the completion of the Requirement R1 risk assessment.

2.3. If the unaffiliated verifying entity recommends that the Transmission Owner add a Transmission station(s) or Transmission substation(s) to, or remove a Transmission station(s) or Transmission substation(s) from, its identification under Requirement R1, the Transmission Owner shall either, within 60 calendar days of completion of the verification, for each recommended addition or removal of a Transmission station or Transmission substation:

- Modify its identification under Requirement R1 consistent with the recommendation; or
- Document the technical basis for not modifying the identification in accordance with the recommendation.

2.4. Each Transmission Owner shall implement procedures, such as the use of non-disclosure agreements, for protecting sensitive or confidential information made available to the unaffiliated third party verifier and to protect or exempt sensitive or confidential information developed pursuant to this Reliability Standard from public disclosure.

M2. Examples of acceptable evidence may include, but are not limited to, dated written or electronic documentation that the Transmission Owner completed an unaffiliated third party verification of the Requirement R1 risk assessment and satisfied all of the applicable provisions of Requirement R2, including, if applicable, documenting the technical basis for not modifying the Requirement R1 identification as specified under Part 2.3. Additionally, examples of evidence may include, but are not limited to, written or electronic documentation of procedures to protect information under Part 2.4.

R3. For a primary control center(s) identified by the Transmission Owner according to Requirement R1, Part 1.2 that a) operationally controls an identified Transmission station or Transmission substation verified according to Requirement R2, and b) is not under the operational control of the Transmission Owner: the Transmission Owner shall, within seven calendar days following completion of Requirement R2, notify the Transmission Operator that has operational control of the primary control center of

such identification and the date of completion of Requirement R2. *[VRF: Lower; Time-Horizon: Long-term Planning]*

3.1. If a Transmission station or Transmission substation previously identified under Requirement R1 and verified according to Requirement R2 is removed from the identification during a subsequent risk assessment performed according to Requirement R1 or a verification according to Requirement R2, then the Transmission Owner shall, within seven calendar days following the verification or the subsequent risk assessment, notify the Transmission Operator that has operational control of the primary control center of the removal.

M3. Examples of acceptable evidence may include, but are not limited to, dated written or electronic notifications or communications that the Transmission Owner notified each Transmission Operator, as applicable, according to Requirement R3.

R4. Each Transmission Owner that identified a Transmission station, Transmission substation, or a primary control center in Requirement R1 and verified according to Requirement R2, and each Transmission Operator notified by a Transmission Owner according to Requirement R3, shall conduct an evaluation of the potential threats and vulnerabilities of a physical attack to each of their respective Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 and verified according to Requirement R2. The evaluation shall consider the following: *[VRF: Medium; Time-Horizon: Operations Planning, Long-term Planning]*

4.1. Unique characteristics of the identified and verified Transmission station(s), Transmission substation(s), and primary control center(s);

4.2. Prior history of attack on similar facilities taking into account the frequency, geographic proximity, and severity of past physical security related events; and

4.3. Intelligence or threat warnings received from sources such as law enforcement, the Electric Reliability Organization (ERO), the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), U.S. federal and/or Canadian governmental agencies, or their successors.

M4. Examples of evidence may include, but are not limited to, dated written or electronic documentation that the Transmission Owner or Transmission Operator conducted an evaluation of the potential threats and vulnerabilities of a physical attack to their respective Transmission station(s), Transmission substation(s) and primary control center(s) as specified in Requirement R4.

R5. Each Transmission Owner that identified a Transmission station, Transmission substation, or primary control center in Requirement R1 and verified according to Requirement R2, and each Transmission Operator notified by a Transmission Owner according to Requirement R3, shall develop and implement a documented physical security plan(s) that covers their respective Transmission station(s), Transmission substation(s), and primary control center(s). The physical security plan(s) shall be

developed within 120 calendar days following the completion of Requirement R2 and executed according to the timeline specified in the physical security plan(s). The physical security plan(s) shall include the following attributes: *[VRF: High; Time-Horizon: Long-term Planning]*

5.1. Resiliency or security measures designed collectively to deter, detect, delay, assess, communicate, and respond to potential physical threats and vulnerabilities identified during the evaluation conducted in Requirement R4.

5.2. Law enforcement contact and coordination information.

5.3. A timeline for executing the physical security enhancements and modifications specified in the physical security plan.

5.4. Provisions to evaluate evolving physical threats, and their corresponding security measures, to the Transmission station(s), Transmission substation(s), or primary control center(s).

M5. Examples of evidence may include, but are not limited to, dated written or electronic documentation of its physical security plan(s) that covers their respective identified and verified Transmission station(s), Transmission substation(s), and primary control center(s) as specified in Requirement R5, and additional evidence demonstrating execution of the physical security plan according to the timeline specified in the physical security plan.

R6. Each Transmission Owner that identified a Transmission station, Transmission substation, or primary control center in Requirement R1 and verified according to Requirement R2, and each Transmission Operator notified by a Transmission Owner according to Requirement R3, shall have an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5. The review may occur concurrently with or after completion of the evaluation performed under Requirement R4 and the security plan development under Requirement R5. *[VRF: Medium; Time-Horizon: Long-term Planning]*

6.1. Each Transmission Owner and Transmission Operator shall select an unaffiliated third party reviewer from the following:

- An entity or organization with electric industry physical security experience and whose review staff has at least one member who holds either a Certified Protection Professional (CPP) or Physical Security Professional (PSP) certification.
- An entity or organization approved by the ERO.
- A governmental agency with physical security expertise.

- An entity or organization with demonstrated law enforcement, government, or military physical security expertise.

6.2. The Transmission Owner or Transmission Operator, respectively, shall ensure that the unaffiliated third party review is completed within 90 calendar days of completing the security plan(s) developed in Requirement R5. The unaffiliated third party review may, but is not required to, include recommended changes to the evaluation performed under Requirement R4 or the security plan(s) developed under Requirement R5.

6.3. If the unaffiliated third party reviewer recommends changes to the evaluation performed under Requirement R4 or security plan(s) developed under Requirement R5, the Transmission Owner or Transmission Operator shall, within 60 calendar days of the completion of the unaffiliated third party review, for each recommendation:

- Modify its evaluation or security plan(s) consistent with the recommendation; or

- Document the reason(s) for not modifying the evaluation or security plan(s) consistent with the recommendation.

6.4. Each Transmission Owner and Transmission Operator shall implement procedures, such as the use of non-disclosure agreements, for protecting sensitive or confidential information made available to the unaffiliated third party reviewer and to protect or exempt sensitive or confidential information developed pursuant to this Reliability Standard from public disclosure.

M6. Examples of evidence may include, but are not limited to, written or electronic documentation that the Transmission Owner or Transmission Operator had an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 as specified in Requirement R6 including, if applicable, documenting the reasons for not modifying the evaluation or security plan(s) in accordance with a recommendation under Part 6.3. Additionally, examples of evidence may include, but are not limited to, written or electronic documentation of procedures to protect information under Part 6.4.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence during an on-site visit to show that it was compliant for the full time period since the last audit.

The Transmission Owner and Transmission Operator shall keep data or evidence to show compliance, as identified below, unless directed by its Compliance Enforcement Authority (CEA) to retain specific evidence for a longer period of time as part of an investigation.

The responsible entities shall retain documentation as evidence for three years.

If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved, or for the time specified above, whichever is longer.

The CEA shall keep the last audit records and all requested and submitted subsequent audit records, subject to the confidentiality provisions of Section 1500 of the Rules of Procedure and the provisions of Section 1.4 below.

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints Text

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-3)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Long-term Planning**	**High**	The Transmission Owner performed an initial risk assessment but did so after the date specified in the implementation plan for performing the initial risk assessment but less than or equal to two calendar months after that date; OR The Transmission Owner that has identified in its previous risk assessment one or more Transmission stations or Transmission substations that if rendered inoperable	The Transmission Owner performed an initial risk assessment but did so more than two calendar months after the date specified in the implementation plan for performing the initial risk assessment but less than or equal to four calendar months after that date; OR The Transmission Owner that has identified in its previous risk assessment one or more Transmission stations or Transmission substations that if	The Transmission Owner performed an initial risk assessment but did so more than four calendar months after the date specified in the implementation plan for performing the initial risk assessment but less than or equal to six calendar months after that date; OR The Transmission Owner that has identified in its previous risk assessment one or more Transmission stations or Transmission substations that if rendered inoperable	The Transmission Owner performed an initial risk assessment but did so more than six calendar months after the date specified in the implementation plan for performing the initial risk assessment; OR The Transmission Owner failed to perform an initial risk assessment; OR The Transmission Owner that has identified in its previous risk assessment one or more Transmission

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-3)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			or damaged could result in instability, uncontrolled separation, or Cascading within an Interconnection performed a subsequent risk assessment but did so after 30 calendar months but less than or equal to 32 calendar months; OR The Transmission Owner that has not identified in its previous risk assessment any Transmission stations or Transmission substations that if rendered inoperable or damaged could result in instability, uncontrolled separation, or Cascading within an	rendered inoperable or damaged could result in instability, uncontrolled separation, or Cascading within an Interconnection performed a subsequent risk assessment but did so after 32 calendar months but less than or equal to 34 calendar months; OR The Transmission Owner that has not identified in its previous risk assessment any Transmission stations or Transmission substations that if rendered inoperable or damaged could result in instability, uncontrolled separation, or Cascading within an	or damaged could result in instability, uncontrolled separation, or Cascading within an Interconnection performed a subsequent risk assessment but did so after 34 calendar months but less than or equal to 36 calendar months; OR The Transmission Owner that has not identified in its previous risk assessment any Transmission stations or Transmission substations that if rendered inoperable or damaged could result in instability, uncontrolled separation, or Cascading within an Interconnection	stations or Transmission substations that if rendered inoperable or damaged could result in instability, uncontrolled separation, or Cascading within an Interconnection performed a subsequent risk assessment but did so after more than 36 calendar months; OR The Transmission Owner that has identified in its previous risk assessment one or more Transmission stations or Transmission substations that if rendered inoperable or damaged could result in instability, uncontrolled

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-3)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Interconnection performed a subsequent risk assessment but did so after 60 calendar months but less than or equal to 62 calendar months.	Interconnection performed a subsequent risk assessment but did so after 62 calendar months but less than or equal to 64 calendar months.	performed a subsequent risk assessment but did so after 64 calendar months but less than or equal to 66 calendar months; OR The Transmission Owner performed a risk assessment but failed to include Part 1.2.	separation, or Cascading within an Interconnection failed to perform a risk assessment; OR The Transmission Owner that has not identified in its previous risk assessment any Transmission stations or Transmission substations that if rendered inoperable or damaged could result in instability, uncontrolled separation, or Cascading within an Interconnection performed a subsequent risk assessment but did so after more than 66 calendar months; OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-3)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						The Transmission Owner that has not identified in its previous risk assessment any Transmission station and Transmission substations that if rendered inoperable or damaged could result in instability, uncontrolled separation, or Cascading within an Interconnection failed to perform a subsequent risk assessment.
R2	**Long-term Planning**	**Medium**	The Transmission Owner had an unaffiliated third party verify the risk assessment performed under Requirement R1 but did so in more than 90 calendar days but less than or equal to 100 calendar days	The Transmission Owner had an unaffiliated third party verify the risk assessment performed under Requirement R1 but did so more than 100 calendar days but less than or equal to 110 calendar days	The Transmission Owner had an unaffiliated third party verify the risk assessment performed under Requirement R1 but did so more than 110 calendar days but less than or equal to 120 calendar days	The Transmission Owner had an unaffiliated third party verify the risk assessment performed under Requirement R1 but did so more than 120 calendar days following

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-3)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			following completion of Requirement R1; OR The Transmission Owner had an unaffiliated third party verify the risk assessment performed under Requirement R1 and modified or documented the technical basis for not modifying its identification under Requirement R1 as required by Part 2.3 but did so more than 60 calendar days and less than or equal to 70 calendar days from completion of the third party verification.	following completion of Requirement R1; Or The Transmission Owner had an unaffiliated third party verify the risk assessment performed under Requirement R1 and modified or documented the technical basis for not modifying its identification under Requirement R1 as required by Part 2.3 but did so more than 70 calendar days and less than or equal to 80 calendar days from completion of the third party verification.	following completion of Requirement R1; OR The Transmission Owner had an unaffiliated third party verify the risk assessment performed under Requirement R1 and modified or documented the technical basis for not modifying its identification under Requirement R1 as required by Part 2.3 but did so more than 80 calendar days from completion of the third party verification; OR The Transmission Owner had an unaffiliated third party verify the risk assessment performed under Requirement R1	completion of Requirement R1; OR The Transmission Owner failed to have an unaffiliated third party verify the risk assessment performed under Requirement R1; OR The Transmission Owner had an unaffiliated third party verify the risk assessment performed under Requirement R1 but failed to implement procedures for protecting information per Part 2.4.

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-3)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					but failed to modify or document the technical basis for not modifying its identification under R1 as required by Part 2.3.	
R3	**Long-term Planning**	**Lower**	The Transmission Owner notified the Transmission Operator that operates the primary control center as specified in Requirement R3 but did so more than seven calendar days and less than or equal to nine calendar days following the completion of Requirement R2; OR The Transmission Owner notified the Transmission Operator that operates the primary	The Transmission Owner notified the Transmission Operator that operates the primary control center as specified in Requirement R3 but did so more than nine calendar days and less than or equal to 11 calendar days following the completion of Requirement R2; OR The Transmission Owner notified the Transmission Operator that operates the primary	The Transmission Owner notified the Transmission Operator that operates the primary control center as specified in Requirement R3 but did so more than 11 calendar days and less than or equal to 13 calendar days following the completion of Requirement R2; OR The Transmission Owner notified the Transmission Operator that operates the primary control center of the removal from	The Transmission Owner notified the Transmission Operator that operates the primary control center as specified in Requirement R3 but did so more than 13 calendar days following the completion of Requirement R2; OR The Transmission Owner failed to notify the Transmission Operator that it operates a control

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-3)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			control center of the removal from the identification in Requirement R1 but did so more than seven calendar days and less than or equal to nine calendar days following the verification or the subsequent risk assessment.	control center of the removal from the identification in Requirement R1 but did so more than nine calendar days and less than or equal to 11 calendar days following the verification or the subsequent risk assessment.	the identification in Requirement R1 but did so more than 11 calendar days and less than or equal to 13 calendar days following the verification or the subsequent risk assessment.	center identified in Requirement R1; OR The Transmission Owner notified the Transmission Operator that operates the primary control center of the removal from the identification in Requirement R1 but did so more than 13 calendar days following the verification or the subsequent risk assessment. OR The Transmission Owner failed to notify the Transmission Operator that operates the primary control center of the removal from the

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-3)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						identification in Requirement R1.
R4	**Operations Planning, Long-term Planning**	**Medium**	N/A	The Responsible Entity conducted an evaluation of the potential physical threats and vulnerabilities to each of its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 but failed to consider one of Parts 4.1 through 4.3 in the evaluation.	The Responsible Entity conducted an evaluation of the potential physical threats and vulnerabilities to each of its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 but failed to consider two of Parts 4.1 through 4.3 in the evaluation.	The Responsible Entity failed to conduct an evaluation of the potential physical threats and vulnerabilities to each of its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1; OR The Responsible Entity conducted an evaluation of the potential physical threats and vulnerabilities to each of its Transmission station(s), Transmission

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-3)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						substation(s), and primary control center(s) identified in Requirement R1 but failed to consider Parts 4.1 through 4.3.
R5	**Long-term Planning**	**High**	The Responsible Entity developed and implemented a documented physical security plan(s) that covers each of its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 but did so more than 120 calendar days but less than or equal to 130 calendar days after completing Requirement R2; OR	The Responsible Entity developed and implemented a documented physical security plan(s) that covers each of its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 but did so more than 130 calendar days but less than or equal to 140 calendar days after completing Requirement R2; OR	The Responsible Entity developed and implemented a documented physical security plan(s) that covers each of its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 but did so more than 140 calendar days but less than or equal to 150 calendar days after completing Requirement R2; OR	The Responsible Entity developed and implemented a documented physical security plan(s) that covers each of its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 but did so more than 150 calendar days after completing the verification in Requirement R2; OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-3)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			The Responsible Entity developed and implemented a documented physical security plan(s) that covers its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 and verified according to Requirement R2 but failed to include one of Parts 5.1 through 5.4 in the plan.	The Responsible Entity developed and implemented a documented physical security plan(s) that covers its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 and verified according to Requirement R2 but failed to include two of Parts 5.1 through 5.4 in the plan.	The Responsible Entity developed and implemented a documented physical security plan(s) that covers its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 and verified according to Requirement R2 but failed to include three of Parts 5.1 through 5.4 in the plan.	The Responsible Entity failed to develop and implement a documented physical security plan(s) that covers its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 and verified according to Requirement R2. OR The Responsible Entity developed and implemented a documented physical security plan(s) that covers its Transmission station(s), Transmission substation(s), and primary control

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-3)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						center(s) identified in Requirement R1 and verified according to Requirement 2 but failed to include Parts 5.1 through 5.4 in the plan.
R6	**Long-term Planning**	**Medium**	The Responsible Entity had an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 but did so in more than 90 calendar days but less than or equal to 100 calendar days; OR The Responsible Entity had an unaffiliated third party review the evaluation performed under Requirement	The Responsible Entity had an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 but did so in more than 100 calendar days but less than or equal to 110 calendar days; OR The Responsible Entity had an unaffiliated third party review the evaluation performed	The Responsible Entity had an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 but did so more than 110 calendar days but less than or equal to 120 calendar days; OR The Responsible Entity had an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed	The Responsible Entity failed to have an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 in more than 120 calendar days; OR The Responsible Entity failed to have an unaffiliated third party review the evaluation performed under Requirement R4 and

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-3)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			R4 and the security plan(s) developed under Requirement R5 and modified or documented the reason for not modifying the security plan(s) as specified in Part 6.3 but did so more than 60 calendar days and less than or equal to 70 calendar days following completion of the third party review.	under Requirement R4 and the security plan(s) developed under Requirement R5 and modified or documented the reason for not modifying the security plan(s) as specified in Part 6.3 but did so more than 70 calendar days and less than or equal to 80 calendar days following completion of the third party review.	under Requirement R5 and modified or documented the reason for not modifying the security plan(s) as specified in Part 6.3 but did so more than 80 calendar days following completion of the third party review; OR The Responsible Entity had an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 but did not document the reason for not modifying the security plan(s) as specified in Part 6.3.	the security plan(s) developed under Requirement R5; OR The Responsible Entity had an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 but failed to implement procedures for protecting information per Part 6.4.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	October 1, 2015	Effective Date	New
2	April 16, 2015	Revised to meet FERC Order 802 directive to remove “widespread”.	Revision
2	May 7, 2015	Adopted by the NERC Board of Trustees	
2	July 14, 2015	FERC Letter Order in Docket No. RD15-4-000 approving CIP-014-2	
3	January 19, 2022	Revised to remove Compliance Section 1.4	Revision
3	June 16,2022	FERC Order Docket No. RD22-3-000 approving modifications to CIP014-3	Revision
3	June 16, 2022	Effective Date	

Guidelines and Technical Basis

Section 4 Applicability

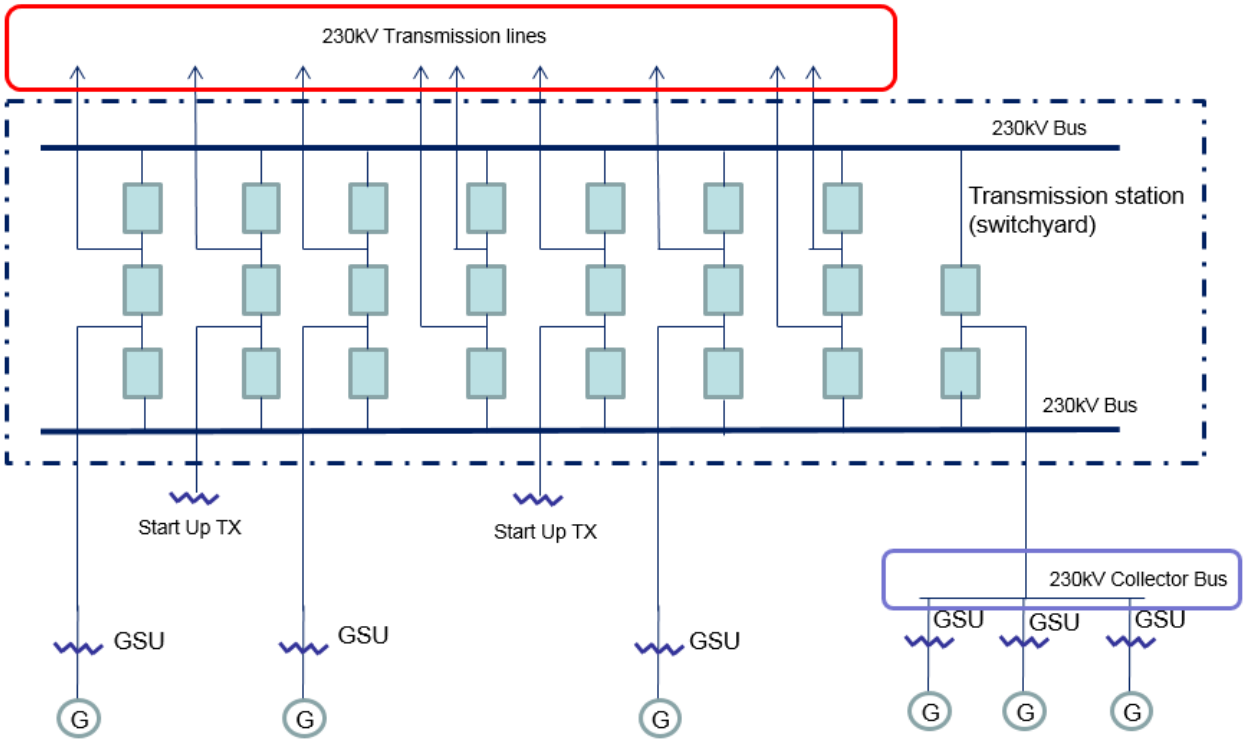
The purpose of Reliability Standard CIP-014 is to protect Transmission stations and Transmission substations, and their associated primary control centers that if rendered inoperable or damaged as a result of a physical attack could result in instability, uncontrolled separation, or Cascading within an Interconnection. To properly include those entities that own or operate such Facilities, the Reliability Standard CIP-014 first applies to Transmission Owners that own Transmission Facilities that meet the specific criteria in Applicability Section 4.1.1.1 through 4.1.1.4. The Facilities described in Applicability Section 4.1.1.1 through 4.1.1.4 mirror those Transmission Facilities that meet the bright line criteria for "Medium Impact" Transmission Facilities under Attachment 1 of Reliability Standard CIP-002-5.1. Each Transmission Owner that owns Transmission Facilities that meet the criteria in Section 4.1.1.1 through 4.1.1.4 is required to perform a risk assessment as specified in Requirement R1 to identify its Transmission stations and Transmission substations, and their associated primary control centers, that if rendered inoperable or damaged as a result of a physical attack could result in instability, uncontrolled separation, or Cascading within an Interconnection. The Standard Drafting Team (SDT) expects this population will be small and that many Transmission Owners that meet the applicability of this standard will not actually identify any such Facilities. Only those Transmission Owners with Transmission stations or Transmission substations identified in the risk assessment (and verified under Requirement R2) have performance obligations under Requirements R3 through R6.

This standard also applies to Transmission Operators. A Transmission Operator's obligations under the standard, however, are only triggered if the Transmission Operator is notified by an applicable Transmission Owner under Requirement R3 that the Transmission Operator operates a primary control center that operationally controls a Transmission station(s) or Transmission substation(s) identified in the Requirement R1 risk assessment. A primary control center operationally controls a Transmission station or Transmission substation when the control center's electronic actions can cause direct physical action at the identified Transmission station or Transmission substation, such as opening a breaker, as opposed to a control center that only has information from the Transmission station or Transmission substation and must coordinate direct action through another entity. Only Transmission Operators who are notified that they have primary control centers under this standard have performance obligations under Requirements R4 through R6. In other words, primary control center for purposes of this Standard is the control center that the Transmission Owner or Transmission Operator, respectively, uses as its primary, permanently-manned site to physically operate a Transmission station or Transmission substation that is identified in Requirement R1 and verified in Requirement R2. Control centers that provide back-up capability are not applicable, as they are a form of resiliency and intentionally redundant.

The SDT considered several options for bright line criteria that could be used to determine applicability and provide an initial threshold that defines the set of Transmission stations and Transmission substations that would meet the directives of the FERC order on physical security (*i.e.*, those that could cause instability, uncontrolled separation, or Cascading within an

Interconnection). The SDT determined that using the criteria for Medium Impact Transmission Facilities in Attachment 1 of CIP-002-5.1 would provide a conservative threshold for defining which Transmission stations and Transmission substations must be included in the risk assessment in Requirement R1 of CIP-014. Additionally, the SDT concluded that using the CIP-002-5.1 Medium Impact criteria was appropriate because it has been approved by stakeholders, NERC, and FERC, and its use provides a technically sound basis to determine which Transmission Owners should conduct the risk assessment. As described in CIP-002-5.1, the failure of a Transmission station or Transmission substation that meets the Medium Impact criteria could have the capability to result in exceeding one or more Interconnection Reliability Operating Limits (IROLs). The SDT understands that using this bright line criteria to determine applicability may require some Transmission Owners to perform risk assessments under Requirement R1 that will result in a finding that none of their Transmission stations or Transmission substations would pose a risk of instability, uncontrolled separation, or Cascading within an Interconnection. However, the SDT determined that higher bright lines could not be technically justified to ensure inclusion of all Transmission stations and Transmission substations, and their associated primary control centers that, if rendered inoperable or damaged as a result of a physical attack could result in instability, uncontrolled separation, or Cascading within an Interconnection. Further guidance and technical basis for the bright line criteria for Medium Impact Facilities can be found in the Guidelines and Technical Basis section of CIP-002-5.1.

Additionally, the SDT determined that it was not necessary to include Generator Operators and Generator Owners in the Reliability Standard. First, Transmission stations or Transmission substations interconnecting generation facilities are considered when determining applicability. Transmission Owners will consider those Transmission stations and Transmission substations that include a Transmission station on the high side of the Generator Step-up transformer (GSU) using Applicability Section 4.1.1.1 and 4.1.1.2. As an example, a Transmission station or Transmission substation identified as a Transmission Owner facility that interconnects generation will be subject to the Requirement R1 risk assessment if it operates at 500kV or greater or if it is connected at 200 kV – 499kV to three or more other Transmission stations or Transmission substations and has an "aggregate weighted value" exceeding 3000 according to the table in Applicability Section 4.1.1.2. Second, the Transmission analysis or analyses conducted under Requirement R1 should take into account the impact of the loss of generation connected to applicable Transmission stations or Transmission substations. Additionally, the FERC order does not explicitly mention generation assets and is reasonably understood to focus on the most critical Transmission Facilities. The diagram below shows an example of a station.



Also, the SDT uses the phrase "Transmission stations or Transmission substations" to recognize the existence of both stations and substations. Many entities in industry consider a substation to be a location with physical borders (i.e. fence, wall, etc.) that contains at least an autotransformer. Locations also exist that do not contain autotransformers, and many entities in industry refer to those locations as stations (switching stations or switchyards). Therefore, the SDT chose to use both "station" and "substation" to refer to the locations where groups of Transmission Facilities exist.

On the issue of joint ownership, the SDT recognizes that this issue is not unique to CIP-014, and expects that the applicable Transmission Owners and Transmission Operators will develop memorandums of understanding, agreements, Coordinated Functional Registrations, or procedures, etc., to designate responsibilities under CIP-014 when joint ownership is at issue, which is similar to what many entities have completed for other Reliability Standards.

The language contained in the applicability section regarding the collector bus is directly copied from CIP-002-5.1, Attachment 1, and has no additional meaning within the CIP-014 standard.

Requirement R1

The initial risk assessment required under Requirement R1 must be completed on or before the effective date of the standard. Subsequent risk assessments are to be performed at least once every 30 or 60 months depending on the results of the previous risk assessment per Requirement R1, Part 1.1. In performing the risk assessment under Requirement R1, the

Transmission Owner should first identify their population of Transmission stations and Transmission substations that meet the criteria contained in Applicability Section 4.1.1. Requirement R1 then requires the Transmission Owner to perform a risk assessment, consisting of a transmission analysis, to determine which of those Transmission stations and Transmission Substations if rendered inoperable or damaged could result in instability, uncontrolled separation, or Cascading within an Interconnection. The requirement is not to require identification of, and thus, not intended to bring within the scope of the standard a Transmission station or Transmission substation unless the applicable Transmission Owner determines through technical studies and analyses based on objective analysis, technical expertise, operating experience and experienced judgment that the loss of such facility would have a critical impact on the operation of the Interconnection in the event the asset is rendered inoperable or damaged. In the November 20, 2014 Order, FERC reiterated that "only an instability that has a "critical impact on the operation of the interconnection" warrants finding that the facility causing the instability is critical under Requirement R1." The Transmission Owner may determine the criteria for critical impact by considering, among other criteria, any of the following:

- Criteria or methodology used by Transmission Planners or Planning Coordinators in TPL-001-4, Requirement R6
- NERC EOP-004-2 reporting criteria
- Area or magnitude of potential impact

The standard does not mandate the specific analytical method for performing the risk assessment. The Transmission Owner has the discretion to choose the specific method that best suites its needs. As an example, an entity may perform a Power Flow analysis and stability analysis at a variety of load levels.

Performing Risk Assessments

The Transmission Owner has the discretion to select a transmission analysis method that fits its facts and system circumstances. To mandate a specific approach is not technically desirable and may lead to results that fail to adequately consider regional, topological, and system circumstances. The following guidance is only an example on how a Transmission Owner may perform a power flow and/or stability analysis to identify those Transmission stations and Transmission substations that if rendered inoperable or damaged as a result of a physical attack could result in instability, uncontrolled separation, or Cascading within an Interconnection. An entity could remove all lines, without regard to the voltage level, to a single Transmission station or Transmission substation and review the simulation results to assess system behavior to determine if Cascading of Transmission Facilities, uncontrolled separation, or voltage or frequency instability is likely to occur over a significant area of the Interconnection. Using engineering judgment, the Transmission Owner (possibly in consultation with regional planning or operation committees and/or ISO/RTO committee input) should develop criteria (e.g. imposing a fault near the removed Transmission station or Transmission substation) to identify a contingency or parameters that result in potential instability, uncontrolled separation, or Cascading within an Interconnection. Regional consultation on these matters is likely to be

helpful and informative, given that the inputs for the risk assessment and the attributes of what constitutes instability, uncontrolled separation, or Cascading within an Interconnection will likely vary from region-to-region or from ISO-to-ISO based on topology, system characteristics, and system configurations. Criteria could also include post-contingency facilities loadings above a certain emergency rating or failure of a power flow case to converge. Available special protection systems (SPS), if any, could be applied to determine if the system experiences any additional instability which may result in uncontrolled separation. Example criteria may include:

(a) Thermal overloads beyond facility emergency ratings;

(b) Voltage deviation exceeding ± 10%; or

(c) Cascading outage/voltage collapse; or

(d) Frequency below under-frequency load shed points

Periodicity

A Transmission Owner who identifies one or more Transmission stations or Transmission substations (as verified under Requirement R2) that if rendered inoperable or damaged could result in instability, uncontrolled separation, or Cascading within an Interconnection is required to conduct a risk assessment at least once every 30 months. This period ensures that the risk assessment remains current with projected conditions and configurations in the planned system. This risk assessment, as the initial assessment, must consider applicable planned Transmission stations and Transmission substations to be in service within 24 months. The 30 month timeframe aligns with the 24 month planned to be in service date because the Transmission Owner is provided the flexibility, depending on its planning cycle and the frequency in which it may plan to construct a new Transmission station or Transmission substation to more closely align these dates. The requirement is to conduct the risk assessment at least once every 30 months, so for a Transmission Owner that believes it is better to conduct a risk assessment once every 24 months, because of its planning cycle, it has the flexibility to do so.

Transmission Owners that have not identified any Transmission stations or Transmission substations (as verified under Requirement R2) that if rendered inoperable or damaged could result in instability, uncontrolled separation, or Cascading within an Interconnection are unlikely to see changes to their risk assessment in the Near-Term Planning Horizon. Consequently, a 60 month periodicity for completing a subsequent risk assessment is specified.

Identification of Primary Control Centers

After completing the risk assessment specified in Requirement R1, it is important to additionally identify the primary control center that operationally controls each Transmission station or Transmission substation that if rendered inoperable or damaged could result in instability, uncontrolled separation, or Cascading within an Interconnection. A primary control center

"operationally controls" a Transmission station or Transmission substation when the control center's electronic actions can cause direct physical actions at the identified Transmission station and Transmission substation, such as opening a breaker.

Requirement R2

This requirement specifies verification of the risk assessment performed under Requirement R1 by an entity other than the owner or operator of the Requirement R1 risk assessment.

A verification of the risk assessment by an unaffiliated third party, as specified in Requirement R2, could consist of:

1. Certifying that the Requirement R1 risk assessment considers the Transmission stations and Transmission substations identified in Applicability Section 4.1.1.
2. Review of the model used to conduct the risk assessment to ensure it contains sufficient system topology to identify Transmission stations and Transmission substations that if rendered inoperable or damaged could cause instability, uncontrolled separation, or Cascading within an Interconnection.
3. Review of the Requirement R1 risk assessment methodology.

This requirement provides the flexibility for a Transmission Owner to select from unaffiliated registered and non-registered entities with transmission planning or analysis experience to perform the verification of the Requirement R1 risk assessment. The term unaffiliated means that the selected verifying entity cannot be a corporate affiliate (*i.e.,* the verifying or third party reviewer cannot be an entity that corporately controls, is controlled by or is under common control with, the Transmission Owner). The verifying entity also cannot be a division of the Transmission Owner that operates as a functional unit.

The prohibition on registered entities using a corporate affiliate to conduct the verification, however, does not prohibit a governmental entity (e.g., a city, a municipality, a U.S. federal power marketing agency, or any other political subdivision of U.S. or Canadian federal, state, or provincial governments) from selecting as the verifying entity another governmental entity within the same political subdivision. For instance, a U.S. federal power marketing agency may select as its verifier another U.S. federal agency to conduct its verification so long as the selected entity has transmission planning or analysis experience. Similarly, a Transmission Owner owned by a Canadian province can use a separate agency of that province to perform the verification. The verifying entity, however, must still be a third party and cannot be a division of the registered entity that operates as a functional unit.

Requirement R2 also provides that the "verification may occur concurrent with or after the risk assessment performed under Requirement R1." This provision is designed to provide the Transmission Owner the flexibility to work with the verifying entity throughout (*i.e.,* concurrent with) the risk assessment, which for some Transmission Owners may be more efficient and effective. In other words, a Transmission Owner could collaborate with their unaffiliated verifying entity to perform the risk assessment under Requirement R1 such that both Requirement R1 and Requirement R2 are satisfied concurrently. The intent of Requirement R2

is to have an entity other than the owner or operator of the facility to be involved in the risk assessment process and have an opportunity to provide input. Accordingly, Requirement R2 is designed to allow entities the discretion to have a two-step process, where the Transmission Owner performs the risk assessment and subsequently has a third party review that assessment, or a one-step process, where the entity collaborates with a third party to perform the risk assessment.

Characteristics to consider in selecting a third party reviewer could include:

- Registered Entity with applicable planning and reliability functions.
- Experience in power system studies and planning.
- The entity's understanding of the MOD standards, TPL standards, and facility ratings as they pertain to planning studies.
- The entity's familiarity with the Interconnection within which the Transmission Owner is located.

With respect to the requirement that Transmission owners develop and implement procedures for protecting confidential and sensitive information, the Transmission Owner could have a method for identifying documents that require confidential treatment. One mechanism for protecting confidential or sensitive information is to prohibit removal of sensitive or confidential information from the Transmission Owner's site. Transmission Owners could include such a prohibition in a non-disclosure agreement with the verifying entity.

A Technical feasibility study is not required in the Requirement R2 documentation of the technical basis for not modifying the identification in accordance with the recommendation.

On the issue of the difference between a verifier in Requirement R2 and a reviewer in Requirement R6, the SDT indicates that the verifier will confirm that the risk assessment was completed in accordance with Requirement R1, including the number of Transmission stations and substations identified, while the reviewer in Requirement R6 is providing expertise on the manner in which the evaluation of threats was conducted in accordance with Requirement R4, and the physical security plan in accordance with Requirement R5. In the latter situation there is no verification of a technical analysis, rather an application of experience and expertise to provide guidance or recommendations, if needed.

Parts 2.4 and 6.4 require the entities to have procedures to protect the confidentiality of sensitive or confidential information. Those procedures may include the following elements:

1. Control and retention of information on site for third party verifiers/reviewers.
2. Only "need to know" employees, etc., get the information.
3. Marking documents as confidential
4. Securely storing and destroying information when no longer needed.
5. Not releasing information outside the entity without, for example, General Counsel sign-off.

Requirement R3

Some Transmission Operators will have obligations under this standard for certain primary control centers. Those obligations, however, are contingent upon a Transmission Owner first completing the risk assessment specified by Requirement R1 and the verification specified by Requirement R2. Requirement R3 is intended to ensure that a Transmission Operator that has operational control of a primary control center identified in Requirement R1 receive notice so that the Transmission Operator may fulfill the rest of the obligations required in Requirements R4 through R6. Since the timing obligations in Requirements R4 through R6 are based upon completion of Requirement R2, the Transmission Owner must also include within the notice the date of completion of Requirement R2. Similarly, the Transmission Owner must notify the Transmission Operator of any removals from identification that result from a subsequent risk assessment under Requirement R1 or as a result of the verification process under Requirement R2.

Requirement R4

This requirement requires owners and operators of facilities identified by the Requirement R1 risk assessment and that are verified under Requirement R2 to conduct an assessment of potential threats and vulnerabilities to those Transmission stations, Transmission substations, and primary control centers using a tailored evaluation process. Threats and vulnerabilities may vary from facility to facility based on any number of factors that include, but are not limited to, location, size, function, existing physical security protections, and attractiveness as a target.

In order to effectively conduct a threat and vulnerability assessment, the asset owner may be the best source to determine specific site vulnerabilities, but current and evolving threats may best be determined by others in the intelligence or law enforcement communities. A number of resources have been identified in the standard, but many others exist and asset owners are not limited to where they may turn for assistance. Additional resources may include state or local fusion centers, U.S. Department of Homeland Security, Federal Bureau of Investigations (FBI), Public Safety Canada, Royal Canadian Mounted Police, and InfraGard chapters coordinated by the FBI.

The Responsible Entity is required to take a number of factors into account in Parts 4.1 to 4.3 in order to make a risk-based evaluation under Requirement R4.

To assist in determining the current threat for a facility, the prior history of attacks on similarly protected facilities should be considered when assessing probability and likelihood of occurrence at the facility in question.

Resources that may be useful in conducting threat and vulnerability assessments include:

- NERC Security Guideline for the Electricity Sector: Physical Security.
- NERC Security Guideline: Physical Security Response.
- ASIS International General Risk Assessment Guidelines.
- ASIS International Facilities Physical Security Measure Guideline.

- ASIS International Security Management Standard: Physical Asset Protection.
- Whole Building Design Guide - Threat/Vulnerability Assessments.

Requirement R5

This requirement specifies development and implementation of a security plan(s) designed to protect against attacks to the facilities identified in Requirement R1 based on the assessment performed under Requirement R4.

Requirement R5 specifies the following attributes for the physical security plan:

- *Resiliency or security measures designed collectively to deter, detect, delay, assess, communicate, and respond to potential physical threats and vulnerabilities identified during the evaluation conducted in Requirement R4.*

  Resiliency may include, among other things:

  a. System topology changes,

  b. Spare equipment,

  c. Construction of a new Transmission station or Transmission substation.

  While most security measures will work together to collectively harden the entire site, some may be allocated to protect specific critical components. For example, if protection from gunfire is considered necessary, the entity may only install ballistic protection for critical components, not the entire site.

- *Law enforcement contact and coordination information.*

  Examples of such information may be posting 9-1-1 for emergency calls and providing substation safety and familiarization training for local and federal law enforcement, fire department, and Emergency Medical Services.

- *A timeline for executing the physical security enhancements and modifications specified in the physical security plan.*

  Entities have the flexibility to prioritize the implementation of the various resiliency or security enhancements and modifications in their security plan according to risk, resources, or other factors. The requirement to include a timeline in the physical security plan for executing the actual physical security enhancements and modifications does not also require that the enhancements and modifications be completed within 120 days. The actual timeline may extend beyond the 120 days, depending on the amount of work to be completed.

- *Provisions to evaluate evolving physical threats, and their corresponding security measures, to the Transmission station(s), Transmission substation(s), or primary control center(s).*

  A registered entity's physical security plan should include processes and responsibilities for obtaining and handling alerts, intelligence, and threat warnings from various

sources. Some of these sources could include the ERO, ES-ISAC, and US and/or Canadian federal agencies. This information should be used to reevaluate or consider changes in the security plan and corresponding security measures of the security plan found in R5.

Incremental changes made to the physical security plan prior to the next required third party review do not require additional third party reviews.

Requirement R6

This requirement specifies review by an entity other than the Transmission Owner or Transmission Operator with appropriate expertise for the evaluation performed according to Requirement R4 and the security plan(s) developed according to Requirement R5. As with Requirement R2, the term unaffiliated means that the selected third party reviewer cannot be a corporate affiliate (*i.e.,* the third party reviewer cannot be an entity that corporately controls, is controlled by or is under common control with, the Transmission Operator). A third party reviewer also cannot be a division of the Transmission Operator that operates as a functional unit.

As noted in the guidance for Requirement R2, the prohibition on registered entities using a corporate affiliate to conduct the review, however, does not prohibit a governmental entity from selecting as the third party reviewer another governmental entity within the same political subdivision. For instance, a city or municipality may use its local enforcement agency, so long as the local law enforcement agency satisfies the criteria in Requirement R6. The third party reviewer, however, must still be a third party and cannot be a division of the registered entity that operates as a functional unit.

The Responsible Entity can select from several possible entities to perform the review:

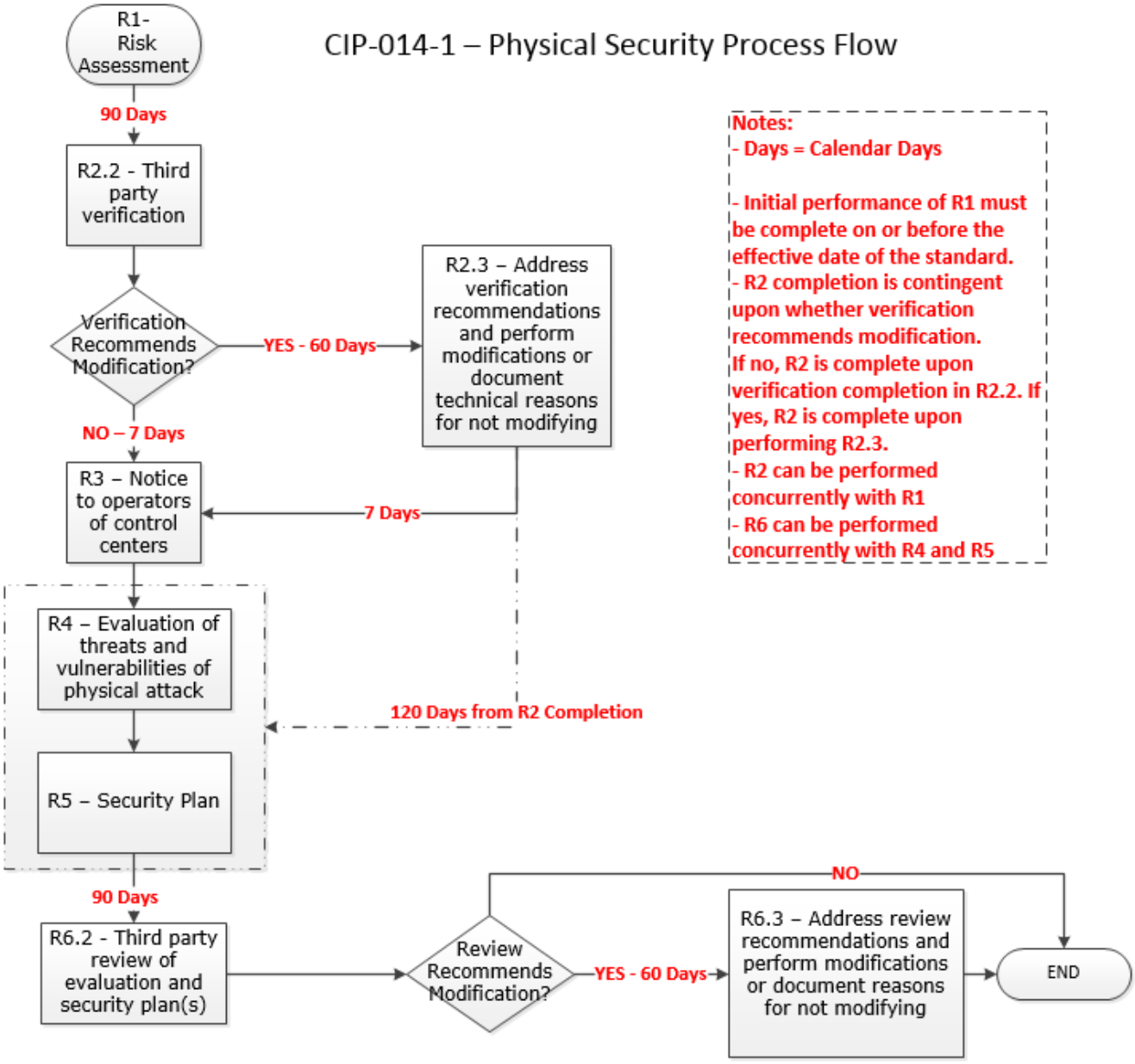
- *An entity or organization with electric industry physical security experience and whose review staff has at least one member who holds either a Certified Protection Professional (CPP) or Physical Security Professional (PSP) certification.*

  In selecting CPP and PSP for use in this standard, the SDT believed it was important that if a private entity such as a consulting or security firm was engaged to conduct the third party review, they must tangibly demonstrate competence to conduct the review. This includes electric industry physical security experience and either of the premier security industry certifications sponsored by ASIS International. The ASIS certification program was initiated in 1977, and those that hold the CPP certification are board certified in security management. Those that hold the PSP certification are board certified in physical security.

- *An entity or organization approved by the ERO.*
- *A governmental agency with physical security expertise.*
- *An entity or organization with demonstrated law enforcement, government, or military physical security expertise.*

As with the verification under Requirement R2, Requirement R6 provides that the "review may occur concurrently with or after completion of the evaluation performed under Requirement R4 and the security plan development under Requirement R5." This provision is designed to provide applicable Transmission Owners and Transmission Operators the flexibility to work with the third party reviewer throughout (*i.e.,* concurrent with) the evaluation performed according to Requirement R4 and the security plan(s) developed according to Requirement R5, which for some Responsible Entities may be more efficient and effective. In other words, a Transmission Owner or Transmission Operator could collaborate with their unaffiliated third party reviewer to perform an evaluation of potential threats and vulnerabilities (Requirement R4) and develop a security plan (Requirement R5) to satisfy Requirements R4 through R6 simultaneously. The intent of Requirement R6 is to have an entity other than the owner or operator of the facility to be involved in the Requirement R4 evaluation and the development of the Requirement R5 security plans and have an opportunity to provide input on the evaluation and the security plan. Accordingly, Requirement R6 is designed to allow entities the discretion to have a two-step process, where the Transmission Owner performs the evaluation and develops the security plan itself and then has a third party review that assessment, or a one-step process, where the entity collaborates with a third party to perform the evaluation and develop the security plan.

Timeline


CIP-014-1 – Physical Security Process Flow
R1- Risk Assessment
90 Days
R2.2 - Third party verification
Verification Recommends Modification?
YES - 60 Days
R2.3 – Address verification recommendations and perform modifications or document technical reasons for not modifying
NO – 7 Days
R3 – Notice to operators of control centers
7 Days
R4 – Evaluation of threats and vulnerabilities of physical attack
120 Days from R2 Completion
R5 – Security Plan
90 Days
R6.2 - Third party review of evaluation and security plan(s)
Review Recommends Modification?
YES - 60 Days
R6.3 – Address review recommendations and perform modifications or document reasons for not modifying
NO
END
Notes:
- Days = Calendar Days
- Initial performance of R1 must be complete on or before the effective date of the standard.
- R2 completion is contingent upon whether verification recommends modification. If no, R2 is complete upon verification completion in R2.2. If yes, R2 is complete upon performing R2.3.
- R2 can be performed concurrently with R1
- R6 can be performed concurrently with R4 and R5

Rationale

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for Requirement R1:
This requirement meets the FERC directive from paragraph 6 of its March 7, 2014 order on physical security to perform a risk assessment to identify which facilities if rendered inoperable or damaged could impact an Interconnection through instability, uncontrolled separation, or cascading failures. The requirement is not intended to bring within the scope of the standard a Transmission station or Transmission substation unless the applicable Transmission Owner determines through technical studies and analyses based on objective analysis, technical expertise, operating experience and experienced judgment that the loss of such facility would have a critical impact on the operation of the Interconnection in the event the asset is rendered inoperable or damaged. In the November 20, 2014 Order, FERC reiterated that "only an instability that has a "critical impact on the operation of the interconnection" warrants finding that the facility causing the instability is critical under Requirement R1." The Transmission Owner may determine the criteria for critical impact by considering, among other criteria, any of the following:

- Criteria or methodology used by Transmission Planners or Planning Coordinators in TPL-001-4, Requirement R6
- NERC EOP-004-2 reporting criteria
- Area or magnitude of potential impact

Requirement R1 also meets the FERC directive for periodic reevaluation of the risk assessment by requiring the risk assessment to be performed every 30 months (or 60 months for an entity that has not identified in a previous risk assessment any Transmission stations or Transmission substations that if rendered inoperable or damaged could result in instability, uncontrolled separation, or Cascading within an Interconnection).

After identifying each Transmission station and Transmission substation that meets the criteria in Requirement R1, it is important to additionally identify the primary control center that operationally controls that Transmission station or Transmission substation (*i.e.,* the control center whose electronic actions can cause direct physical actions at the identified Transmission station and Transmission substation, such as opening a breaker, compared to a control center that only has the ability to monitor the Transmission station and Transmission substation and, therefore, must coordinate direct physical action through another entity).

Rationale for Requirement R2:
This requirement meets the FERC directive from paragraph 11 in the order on physical security requiring verification by an entity other than the owner or operator of the risk assessment performed under Requirement R1.

This requirement provides the flexibility for a Transmission Owner to select registered and non-registered entities with transmission planning or analysis experience to perform the verification of the Requirement R1 risk assessment. The term "unaffiliated" means that the selected verifying entity cannot be a corporate affiliate (*i.e.*, the verifying entity cannot be an entity that controls, is controlled by, or is under common control with, the Transmission owner). The verifying entity also cannot be a division of the Transmission Owner that operates as a functional unit. The term "unaffiliated" is not intended to prohibit a governmental entity from using another government entity to be a verifier under Requirement R2.

Requirement R2 also provides the Transmission Owner the flexibility to work with the verifying entity throughout the Requirement R1 risk assessment, which for some Transmission Owners may be more efficient and effective. In other words, a Transmission Owner could coordinate with their unaffiliated verifying entity to perform a Requirement R1 risk assessment to satisfy both Requirement R1 and Requirement R2 concurrently.

Planning Coordinator is a functional entity listed in Part 2.1. The Planning Coordinator and Planning Authority are the same entity as shown in the NERC Glossary of Terms Used in NERC Reliability Standards.

Rationale for Requirement R3:
Some Transmission Operators will have obligations under this standard for certain primary control centers. Those obligations, however, are contingent upon a Transmission Owner first identifying which Transmission stations and Transmission substations meet the criteria specified by Requirement R1, as verified according to Requirement R2. This requirement is intended to ensure that a Transmission Operator that has operational control of a primary control center identified in Requirement R1, Part 1.2 of a Transmission station or Transmission substation verified according to Requirement R2 receives notice of such identification so that the Transmission Operator may timely fulfill its resulting obligations under Requirements R4 through R6. Since the timing obligations in Requirements R4 through R6 are based upon completion of Requirement R2, the Transmission Owner must also include notice of the date of completion of Requirement R2. Similarly, the Transmission Owner must notify the Transmission Operator of any removals from identification that result from a subsequent risk assessment under Requirement R1 or the verification process under Requirement R2.

Rationale for Requirement R4:
This requirement meets the FERC directive from paragraph 8 in the order on physical security that the reliability standard must require tailored evaluation of potential threats and vulnerabilities to facilities identified in Requirement R1 and verified according to Requirement R2. Threats and vulnerabilities may vary from facility to facility based on factors such as the facility's location, size, function, existing protections, and attractiveness of the target. As such, the requirement does not mandate a one-size-fits-all approach but requires entities to account for the unique characteristics of their facilities.

Requirement R4 does not explicitly state when the evaluation of threats and vulnerabilities must occur or be completed. However, Requirement R5 requires that the entity's security

plan(s), which is dependent on the Requirement R4 evaluation, must be completed within 120 calendar days following completion of Requirement R2. Thus, an entity has the flexibility when to complete the Requirement R4 evaluation, provided that it is completed in time to comply with the requirement in Requirement R5 to develop a physical security plan 120 calendar days following completion of Requirement R2.

Rationale for Requirement R5:
This requirement meets the FERC directive from paragraph 9 in the order on physical security requiring the development and implementation of a security plan(s) designed to protect against attacks to the facilities identified in Requirement R1 based on the assessment performed under Requirement R4.

Rationale for Requirement R6:
This requirement meets the FERC directive from paragraph 11 in the order on physical security requiring review by an entity other than the owner or operator with appropriate expertise of the evaluation performed according to Requirement R4 and the security plan(s) developed according to Requirement R5.

As with the verification required by Requirement R2, Requirement R6 provides Transmission Owners and Transmission Operators the flexibility to work with the third party reviewer throughout the Requirement R4 evaluation and the development of the Requirement R5 security plan(s). This would allow entities to satisfy their obligations under Requirement R6 concurrent with the satisfaction of their obligations under Requirements R4 and R5.

Appendix CIP-014-3-QC-1
Specific provisions applicable in Québec for standard CIP-014-2 —Physical Security

This appendix establishes specific provisions for the application of the standard in Québec. Provisions of the standard and of this appendix must be read jointly for the comprehension and interpretation purposes. Where the standard and appendix differ, the appendix shall prevail.

A. Introduction

1. Title: No specific provision.

2. Number: No specific provision.

3. Purpose: No specific provision.

4. Applicability:

4.1. Functional Entities

No specific provision.

Facilities

This standard only applies to the facilities of the Main Transmission System (RTP) that meet the criteria established in the "Applicability" section. In application of this standard, any reference to the term "BES" shall be replaced by the term "RTP".

5. Effective Date:

5.1. Adoption of the standard by the Régie de l'énergie: November 18, 2022

5.2. Adoption of the appendix by the Régie de l'énergie: November 18, 2022

5.3. Effective date of the standard and its appendix in Québec: April 1, 2023

6. Background: No specific provision.

B. Requirements and Measures

No specific provision.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

In Québec, "Compliance Enforcement Authority" means the Régie de l'énergie in its roles of monitoring and enforcing compliance with respect to the Reliability Standard and to this appendix.

1.2. Evidence Retention

In Québec, the CEA is subject to the confidentiality provisions as specified in applicable sections of the "Québec Reliability Standards Compliance Monitoring and Enforcement Program (QCMEP)".

1.3. Compliance Monitoring and Assessment Processes

No specific provision.

2. Table of Compliance Elements

No specific provision.

D. Regional Variances

No specific provision.

E. Interpretations

No specific provision.

F. Associated Documents

No specific provision.

Guidelines and Technical Basis

No specific provision.

Rationale

No specific provision.

Version History

Version	Date	Action	Change Tracking
1	November 18, 2022	New appendix as per decision D-2022-133.	New

A. Introduction

1. **Title:** **Communications**

2. **Number:** **COM-001-3**

3. **Purpose:** To establish Interpersonal Communication capabilities necessary to maintain reliability.

4. **Applicability:**

   4.1. Functional Entities:

   4.1.1. Transmission Operator

   4.1.2. Balancing Authority

   4.1.3. Reliability Coordinator

   4.1.4. Distribution Provider

   4.1.5. Generator Operator

5. **Effective Date:** See Implementation Plan

B. Requirements and Measures

R1. Each Reliability Coordinator shall have Interpersonal Communication capability with the following entities (unless the Reliability Coordinator detects a failure of its Interpersonal Communication capability in which case Requirement R10 shall apply): *[Violation Risk Factor: High] [Time Horizon: Real-time Operations]*

1.1. All Transmission Operators and Balancing Authorities within its Reliability Coordinator Area.

1.2. Each adjacent Reliability Coordinator within the same Interconnection.

M1. Each Reliability Coordinator shall have and provide upon request evidence that it has Interpersonal Communication capability with all Transmission Operators and Balancing Authorities within its Reliability Coordinator Area and with each adjacent Reliability Coordinator within the same Interconnection, which could include, but is not limited to:

- physical assets, or
- dated evidence, such as, equipment specifications and installation documentation, test records, operator logs, voice recordings, transcripts of voice recordings, or electronic communications. (R1.)

R2. Each Reliability Coordinator shall designate an Alternative Interpersonal Communication capability with the following entities: *[Violation Risk Factor: High] [Time Horizon: Real-time Operations]*

2.1. All Transmission Operators and Balancing Authorities within its Reliability Coordinator Area.

2.2. Each adjacent Reliability Coordinator within the same Interconnection.

M2. Each Reliability Coordinator shall have and provide upon request evidence that it designated an Alternative Interpersonal Communication capability with all Transmission Operators and Balancing Authorities within its Reliability Coordinator Area and with each adjacent Reliability Coordinator within the same Interconnection, which could include, but is not limited to:

- physical assets, or
- dated evidence, such as, equipment specifications and installation documentation, test records, operator logs, voice recordings, transcripts of voice recordings, or electronic communications. (R2.)

R3. Each Transmission Operator shall have Interpersonal Communication capability with the following entities (unless the Transmission Operator detects a failure of its Interpersonal Communication capability in which case Requirement R10 shall apply): *[Violation Risk Factor: High] [Time Horizon: Real-time Operations]*

3.1. Its Reliability Coordinator.

3.2. Each Balancing Authority within its Transmission Operator Area.

3.3. Each Distribution Provider within its Transmission Operator Area.

3.4. Each Generator Operator within its Transmission Operator Area.

3.5. Each adjacent Transmission Operator synchronously connected.

3.6. Each adjacent Transmission Operator asynchronously connected.

M3. Each Transmission Operator shall have and provide upon request evidence that it has Interpersonal Communication capability with its Reliability Coordinator, each Balancing Authority, Distribution Provider, and Generator Operator within its Transmission Operator Area, and each adjacent Transmission Operator asynchronously or synchronously connected, which could include, but is not limited to:

- Physical assets, or
- Dated evidence, such as, equipment specifications and installation documentation, test records, operator logs, voice recordings, transcripts of voice recordings, or electronic communication. (R3.)

R4. Each Transmission Operator shall designate an Alternative Interpersonal Communication capability with the following entities: *[Violation Risk Factor: High] [Time Horizon: Real-time Operations]*

4.1. Its Reliability Coordinator.

4.2. Each Balancing Authority within its Transmission Operator Area.

4.3. Each adjacent Transmission Operator synchronously connected.

4.4. Each adjacent Transmission Operator asynchronously connected.

M4. Each Transmission Operator shall have and provide upon request evidence that it designated an Alternative Interpersonal Communication capability with its Reliability Coordinator, each Balancing Authority within its Transmission Operator Area, and each adjacent Transmission Operator asynchronously and synchronously connected, which could include, but is not limited to:

- Physical assets, or
- Dated evidence, such as, equipment specifications and installation documentation, test records, operator logs, voice recordings, transcripts of voice recordings, or electronic communications. (R4.)

R5. Each Balancing Authority shall have Interpersonal Communication capability with the following entities (unless the Balancing Authority detects a failure of its Interpersonal Communication capability in which case Requirement R10 shall apply): *[Violation Risk Factor: High] [Time Horizon: Real-time Operations]*

5.1. Its Reliability Coordinator.

5.2. Each Transmission Operator that operates Facilities within its Balancing Authority Area.

5.3. Each Distribution Provider within its Balancing Authority Area.

5.4. Each Generator Operator that operates Facilities within its Balancing Authority Area.

5.5. Each Adjacent Balancing Authority.

M5. Each Balancing Authority shall have and provide upon request evidence that it has Interpersonal Communication capability with its Reliability Coordinator, each Transmission Operator and Generator Operator that operates Facilities within its Balancing Authority Area, each Distribution Provider within its Balancing Authority Area, and each adjacent Balancing Authority, which could include, but is not limited to:

- Physical assets, or
- Dated evidence, such as, equipment specifications and installation documentation, test records, operator logs, voice recordings, transcripts of voice recordings, or electronic communications. (R5.)

R6. Each Balancing Authority shall designate an Alternative Interpersonal Communication capability with the following entities: *[Violation Risk Factor: High] [Time Horizon: Real-time Operations]*

6.1. Its Reliability Coordinator.

6.2. Each Transmission Operator that operates Facilities within its Balancing Authority Area.

6.3. Each Adjacent Balancing Authority.

M6. Each Balancing Authority shall have and provide upon request evidence that it designated an Alternative Interpersonal Communication capability with its Reliability Coordinator, each Transmission Operator that operates Facilities within its Balancing Authority Area, and each adjacent Balancing Authority, which could include, but is not limited to:

- Physical assets, or
- Dated evidence, such as, equipment specifications and installation documentation, test records, operator logs, voice recordings, transcripts of voice recordings, or electronic communications. (R6.)

R7. Each Distribution Provider shall have Interpersonal Communication capability with the following entities (unless the Distribution Provider detects a failure of its Interpersonal Communication capability in which case Requirement R11 shall apply): *[Violation Risk Factor: Medium] [Time Horizon: Real-time Operations]*

7.1. Its Balancing Authority.

7.2. Its Transmission Operator.

M7. Each Distribution Provider shall have and provide upon request evidence that it has Interpersonal Communication capability with its Transmission Operator and its Balancing Authority, which could include, but is not limited to:

- Physical assets, or
- Dated evidence, such as, equipment specifications and installation documentation, test records, operator logs, voice recordings, transcripts of voice recordings, or electronic communications. (R7.)

R8. Each Generator Operator shall have Interpersonal Communication capability with the following entities (unless the Generator Operator detects a failure of its Interpersonal Communication capability in which case Requirement R11 shall apply): *[Violation Risk Factor: High] [Time Horizon: Real-time Operations]*

8.1. Its Balancing Authority.

8.2. Its Transmission Operator.

M8. Each Generator Operator shall have and provide upon request evidence that it has Interpersonal Communication capability with its Balancing Authority and its Transmission Operator, which could include, but is not limited to:

- Physical assets, or
- Dated evidence, such as, equipment specifications and installation documentation, test records, operator logs, voice recordings, transcripts of voice recordings, or electronic communications. (R8.)

R9. Each Reliability Coordinator, Transmission Operator, and Balancing Authority shall test its Alternative Interpersonal Communication capability at least once each calendar month. If the test is unsuccessful, the responsible entity shall initiate action to repair or designate a replacement Alternative Interpersonal Communication capability within 2 hours. *[Violation Risk Factor: Medium][Time Horizon: Real-time Operations, Same-day Operations]*

M9. Each Reliability Coordinator, Transmission Operator, and Balancing Authority shall have and provide upon request evidence that it tested, at least once each calendar month, its Alternative Interpersonal Communication capability designated in Requirements R2, R4, or R6. If the test was unsuccessful, the entity shall have and provide upon request evidence that it initiated action to repair or designated a replacement Alternative Interpersonal Communication capability within 2 hours. Evidence could include, but is not limited to: dated and time-stamped test records, operator logs, voice recordings, transcripts of voice recordings, or electronic communications. (R9.)

R10. Each Reliability Coordinator, Transmission Operator, and Balancing Authority shall notify entities as identified in Requirements R1, R3, and R5, respectively within 60 minutes of the detection of a failure of its Interpersonal Communication capability that lasts 30 minutes or longer. *[Violation Risk Factor: Medium] [Time Horizon: Real-time Operations]*

M10. Each Reliability Coordinator, Transmission Operator, and Balancing Authority shall have and provide upon request evidence that it notified entities as identified in Requirements R1, R3, and R5, respectively within 60 minutes of the detection of a failure of its Interpersonal Communication capability that lasted 30 minutes or longer. Evidence could include, but is not limited to: dated and time-stamped test records, operator logs, voice recordings, transcripts of voice recordings, or electronic communications. (R10.)

R11. Each Distribution Provider and Generator Operator that detects a failure of its Interpersonal Communication capability shall consult each entity affected by the failure, as identified in Requirement R7 for a Distribution Provider or Requirement R8 for a Generator Operator, to determine a mutually agreeable action for the

restoration of its Interpersonal Communication capability. *[Violation Risk Factor: Medium] [Time Horizon: Real-time Operations]*

M11. Each Distribution Provider and Generator Operator that detected a failure of its Interpersonal Communication capability shall have and provide upon request evidence that it consulted with each entity affected by the failure, as identified in Requirement R7 for a Distribution Provider or Requirement R8 for a Generator Operator, to determine mutually agreeable action to restore the Interpersonal Communication capability. Evidence could include, but is not limited to: dated operator logs, voice recordings, transcripts of voice recordings, or electronic communications. (R11.)

R12. Each Reliability Coordinator, Transmission Operator, Generator Operator, and Balancing Authority shall have internal Interpersonal Communication capabilities for the exchange of information necessary for the Reliable Operation of the BES. This includes communication capabilities between Control Centers within the same functional entity, and/or between a Control Center and field personnel. *[Violation Risk Factor: High] [Time Horizon: Real-time Operations]*

M12. Each Reliability Coordinator, Transmission Operator, Generator Operator, and Balancing Authority shall have and provide upon request evidence that it has internal Interpersonal Communication capability, which could include, but is not limited to:

- physical assets, or
- dated evidence, such as, equipment specifications and installation documentation, operating procedures, test records, operator logs, voice recordings, transcripts of voice recordings, or electronic communications.

R13. Each Distribution Provider shall have internal Interpersonal Communication capabilities for the exchange of information necessary for the Reliable Operation of the BES. This includes communication capabilities between control centers within the same functional entity, and/or between a control center and field personnel. *[Violation Risk Factor: Medium] [Time Horizon: Real-time Operations]*

M13. Each Distribution Provider shall have and provide upon request evidence that it has internal Interpersonal Communication capability, which could include, but is not limited to:

- physical assets, or
- dated evidence, such as, equipment specifications and installation documentation, operating procedures, test records, operator logs, voice recordings, transcripts of voice recordings, or electronic communications.

Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority:

"Compliance Enforcement Authority" or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention

The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation:

- The Reliability Coordinator for Requirements R1, R2, R9, and R10, Measures M1, M2, M9, and M10 shall retain written documentation for the most recent twelve calendar months and voice recordings for the most recent 90 calendar days.
- The Transmission Operator for Requirements R3, R4, R9, and R10, Measures M3, M4, M9, and M10 shall retain written documentation for the most recent twelve calendar months and voice recordings for the most recent 90 calendar days.
- The Balancing Authority for Requirements R5, R6, R9, and R10, Measures M5, M6, M9, and M10 shall retain written documentation for the most recent twelve calendar months and voice recordings for the most recent 90 calendar days.
- The Distribution Provider for Requirements R7 and R11, Measures M7 and M11 shall retain written documentation for the most recent twelve calendar months and voice recordings for the most recent 90 calendar days.
- The Generator Operator for Requirements R8 and R11, Measures M8 and M11 shall retain written documentation for the most recent twelve calendar months and voice recordings for the most recent 90 calendar days.
- Responsible entities under Requirement R12, Measure M12 shall retain written documentation for the most recent twelve calendar months and voice recordings for the most recent 90 calendar days.

- Responsible entities under Requirement R13, Measure M13 shall retain written documentation for the most recent twelve calendar months and voice recordings for the most recent 90 calendar days.

1.3. Compliance Monitoring and Enforcement Program

As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	**N/A**	**N/A**	The Reliability Coordinator failed to have Interpersonal Communication capability with one of the entities listed in Requirement R1, Parts 1.1 or 1.2, except when the Reliability Coordinator detected a failure of its Interpersonal Communication capability in accordance with Requirement R10.	The Reliability Coordinator failed to have Interpersonal Communication capability with two or more of the entities listed in Requirement R1, Parts 1.1 or 1.2, except when the Reliability Coordinator detected a failure of its Interpersonal Communication capability in accordance with Requirement R10.
R2.	**N/A**	**N/A**	The Reliability Coordinator failed to designate Alternative Interpersonal Communication capability with one of the entities listed in Requirement R2, Parts 2.1 or 2.2.	The Reliability Coordinator failed to designate Alternative Interpersonal Communication capability with two or more of the entities listed in Requirement R2, Parts 2.1 or 2.2.
R3.	**N/A**	**N/A**	The Transmission Operator failed to have Interpersonal Communication capability	The Transmission Operator failed to have Interpersonal Communication capability

			with one of the entities listed in Requirement R3, Parts 3.1, 3.2, 3.3, 3.4, 3.5, or 3.6, except when the Transmission Operator detected a failure of its Interpersonal Communication capability in accordance with Requirement R10.	with two or more of the entities listed in Requirement R3, Parts 3.1, 3.2, 3.3, 3.4, 3.5, or 3.6, except when the Transmission Operator detected a failure of its Interpersonal Communication capability in accordance with Requirement R10.
R4.	**N/A**	**N/A**	The Transmission Operator failed to designate Alternative Interpersonal Communication capability with one of the entities listed in Requirement R4, Parts 4.1, 4.2, 4.3, or 4.4.	The Transmission Operator failed to designate Alternative Interpersonal Communication capability with two or more of the entities listed in Requirement R4, Parts 4.1, 4.2, 4.3, or 4.4.
R5.	**N/A**	**N/A**	The Balancing Authority failed to have Interpersonal Communication capability with one of the entities listed in Requirement R5, Parts 5.1, 5.2, 5.3, 5.4, or 5.5, except when the Balancing Authority detected a failure of its Interpersonal Communication capability in	The Balancing Authority failed to have Interpersonal Communication capability with two or more of the entities listed in Requirement R5, Parts 5.1, 5.2, 5.3, 5.4, or 5.5, except when the Balancing Authority detected a failure of its Interpersonal Communication capability in

			accordance with Requirement R10.	accordance with Requirement R10.
R6.	**N/A**	**N/A**	The Balancing Authority failed to designate Alternative Interpersonal Communication capability with one of the entities listed in Requirement R6, Parts 6.1, 6.2, or 6.3.	The Balancing Authority failed to designate Alternative Interpersonal Communication capability with two or more of the entities listed in Requirement R6, Parts 6.1, 6.2, or 6.3.
R7.	**N/A**	**N/A**	The Distribution Provider failed to have Interpersonal Communication capability with one of the entities listed in Requirement R7, Parts 7.1 or 7.2, except when the Distribution Provider detected a failure of its Interpersonal Communication capability in accordance with Requirement R11.	The Distribution Provider failed to have Interpersonal Communication capability with two or more of the entities listed in Requirement R7, Parts 7.1 or 7.2, except when the Distribution Provider detected a failure of its Interpersonal Communication capability in accordance with Requirement R11.
R8.	**N/A**	**N/A**	The Generator Operator failed to have Interpersonal Communication capability with one of the entities listed in Requirement R8, Parts 8.1 or 8.2, except when	The Generator Operator failed to have Interpersonal Communication capability with two or more of the entities listed in Requirement R8, Parts 8.1 or

			a Generator Operator detected a failure of its Interpersonal Communication capability in accordance with Requirement R11.	8.2, except when a Generator Operator detected a failure of its Interpersonal Communication capability in accordance with Requirement R11.
R9.	The Reliability Coordinator, Transmission Operator, or Balancing Authority tested the Alternative Interpersonal Communication capability but failed to initiate action to repair or designate a replacement Alternative Interpersonal Communication in more than 2 hours and less than or equal to 4 hours upon an unsuccessful test.	The Reliability Coordinator, Transmission Operator, or Balancing Authority tested the Alternative Interpersonal Communication capability but failed to initiate action to repair or designate a replacement Alternative Interpersonal Communication in more than 4 hours and less than or equal to 6 hours upon an unsuccessful test.	The Reliability Coordinator, Transmission Operator, or Balancing Authority tested the Alternative Interpersonal Communication capability but failed to initiate action to repair or designate a replacement Alternative Interpersonal Communication in more than 6 hours and less than or equal to 8 hours upon an unsuccessful test.	The Reliability Coordinator, Transmission Operator, or Balancing Authority failed to test the Alternative Interpersonal Communication capability once each calendar month. OR The Reliability Coordinator, Transmission Operator, or Balancing Authority tested the Alternative Interpersonal Communication capability but failed to initiate action to repair or designate a replacement Alternative Interpersonal Communication in more than 8 hours upon an unsuccessful test.
R10.	The Reliability Coordinator, Transmission Operator, or	The Reliability Coordinator, Transmission Operator, or	The Reliability Coordinator, Transmission Operator, or	The Reliability Coordinator, Transmission Operator, or

	Balancing Authority failed to notify the entities identified in Requirements R1, R3, and R5, respectively upon the detection of a failure of its Interpersonal Communication capability in more than 60 minutes but less than or equal to 70 minutes.	Balancing Authority failed to notify the entities identified in Requirements R1, R3, and R5, respectively upon the detection of a failure of its Interpersonal Communication capability in more than 70 minutes but less than or equal to 80 minutes.	Balancing Authority failed to notify the entities identified in Requirements R1, R3, and R5, respectively upon the detection of a failure of its Interpersonal Communication capability in more than 80 minutes but less than or equal to 90 minutes.	Balancing Authority failed to notify the entities identified in Requirements R1, R3, and R5, respectively upon the detection of a failure of its Interpersonal Communication capability in more than 90 minutes.
R11.	**N/A**	**N/A**	**N/A**	The Distribution Provider or Generator Operator that detected a failure of its Interpersonal Communication capability failed to consult with each entity affected by the failure, as identified in Requirement R7 for a Distribution Provider or Requirement R8 for a Generator Operator, to determine a mutually agreeable action for the restoration of the Interpersonal Communication capability.
R12.	**N/A**	**N/A**	**N/A**	The Reliability Coordinator, Transmission Operator, Generator Operator, or Balancing Authority failed to

				have internal Interpersonal Communication capability for the exchange of operating information.
R13.	**N/A**	**N/A**	**N/A**	The Distribution Provider failed to have internal Interpersonal Communication capability for the exchange of operating information.

Regional Variances

None.

Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
0	April 1, 2005	Effective Date	New
0	August 8, 2005	Removed “Proposed” from Effective Date	Errata
1	November 1, 2006	Adopted by Board of Trustees	Revised
1	April 4, 2007	Regulatory Approval — Effective Date	New
1	April 6, 2007	Requirement 1, added the word “for” between “facilities” and “the exchange.”	Errata
1.1	October 29, 2008	BOT adopted errata changes; updated version number to “1.1”	Errata
2	November 7, 2012	Adopted by Board of Trustees	Revised in accordance with SAR for Project 2006-06, Reliability Coordination (RC SDT). Replaced R1 with R1-R8; R2 replaced by R9; R3 included within new R1; R4 remains enforce pending Project 2007-02; R5 redundant with EOP-008-0, retiring R5 as redundant with EOP-008-0, R1; retiring R6, relates to ERO procedures; R10 & R11, new.
2	April 16, 2015	FERC Order issued approving COM-001-2	
2.1	August 25, 2015	Changed numbered parts under	2.1
2.1	November 13, 2015	FERC Order issued approving errata to COM-001-2.1	Errata to correct inadvertent numbering errors in the parts to Requirement R6.

3	August 11, 2016	Adopted by the NERC Board of Trustees	New
3	October 28, 2016	FERC letter Order issued approving COM-001-3. Docket No. RD16-9-000.	

Rationale

Rationale for Requirement R12:

The focus of the requirement is on the *capabilities* that an entity must have for the purpose of exchanging information necessary for the Reliable Operation of the BES. That is, the entity must have the capability to communicate internally by, "any medium that allows two or more individuals to interact, consult, or exchange information." The standard does not prescribe the specific type of capability (*i.e.,* hardware or software). The determination of the appropriate type of capability is left to the entity. Regardless, the entity must have the capability to exchange information *whenever* the internal Interpersonal Communications may directly impact operations of the BES. Therefore, the applicable entities must have the capability to exchange information between Control Centers of that functional entity. For example, a TOP with multiple control centers that are geographical separated must have the capability to communicate internally between or among those control centers. The communication capability may occur through any medium that supports Interpersonal Communication, such as land line telephone, cellular device, Voice Over Internet Protocol (VOIP), satellite telephone, radio, or electronic message. Also, applicable entities must have the capability to exchange information between a Control Center and field personnel. For example, a TOP system operator providing instruction to a field personnel to perform a reliability activity, such as switching Facilities.

In the course of normal control center operation, system operators within a single Control Center communicate as needed to ensure the reliability of the BES, including face-to-face communications. These internal communications are ongoing and occur throughout the day as part of day-to-day operations. However, these types of communications are not the focus of this requirement. The focus is on the capability of an entity to communicate internally where face-to-face communications are not available.

Rationale for Requirement R13:

The NERC Glossary definition for "Control Center" was not used in this requirement because Distribution Provider is not listed as an entity within the definition. The Glossary definition for "Control Center" is, "[o]ne or more facilities hosting operating personnel that monitor and control the Bulk Electric System (BES) in real-time to perform the reliability tasks, including their associated data centers, of: 1) a Reliability Coordinator, 2) a Balancing Authority, 3) a Transmission Operator for transmission Facilities at two or more locations, or 4) a Generator Operator for generation Facilities at two or more locations." Therefore in this requirement, control center is intended to mean the Distribution Provider facilities hosting operating personnel performing the operational functions of the Distribution Provider that are necessary for the Reliable Operation of the BES, often referred to as a distribution control center, or distribution center. Examples of Distribution Providers exchanging information necessary for the Reliable Operation of the BES include Distribution Providers included in restoration plans, load shed plans, load reconfiguration, and voltage control plans. The Distribution Provider must have the capability to exchange information *whenever* the internal Interpersonal Communications may directly impact operations of the BES. Therefore, the Distribution

Provider must have the capability to exchange information between control centers as necessary. For example, a Distribution Provider with multiple control centers that are geographical separated, where face-to-face communications are not available, must have the capability to communicate internally between or among those control centers.

Appendix QC-COM-001-3
Provisions specific to the standard COM-001-3 applicable in Québec

This appendix establishes specific provisions for the application of the standard in Québec. Provisions of the standard and of its appendix must be read together for the purposes of understanding and interpretation. Where the standard and appendix differ, the appendix shall prevail.

A. Introduction

1. Title: **Communications**

2. Number: COM-001-3

3. Purpose: No specific provision

4. Applicability: No specific provision

5. Effective Date:

5.1. Adoption of the standard by the Régie de l'énergie: June 8, 2020

5.2. Adoption of the appendix by the Régie de l'énergie: June 8, 2020

5.3. Effective date of the standard and its appendix in Québec: April 1, 2021

B. Requirements and Measures

No specific provision

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

The Régie de l'énergie is responsible, in Québec, for compliance enforcement with respect to the reliability standard and its appendix that it adopts.

1.2. Evidence Retention

No specific provision

1.3. Compliance Monitoring and Enforcement Program

The Québec Reliability Standards Compliance Monitoring and Enforcement Program (QCMEP) of the Régie de l'énergie identifies the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Appendix QC-COM-001-3
Provisions specific to the standard COM-001-3 applicable in Québec

Violation Severity Levels

No specific provision

The following provide corrections of the table in the standard:

Appendix QC-COM-001-3
Provisions specific to the standard COM-001-3 applicable in Québec

R9	The Reliability Coordinator, Transmission Operator, or Balancing Authority tested the Alternative Interpersonal Communication capability but initiated action to repair or designated a replacement Alternative Interpersonal Communication in more than 2 hours and less than or equal to 4 hours upon an unsuccessful test.	The Reliability Coordinator, Transmission Operator, or Balancing Authority tested the Alternative Interpersonal Communication capability but initiated action to repair or designated a replacement Alternative Interpersonal Communication in more than 4 hours and less than or equal to 6 hours upon an unsuccessful test.	The Reliability Coordinator, Transmission Operator, or Balancing Authority tested the Alternative Interpersonal Communication capability but initiated action to repair or designated a replacement Alternative Interpersonal Communication in more than 6 hours and less than or equal to 8 hours upon an unsuccessful test.	The Reliability Coordinator, Transmission Operator, or Balancing Authority failed to test the Alternative Interpersonal Communication capability once each calendar month. OR The Reliability Coordinator, Transmission Operator, or Balancing Authority tested the Alternative Interpersonal Communication capability but failed to initiate action to repair or designate a replacement Alternative Interpersonal Communication in more than 8 hours upon an unsuccessful test.
R10	The Reliability Coordinator, Transmission Operator, or Balancing Authority notified the entities identified in Requirements R1, R3, and R5, respectively upon the detection of a failure of its Interpersonal Communication capability in more than 60 minutes but less than or equal to 70 minutes.	The Reliability Coordinator, Transmission Operator, or Balancing Authority notified the entities identified in Requirements R1, R3, and R5, respectively upon the detection of a failure of its Interpersonal Communication capability in more than 70 minutes but less than or equal to 80 minutes.	The Reliability Coordinator, Transmission Operator, or Balancing Authority notified the entities identified in Requirements R1, R3, and R5, respectively upon the detection of a failure of its Interpersonal Communication capability in more than 80 minutes but less than or equal to 90 minutes.	The Reliability Coordinator, Transmission Operator, or Balancing Authority failed to notify the entities identified in Requirements R1, R3, and R5, respectively upon the detection of a failure of its Interpersonal Communication capability in more than 90 minutes.

Appendix QC-COM-001-3
Provisions specific to the standard COM-001-3 applicable in Québec

Regional Differences

No specific provision

Associated Documents

No specific provision

Version History

The following provide corrections of the table in the standard:

2.1	August 25, 2015	Changed numbered parts under Requirement R6 to line up with the appropriate requirement.	2.1

Revision History

Revision	Date	Action	Change Tracking
0	June 8, 2020	New appendix	New

A. Introduction

1. **Title:** Operating Personnel Communications Protocols
2. **Number:** COM-002-4
3. **Purpose:** To improve communications for the issuance of Operating Instructions with predefined communications protocols to reduce the possibility of miscommunication that could lead to action or inaction harmful to the reliability of the Bulk Electric System (BES).
4. **Applicability:**
   - **4.1. Functional Entities**
     - **4.1.1** Balancing Authority
     - **4.1.2** Distribution Provider
     - **4.1.3** Reliability Coordinator
     - **4.1.4** Transmission Operator
     - **4.1.5** Generator Operator
5. **Effective Date:** The standard shall become effective on the first day of the first calendar quarter that is twelve (12) months after the date that the standard is approved by an applicable governmental authority or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective on the first day of the first calendar quarter that is twelve (12) months after the date the standard is adopted by the NERC Board of Trustees or as otherwise provided for in that jurisdiction.

B. Requirements

R1. Each Balancing Authority, Reliability Coordinator, and Transmission Operator shall develop documented communications protocols for its operating personnel that issue and receive Operating Instructions. The protocols shall, at a minimum: *[Violation Risk Factor: Low][Time Horizon: Long-term Planning]*

1.1. Require its operating personnel that issue and receive an oral or written Operating Instruction to use the English language, unless agreed to otherwise. An alternate language may be used for internal operations.

1.2. Require its operating personnel that issue an oral two-party, person-to-person Operating Instruction to take one of the following actions:

- Confirm the receiver's response if the repeated information is correct.
- Reissue the Operating Instruction if the repeated information is incorrect or if requested by the receiver.

- Take an alternative action if a response is not received or if the Operating Instruction was not understood by the receiver.

1.3. Require its operating personnel that receive an oral two-party, person-to-person Operating Instruction to take one of the following actions:

- Repeat, not necessarily verbatim, the Operating Instruction and receive confirmation from the issuer that the response was correct.
- Request that the issuer reissue the Operating Instruction.

1.4. Require its operating personnel that issue a written or oral single-party to multiple-party burst Operating Instruction to confirm or verify that the Operating Instruction was received by at least one receiver of the Operating Instruction.

1.5. Specify the instances that require time identification when issuing an oral or written Operating Instruction and the format for that time identification.

1.6. Specify the nomenclature for Transmission interface Elements and Transmission interface Facilities when issuing an oral or written Operating Instruction.

R2. Each Balancing Authority, Reliability Coordinator, and Transmission Operator shall conduct initial training for each of its operating personnel responsible for the Real-time operation of the interconnected Bulk Electric System on the documented communications protocols developed in Requirement R1 prior to that individual operator issuing an Operating Instruction. *[Violation Risk Factor: Low][Time Horizon: Long-term Planning]*

R3. Each Distribution Provider and Generator Operator shall conduct initial training for each of its operating personnel who can receive an oral two-party, person-to-person Operating Instruction prior to that individual operator receiving an oral two-party, person-to-person Operating Instruction to either: *[Violation Risk Factor: Low][Time Horizon: Long-term Planning]*

- Repeat, not necessarily verbatim, the Operating Instruction and receive confirmation from the issuer that the response was correct, or
- Request that the issuer reissue the Operating Instruction.

R4. Each Balancing Authority, Reliability Coordinator, and Transmission Operator shall at least once every twelve (12) calendar months: *[Violation Risk Factor: Medium][Time Horizon: Operations Planning]*

4.1. Assess adherence to the documented communications protocols in Requirement R1 by its operating personnel that issue and receive Operating Instructions, provide feedback to those operating personnel and take corrective action, as deemed appropriate by the entity, to address deviations from the documented protocols.

4.2. Assess the effectiveness of its documented communications protocols in Requirement R1 for its operating personnel that issue and receive Operating Instructions and modify its documented communication protocols, as necessary.

R5. Each Balancing Authority, Reliability Coordinator, and Transmission Operator that issues an oral two-party, person-to-person Operating Instruction during an Emergency, excluding written or oral single-party to multiple-party burst Operating Instructions, shall either: *[Violation Risk Factor: High][Time Horizon: Real-time Operations]*

- Confirm the receiver's response if the repeated information is correct (in accordance with Requirement R6).
- Reissue the Operating Instruction if the repeated information is incorrect or if requested by the receiver, or
- Take an alternative action if a response is not received or if the Operating Instruction was not understood by the receiver.

R6. Each Balancing Authority, Distribution Provider, Generator Operator, and Transmission Operator that receives an oral two-party, person-to-person Operating Instruction during an Emergency, excluding written or oral single-party to multiple-party burst Operating Instructions, shall either: *[Violation Risk Factor: High][Time Horizon: Real-time Operations]*

- Repeat, not necessarily verbatim, the Operating Instruction and receive confirmation from the issuer that the response was correct, or
- Request that the issuer reissue the Operating Instruction.

R7. Each Balancing Authority, Reliability Coordinator, and Transmission Operator that issues a written or oral single-party to multiple-party burst Operating Instruction during an Emergency shall confirm or verify that the Operating Instruction was received by at least one receiver of the Operating Instruction. *[Violation Risk Factor: High][Time Horizon: Real-time Operations]*

C. Measures

M1. Each Balancing Authority, Reliability Coordinator, and Transmission Operator shall provide its documented communications protocols developed for Requirement R1.

M2. Each Balancing Authority, Reliability Coordinator, and Transmission Operator shall provide its initial training records related to its documented communications protocols developed for Requirement R1 such as attendance logs, agendas, learning objectives, or course materials in fulfillment of Requirement R2.

M3. Each Distribution Provider and Generator Operator shall provide its initial training records for its operating personnel such as attendance logs, agendas, learning objectives, or course materials in fulfillment of Requirement R3.

M4. Each Balancing Authority, Reliability Coordinator, and Transmission Operator shall provide evidence of its assessments, including spreadsheets, logs or other evidence of feedback, findings of effectiveness and any changes made to its documented communications protocols developed for Requirement R1 in fulfillment of

Requirement R4. The entity shall provide, as part of its assessment, evidence of any corrective actions taken where an operating personnel's non-adherence to the protocols developed in Requirement R1 is the sole or partial cause of an Emergency and for all other instances where the entity determined that it was appropriate to take a corrective action to address deviations from the documented protocols developed in Requirement R1.

M5. Each Reliability Coordinator, Transmission Operator, and Balancing Authority that issued an oral two-party, person-to-person Operating Instruction during an Emergency, excluding oral single-party to multiple-party burst Operating Instructions, shall have evidence that the issuer either: 1) confirmed that the response from the recipient of the Operating Instruction was correct; 2) reissued the Operating Instruction if the repeated information was incorrect or if requested by the receiver; or 3) took an alternative action if a response was not received or if the Operating Instruction was not understood by the receiver. Such evidence could include, but is not limited to, dated and time-stamped voice recordings, or dated and time-stamped transcripts of voice recordings, or dated operator logs in fulfillment of Requirement R5.

M6. Each Balancing Authority, Distribution Provider, Generator Operator, and Transmission Operator that was the recipient of an oral two-party, person-to-person Operating Instruction during an Emergency, excluding oral single-party to multiple-party burst Operating Instructions, shall have evidence to show that the recipient either repeated, not necessarily verbatim, the Operating Instruction and received confirmation from the issuer that the response was correct, or requested that the issuer reissue the Operating Instruction in fulfillment of Requirement R6. Such evidence may include, but is not limited to, dated and time-stamped voice recordings (if the entity has such recordings), dated operator logs, an attestation from the issuer of the Operating Instruction, memos or transcripts.

M7. Each Balancing Authority, Reliability Coordinator and Transmission Operator that issued a written or oral single or multiple-party burst Operating Instruction during an Emergency shall provide evidence that the Operating Instruction was received by at least one receiver. Such evidence may include, but is not limited to, dated and time-stamped voice recordings (if the entity has such recordings), dated operator logs, electronic records, memos or transcripts.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Data Retention

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to

provide other evidence to show that it was compliant for the full time period since the last audit.

Each Balancing Authority, Distribution Provider, Generator Operator, Reliability Coordinator, and Transmission Operator shall each keep data or evidence for each applicable Requirement for the current calendar year and one previous calendar year, with the exception of voice recordings which shall be retained for a minimum of 90 calendar days, unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

If a Balancing Authority, Distribution Provider, Generator Operator, Reliability Coordinator, or Transmission Operator is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time period specified above, whichever is longer.

The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

Compliance Monitoring and Assessment Processes

Compliance Audit

Self-Certification

Spot Checking

Compliance Investigation

Self-Reporting

Complaint

1.3. Additional Compliance Information

None

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	Long-term Planning	Low	The responsible entity did not specify the instances that require time identification when issuing an oral or written Operating Instruction and the format for that time identification, as required in Requirement R1, Part 1.5 OR The responsible entity did not specify the nomenclature for Transmission interface Elements and Transmission interface Facilities when issuing an oral or written Operating Instruction, as required in Requirement R1, Part 1.6.	The responsible entity did not require the issuer and receiver of an oral or written Operating Instruction to use the English language, unless agreed to otherwise, as required in Requirement R1, Part 1.1. An alternate language may be used for internal operations.	The responsible entity did not include Requirement R1, Part 1.4 in its documented communication protocols.	The responsible entity did not include Requirement R1, Part 1.2 in its documented communications protocols OR The responsible entity did not include Requirement R1, Part 1.3 in its documented communications protocols OR The responsible entity did not develop any documented communications protocols as required in Requirement R1.

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R2	Long-term Planning	Low	N/A	N/A	An individual operator responsible for the Real-time operation of the interconnected Bulk Electric System at the responsible entity issued an Operating Instruction, prior to being trained on the documented communications protocols developed in Requirement R1.	An individual operator responsible for the Real-time operation of the interconnected Bulk Electric System at the responsible entity issued an Operating Instruction during an Emergency prior to being trained on the documented communications protocols developed in Requirement R1.
R3	Long-term Planning	Low	N/A	N/A	An individual operator at the responsible entity received an Operating Instruction prior to being trained.	An individual operator at the responsible entity received an Operating Instruction during an Emergency prior to being trained.

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R4	Operations Planning	Medium	The responsible entity assessed adherence to the documented communications protocols in Requirements R1 by its operating personnel that issue and receive Operating Instructions and provided feedback to those operating personnel and took corrective action, as appropriate AND The responsible entity assessed the effectiveness of its documented communications protocols in Requirement R1 for its operating personnel that issue and receive Operating Instructions and modified its documented communication	The responsible entity assessed adherence to the documented communications protocols in Requirement R1 by its operating personnel that issue and receive Operating Instructions, but did not provide feedback to those operating personnel OR The responsible entity assessed adherence to the documented communications protocols in Requirements R1 by its operating personnel that issue and receive Operating Instructions and provided feedback to those operating personnel but did not take corrective action, as appropriate OR The responsible entity assessed the effectiveness of its documented communications protocols	The responsible entity did not assess adherence to the documented communications protocols in Requirements R1 by its operating personnel that issue and receive Operating Instructions OR The responsible entity did not assess the effectiveness of its documented communications protocols in Requirement R1 for its operating personnel that issue and receive Operating Instructions.	The responsible entity did not assess adherence to the documented communications protocols in Requirements R1 by its operating personnel that issue and receive Operating Instructions AND The responsible entity did not assess the effectiveness of its documented communications protocols in Requirement R1 for its operating personnel that issue and receive Operating Instructions.

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			protocols, as necessary AND The responsible entity exceeded twelve (12) calendar months between assessments.	in Requirement R1 for its operating personnel that issue and receive Operating Instructions, but did not modify its documented communication protocols, as necessary.		

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R5	Real-time Operations	High	N/A	The responsible entity that issued an Operating Instruction during an Emergency did not take one of the following actions: • Confirmed the receiver's response if the repeated information was correct (in accordance with Requirement R6). • Reissued the Operating Instruction if the repeated information was incorrect or if requested by the receiver. • Took an alternative action if a response was not received or if the Operating Instruction was not understood by the receiver.	N/A	The responsible entity that issued an Operating Instruction during an Emergency did not take one of the following actions: • Confirmed the receiver's response if the repeated information was correct (in accordance with Requirement R6). • Reissued the Operating Instruction if the repeated information was incorrect or if requested by the receiver. • Took an alternative action if a response was not received or if the Operating Instruction was not understood by the receiver. AND Instability, uncontrolled separation, or cascading failures occurred as a result.

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R6	Real-time Operations	High	N/A	The responsible entity did not repeat, not necessarily verbatim, the Operating Instruction during an Emergency and receive confirmation from the issuer that the response was correct, or request that the issuer reissue the Operating Instruction when receiving an Operating Instruction.	N/A	The responsible entity did not repeat, not necessarily verbatim, the Operating Instruction during an Emergency and receive confirmation from the issuer that the response was correct, or request that the issuer reissue the Operating Instruction when receiving an Operating Instruction AND Instability, uncontrolled separation, or cascading failures occurred as a result.
R7	Real-time Operations	High	N/A	The responsible entity that that issued a written or oral single-party to multiple-party burst Operating Instruction during an Emergency did not confirm or verify that the Operating Instruction was received by at least one receiver of the Operating Instruction.	N/A	The responsible entity that that issued a written or oral single-party to multiple-party burst Operating Instruction during an Emergency did not confirm or verify that the Operating Instruction was received by at least one receiver of the Operating Instruction AND Instability, uncontrolled separation, or cascading failures occurred as a result.

E. Regional Variances

None

Version History

Version	Date	Action	Change Tracking
0	April 1, 2005	Effective Date	New
0	August 8, 2005	Removed "Proposed" from Effective Date	Errata
1	February 7, 2006	Adopted by Board of Trustees	Added measures and compliance elements
2	November 1, 2006	Adopted by Board of Trustees	Revised in accordance with SAR for Project 2006-06, Reliability Coordination (RC SDT). Retired R1, R1.1, M1, M2 and updated the compliance monitoring information. Replaced R2 with new R1, R2 and R3.
2a	February 9, 2012	Interpretation of R2 adopted by Board of Trustees	Project 2009-22
3	November 7, 2012	Adopted by Board of Trustees	
4	May 6, 2014	Adopted by Board of Trustees	
4	April 16, 2015	FERC Order issued approving COM-002-4	

Appendix QC-COM-002-4
Provisions specific to the standard COM-002-4 applicable in Québec

This appendix establishes specific provisions for the application of the standard in Québec. Provisions of the standard and of its appendix must be read together for the purposes of understanding and interpretation. Where the standard and appendix differ, the appendix shall prevail.

A. Introduction

1. Title: **Operating Personnel Communications Protocols**

2. Number: COM-002-4

3. Purpose: No specific provision

4. Applicability: No specific provision

Functional entities

No specific provision

Facilities

Any reference to the term "BES" shall be replaced by the term "RTP".

5. Effective Date:

5.1. Adoption of the standard by the Régie de l'énergie: December 22, 2016

5.2. Adoption of the appendix by the Régie de l'énergie: December 22, 2016

5.3. Effective date of the standard and its appendix in Québec: January 1, 2018

B. Requirements

No specific provision

C. Requirements

No specific provision

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

The Régie de l'énergie is responsible, in Québec, for compliance enforcement with respect to the reliability standard and its appendix that it adopts.

1.2. Data Retention

No specific provision

Compliance Monitoring and Assessment Processes

No specific provision

1.3. Additional Compliance Information

No specific provision

E. Regional Variances

No specific provision

Appendix QC-COM-002-4
Provisions specific to the standard COM-002-4 applicable in Québec

Revision History

Revision	Adoption Date	Action	Change Tracking
0	December 22, 2016	New appendix	New

A. Introduction

1. **Title:** Event Reporting

2. **Number:** EOP-004-4

3. **Purpose:** To improve the reliability of the Bulk Electric System by requiring the reporting of events by Responsible Entities.

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the Requirements and the EOP-004 Attachment 1 contained herein, the following Functional Entities will be collectively referred to as "Responsible Entity."

   4.1.1. Reliability Coordinator

   4.1.2. Balancing Authority

   4.1.3. Transmission Owner

   4.1.4. Transmission Operator

   4.1.5. Generator Owner

   4.1.6. Generator Operator

   4.1.7. Distribution Provider

5. **Effective Date:** See the Implementation Plan for EOP-004-4.

B. Requirements and Measures

R1. Each Responsible Entity shall have an event reporting Operating Plan in accordance with EOP-004-4 Attachment 1 that includes the protocol(s) for reporting to the Electric Reliability Organization and other organizations (e.g., the Regional Entity, company personnel, the Responsible Entity's Reliability Coordinator, law enforcement, or governmental authority). *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M1. Each Responsible Entity will have a dated event reporting Operating Plan that includes protocol(s) and each organization identified to receive an event report for event types specified in EOP-004-4 Attachment 1 and in accordance with the entity responsible for reporting.

R2. Each Responsible Entity shall report events specified in EOP-004-4 Attachment 1 to the entities specified per their event reporting Operating Plan by the later of 24 hours of recognition of meeting an event type threshold for reporting or by the end of the Responsible Entity's next business day (4 p.m. local time will be considered the end of the business day). *[Violation Risk Factor: Medium] [Time Horizon: Operations Assessment]*

M2. Each Responsible Entity will have as evidence of reporting an event to the entities specified per their event reporting Operating Plan either a copy of the completed EOP-004-4 Attachment 2 form or a DOE-OE-417 form; and some evidence of submittal (e.g., operator log or other operating documentation, voice recording, electronic mail message, or confirmation of facsimile) demonstrating that the event report was submitted by the later of 24 hours of recognition of meeting an event type threshold for reporting or by the end of the Responsible Entity's next business day (4 p.m. local time will be considered the end of the business day).

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority:

"Compliance Enforcement Authority" means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention:

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

- Each Responsible Entity shall retain the current Operating Plan plus each version issued since the last audit for Requirement R1, and Measure M1.
- Each Responsible Entity shall retain evidence of compliance since the last audit for Requirement R2 and Measure M2.

If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the duration specified above, whichever is longer.

The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program

As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	The Responsible Entity had an event reporting Operating Plan, but failed to include one applicable event type.	The Responsible Entity had an event reporting Operating Plan, but failed to include two applicable event types.	The Responsible Entity had an event reporting Operating Plan, but failed to include three applicable event types.	The Responsible Entity had an event reporting Operating Plan, but failed to include four or more applicable event types. OR The Responsible Entity failed to have an event reporting Operating Plan.
R2.	The Responsible Entity submitted an event report (e.g., written or verbal) to all required recipients up to 24 hours after the timing requirement for submittal. OR The Responsible Entity failed to submit an event report (e.g., written or verbal) to one entity identified in its event reporting Operating Plan within 24 hours or by the end of the next business day, as applicable.	The Responsible Entity submitted an event report (e.g., written or verbal) to all required recipients more than 24 hours but less than or equal to 48 hours after the timing requirement for submittal. OR The Responsible Entity failed to submit an event report (e.g., written or verbal) to two entities identified in its event reporting Operating Plan within 24 hours or by	The Responsible Entity submitted an event report (e.g., written or verbal) to all required recipients more than 48 hours but less than or equal to 72 hours after the timing requirement for submittal. OR The Responsible Entity failed to submit an event report (e.g., written or verbal) to three entities identified in its event reporting Operating Plan within 24 hours or by	The Responsible Entity submitted an event report (e.g., written or verbal) to all required recipients more than 72 hours after the timing requirement for submittal. OR The Responsible Entity failed to submit an event report (e.g., written or verbal) to four or more entities identified in its event reporting Operating Plan within 24 hours or by the

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		the end of the next business day, as applicable.	the end of the next business day, as applicable.	end of the next business day, as applicable. OR The Responsible Entity failed to submit a report for an event in EOP-004-4 Attachment 1.

D. Regional Variances

None.

E. Associated Documents

Link to the Implementation Plan and other important associated documents.

EOP-004 - Attachment 1: Reportable Events

NOTE: Under certain adverse conditions (e.g. severe weather, multiple events) it may not be possible to report the damage caused by an event and issue a written event report within the timing in the standard. In such cases, the affected Responsible Entity shall notify parties per Requirement R2 and provide as much information as is available at the time of the notification. Submit reports to the ERO via one of the following: e-mail: systemawareness@nerc.net, Facsimile 404-446-9770 or Voice: 404-446-9780, select Option 1.

Submit EOP-004 Attachment 2 (or DOE-OE-417) pursuant to Requirements R1 and R2.

Rationale for Attachment 1:

System-wide voltage reduction to maintain the continuity of the BES: The TOP is operating the system and is the only entity that would implement system-wide voltage reduction.

Complete loss of Interpersonal Communication and Alternative Interpersonal Communication capability at a BES control center: To align EOP-004-4 with COM-001-2.1. COM-001-2.1 defined Interpersonal Communication for the NERC Glossary of Terms as: "Any medium that allows two or more individuals to interact, consult, or exchange information." The NERC Glossary of Terms defines Alternative Interpersonal Communication as: "Any Interpersonal Communication that is able to serve as a substitute for, and does not utilize the same infrastructure (medium) as, Interpersonal Communication used for day-to-day operation."

Complete loss of monitoring or control capability at a BES control center: Language revisions to: "Complete loss of monitoring or control capability at a BES control center for 30 continuous minutes or more" provides clarity to the "Threshold for Reporting" and better aligns with the ERO Event Analysis Process.

Event Type	Entity with Reporting Responsibility	Threshold for Reporting
Damage or destruction of a Facility	RC, BA, TOP	Damage or destruction of a Facility within its Reliability Coordinator Area, Balancing Authority Area or Transmission Operator Area that results in action(s) to avoid a BES Emergency.

Event Type	Entity with Reporting Responsibility	Threshold for Reporting
Damage or destruction of its Facility	TO, TOP, GO, GOP, DP	Damage or destruction of its Facility that results from actual or suspected intentional human action. It is not necessary to report theft unless it degrades normal operation of its Facility.
Physical threats to its Facility	TO, TOP, GO, GOP, DP	Physical threat to its Facility excluding weather or natural disaster related threats, which has the potential to degrade the normal operation of the Facility. OR Suspicious device or activity at its Facility.
Physical threats to its BES control center	RC, BA, TOP	Physical threat to its BES control center, excluding weather or natural disaster related threats, which has the potential to degrade the normal operation of the control center. OR Suspicious device or activity at its BES control center.
Public appeal for load reduction resulting from a BES Emergency	BA	Public appeal for load reduction to maintain continuity of the BES.
System-wide voltage reduction resulting from a BES Emergency	TOP	System-wide voltage reduction of 3% or more.
Firm load sheddingresulting from a BES Emergency	Initiating RC, BA, or TOP	Firm load shedding ≥ 100 MW (manual or automatic).

Event Type	Entity with Reporting Responsibility	Threshold for Reporting
BES Emergency resulting in voltage deviation on a Facility	TOP	A voltage deviation of =/> 10% of nominal voltage sustained for ≥ 15 continuous minutes.
Uncontrolled loss of firm load resulting from a BES Emergency	BA, TOP, DP	Uncontrolled loss of firm load for ≥ 15 minutes from a single incident: ≥ 300 MW for entities with previous year's peak demand ≥ 3,000 MW OR ≥ 200 MW for all other entities
System separation (islanding)	RC, BA, TOP	Each separation resulting in an island ≥ 100 MW
Generation loss	BA	Total generation loss, within one minute, of: ≥ 2,000 MW in the Eastern, Western, or Quebec Interconnection OR ≥ 1,400 MW in the ERCOT Interconnection Generation loss will be used to report Forced Outages not weather patterns or fuel supply unavailability for dispersed power producing resources.

Event Type	Entity with Reporting Responsibility	Threshold for Reporting
Complete loss of off-site power to a nuclear generating plant (grid supply)	TO, TOP	Complete loss of off-site power (LOOP) affecting a nuclear generating station per the Nuclear Plant Interface Requirements
Transmission loss	TOP	Unexpected loss within its area, contrary to design, of three or more BES Facilities caused by a common disturbance (excluding successful automatic reclosing).
Unplanned evacuation of its BES control center	RC, BA, TOP	Unplanned evacuation from its BES control center facility for 30 continuous minutes or more.
Complete loss of Interpersonal Communication and Alternative Interpersonal Communication capability at its staffed BES control center	RC, BA, TOP	Complete loss of Interpersonal Communication and Alternative Interpersonal Communication capability affecting its staffed BES control center for 30 continuous minutes or more.
Complete loss of monitoring or control capability at its staffed BES control center	RC, BA, TOP	Complete loss of monitoring or control capability at its staffed BES control center for 30 continuous minutes or more.

EOP-004 - Attachment 2: Event Reporting Form

EOP-004 Attachment 2: Event Reporting Form

Use this form to report events. The Electric Reliability Organization will accept the DOE OE-417 form in lieu of this form if the entity is required to submit an OE-417 report. Submit reports to the ERO via one of the following: e-mail: systemawareness@nerc.net, Facsimile 404-446-9770 or voice: 404-446-9780, Option 1. Also submit to other applicable organizations per Requirement R1 "… (e.g., the Regional Entity, company personnel, the Responsible Entity's Reliability Coordinator, law enforcement, or Applicable Governmental Authority)."

	Task	Comments
1.	Entity filing the report include: Company name: Name of contact person: Email address of contact person: Telephone Number: Submitted by (name):	
2.	Date and Time of recognized event. Date: (mm/dd/yyyy) Time: (hh:mm) Time/Zone:	
3.	Did the event originate in your system?	Yes ☐ No☐ Unknown ☐
4.	**Event Identification and Description:**	
	(Check applicable box) ☐ Damage or destruction of a Facility ☐ Physical threat to its Facility ☐ Physical threat to its BES control center ☐ BES Emergency: ☐ firm load shedding ☐ public appeal for load reduction ☐ System-wide voltage reduction ☐ voltage deviation on a Facility ☐ uncontrolled loss of firm load ☐ System separation (islanding) ☐ Generation loss ☐ Complete loss of off-site power to a nuclear generating plant (grid supply) ☐ Transmission loss ☐ Unplanned evacuation of its BES control center ☐ Complete loss of Interpersonal Communication and Alternative Interpersonal Communication capability at its staffed BES control center ☐ Complete loss of monitoring or control capability at its staffed BES control center	Written description (optional):

Version History

Version	Date	Action	Change Tracking
2		Merged CIP-001-2a Sabotage Reporting and EOP-004-1 Disturbance Reporting into EOP-004-2 Event Reporting; Retire CIP-001-2a Sabotage Reporting and Retired EOP-004-1 Disturbance Reporting.	Revision to entire standard (Project 2009-01)
2	November 7, 2012	Adopted by the NERC Board of Trustees	
2	June 20, 2013	FERC approved	
3	November 13, 2014	Adopted by the NERC Board of Trustees	Replaced references to Special protection System and SPS with Remedial Action Scheme and RAS
3	November 19, 2015	FERC Order issued approving EOP-004-3. Docket No. RM15-13-000.	
4	February 9, 2017	Adopted by the NERC Board of Trustees	Revised
4	January 18, 2018	FERC order issued approving EOP-004-4. Docket No. RM17-12-000	

Guideline and Technical Basis

Multiple Reports for a Single Organization

For entities that have multiple registrations, the requirement is that these entities will only have to submit one report for any individual event. For example, if an entity is registered as a Reliability Coordinator, Balancing Authority and Transmission Operator, the entity would only submit one report for a particular event rather submitting three reports as each individual registered entity.

Law Enforcement Reporting

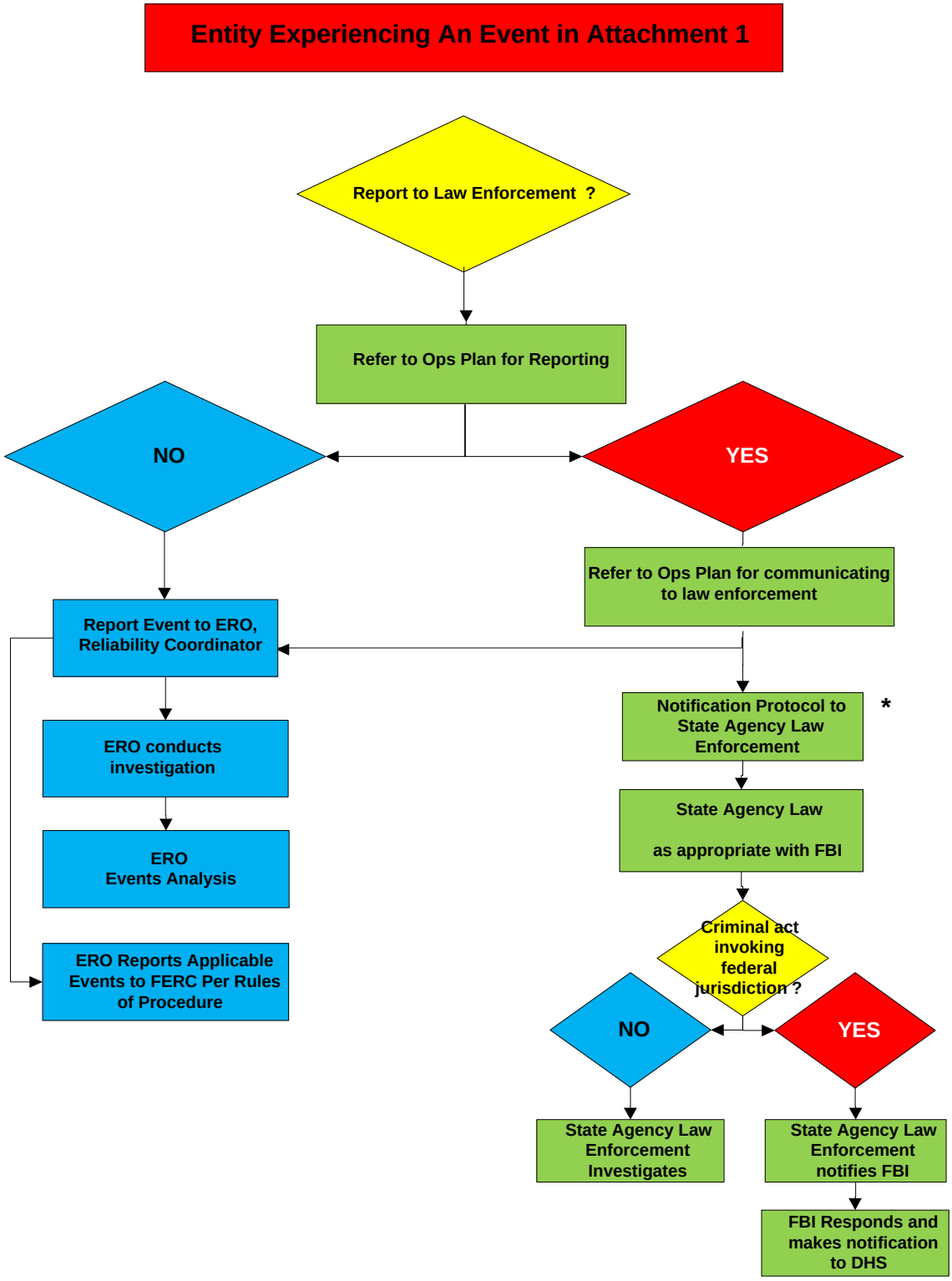
The reliability objective of EOP-004-4 is to improve the reliability of the Bulk Electric System by requiring the reporting of events by Responsible Entities. Certain outages, such as those due to vandalism and terrorism, may not be reasonably preventable. These are the types of events that should be reported to law enforcement. Entities rely upon law enforcement agencies to respond to and investigate those events which have the potential to impact a wider area of the BES. The inclusion of reporting to law enforcement enables and supports reliability principles such as protection of Bulk Electric System from malicious physical attack. The importance of BES awareness of the threat around them is essential to the effective operation and planning to mitigate the potential risk to the BES.

Stakeholders in the Reporting Process

- Industry
- NERC (ERO), Regional Entity
- FERC
- DOE
- NRC
- DHS – Federal
- Homeland Security- State
- State Regulators
- Local Law Enforcement
- State or Provincial Law Enforcement
- FBI
- Royal Canadian Mounted Police (RCMP)

The above stakeholders have an interest in the timely notification, communication and response to an incident at a Facility. The stakeholders have various levels of accountability and have a vested interest in the protection and response to ensure the reliability of the BES.

Example of Reporting Process including Law Enforcement



* Canadian entities will follow law enforcement protocols applicable in their jurisdictions

Potential Uses of Reportable Information

General situational awareness, correlation of data, trend identification, and identification of potential events of interest for further analysis in the ERO Event Analysis Process are a few potential uses for the information reported under this standard. The standard requires Functional Entities to report the incidents and provide information known at the time of the report. Further data gathering necessary for analysis is provided for under the ERO Event Analysis Program and the NERC Rules of Procedure. The NERC Rules of Procedure (section 800) provide an overview of the responsibilities of the ERO in regards to analysis and dissemination of information for reliability. Jurisdictional agencies (which may include DHS, FBI, NERC, RE, FERC, Provincial Regulators, and DOE) have other duties and responsibilities.

Appendix EOP-004-4-QC-1

Specific provisions applicable in Québec for standard EOP-004-4 – Event Reporting

This appendix establishes specific provisions for the application of the standard in Québec. Provisions of the standard and of this appendix must be read jointly for comprehension and interpretation purposes. Where the standard and appendix differ, the appendix shall prevail.

A. Introduction

1. Title: No specific provisions.

2. Number: No specific provisions.

3. Purpose: No specific provisions.

4. Applicability:

4.1. Functional Entities

No specific provisions.

The Facilities subject to this standard are the Facilities of the Main Transmission System (RTP).

5. Effective date:

5.1.	Adoption of the standard by the Régie de l'énergie:	October 8, 2020
5.2.	Adoption of this appendix by the Régie de l'énergie:	October 8, 2020
5.3.	Effective date of the standard and of this appendix in Québec:	January 1, 2021

B. Requirements and Measures

No specific provisions.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

In Québec, "Compliance Enforcement Authority" means the Régie de l'énergie in its roles of monitoring and enforcing compliance with respect to the Reliability Standard and to this appendix.

1.2. Evidence Retention

No specific provisions.

1.3. Compliance Monitoring and Enforcement Program

The Régie de l'énergie establishes the monitoring processes used to evaluate data or information for the purpose of determining compliance or non-compliance with the Reliability Standard and with this appendix.

Violation Severity Levels

No specific provisions.

D. Regional Variances

No specific provisions.

E. Associated Documents

No specific provisions.

EOP-004 – Attachment 1: Reportable Events

Replace “BES” with “RTP.”

EOP-004 – Attachment 2: Event Reporting Form

Replace “BES” with “RTP.”

Guidelines and Technical Basis

Replace “BES” with “RTP.”

Version history

Version	Date	Action	Change tracking
1	October 8, 2020	New appendix	New

A. Introduction

1. **Title:** System Restoration from Blackstart Resources

2. **Number:** EOP-005-3

3. **Purpose:** Ensure plans, Facilities, and personnel are prepared to enable System restoration from Blackstart Resources to ensure reliability is maintained during restoration and priority is placed on restoring the Interconnection.

4. **Applicability:**

   4.1. Functional Entities:

   4.1.1. Transmission Operators

   4.1.2. Generator Operators

   4.1.3. Transmission Owners identified in the Transmission Operators restoration plan

   4.1.4. Distribution Providers identified in the Transmission Operators restoration plan

5. **Effective Date:** See the Implementation Plan for EOP-005-3.

6. **Standard-Only Definition:** None

B. Requirements and Measures

R1. Each Transmission Operator shall develop and implement a restoration plan approved by its Reliability Coordinator. The restoration plan shall be implemented to restore the Transmission Operator's System following a Disturbance in which one or more areas of the Bulk Electric System (BES) shuts down and the use of Blackstart Resources is required to restore the shutdown area to a state whereby the choice of the next Load to be restored is not driven by the need to control frequency or voltage regardless of whether the Blackstart Resource is located within the Transmission Operator's System. The restoration plan shall include: *[Violation Risk Factor = High] [Time Horizon = Operations Planning, Real-time Operations]*

1.1. Strategies for System restoration that are coordinated with its Reliability Coordinator's high level strategy for restoring the Interconnection.

1.2. A description of how all Agreements or mutually-agreed upon procedures or protocols for off-site power requirements of nuclear power plants, including priority of restoration, will be fulfilled during System restoration.

1.3. Procedures for restoring interconnections with other Transmission Operators under the direction of its Reliability Coordinator.

1.4. Identification of each Blackstart Resource and its characteristics including but not limited to the following: the name of the Blackstart Resource, location, megawatt and megavar capacity, and type of unit.

1.5. Identification of Cranking Paths and initial switching requirements between each Blackstart Resource and the unit(s) to be started.

1.6. Identification of acceptable operating voltage and frequency limits during restoration.

1.7. Operating Processes to reestablish connections within the Transmission Operator's System for areas that have been restored and are prepared for reconnection.

1.8. Operating Processes to restore Loads required to restore the System, such as station service for substations, units to be restarted or stabilized, the Load needed to stabilize generation and frequency, and provide voltage control.

1.9. Operating Processes for transferring operations back to the Balancing Authority in accordance with its Reliability Coordinator's criteria.

M1. Each Transmission Operator shall have a dated, documented System restoration plan developed in accordance with Requirement R1 that has been approved by its Reliability Coordinator as shown with the documented approval from its Reliability Coordinator and will have evidence, such as operator logs, voice recordings or other operating documentation, voice recordings or other communication documentation to show that its restoration plan was implemented for times when a Disturbance has occurred, in accordance with Requirement R1.

R2. Each Transmission Operator shall provide the entities identified in its approved restoration plan with a description of any changes to their roles and specific tasks prior to the effective date of the plan. *[Violation Risk Factor = Medium] [Time Horizon = Operations Planning]*

M2. Each Transmission Operator shall have evidence such as dated electronic receipts or registered mail receipts that it provided the entities identified in its approved restoration plan with a description of any changes to their roles and specific tasks prior to the effective date of the plan in accordance with Requirement R2.

R3. Each Transmission Operator shall review its restoration plan and submit it to its Reliability Coordinator annually on a mutually-agreed, predetermined schedule. *[Violation Risk Factor = Medium] [Time Horizon = Operations Planning]*

M3. Each Transmission Operator shall have documentation such as a dated review signature sheet, revision histories, dated electronic receipts, or registered mail receipts, that it has annually reviewed and submitted the Transmission Operator's restoration plan to its Reliability Coordinator in accordance with Requirement R3.

R4. Each Transmission Operator shall submit its revised restoration plan to its Reliability Coordinator for approval, when the revision would change its ability to implement its restoration plan, as follows: *[Violation Risk Factor = Medium] [Time Horizon = Operations Planning]*

4.1. Within 90 calendar days after identifying any unplanned permanent BES modifications.

4.2. Prior to implementing a planned permanent BES modification subject to its Reliability Coordinator approval requirements per EOP-006.

M4. Each Transmission Operator shall have documentation such as dated review signature sheets, revision histories, dated electronic receipts, or registered mail receipts, that it has submitted the revised restoration plan to its Reliability Coordinator in accordance with Requirement R4.

R5. Each Transmission Operator shall have a copy of its latest Reliability Coordinator approved restoration plan within its primary and backup control rooms so that it is available to all of its System Operators prior to its effective date. *[Violation Risk Factor = Lower] [Time Horizon = Operations Planning]*

M5. Each Transmission Operator shall have documentation that it has made the latest Reliability Coordinator approved copy of its restoration plan, in electronic or hardcopy format, in its primary and backup control rooms and available to its System Operators prior to its effective date in accordance with Requirement R5.

R6. Each Transmission Operator shall verify through analysis of actual events, a combination of steady state and dynamic simulations, or testing that its restoration plan accomplishes its intended function. This shall be completed at least once every five years. Such analysis, simulations or testing shall verify: *[Violation Risk Factor = Medium] [Time Horizon = Long-term Planning]*

6.1. The capability of Blackstart Resources to meet the Real and Reactive Power requirements of the Cranking Paths and the dynamic capability to supply initial Loads.

6.2. The location and magnitude of Loads required to control voltages and frequency within acceptable operating limits.

6.3. The capability of generating resources required to control voltages and frequency within acceptable operating limits.

M6. Each Transmission Operator shall have documentation, such as power flow outputs, that it has verified that its latest restoration plan will accomplish its intended function in accordance with Requirement R6.

R7. Each Transmission Operator shall have Blackstart Resource testing requirements to verify that each Blackstart Resource is capable of meeting the requirements of its restoration plan. These Blackstart Resource testing requirements shall include: *[Violation Risk Factor = Medium] [Time Horizon = Operations Planning]*

7.1. The frequency of testing such that each Blackstart Resource is tested at least once every three calendar years.

7.2. A list of required tests including:

7.2.1. The ability to start the unit when isolated with no support from the BES or when designed to remain energized without connection to the remainder of the System.

7.2.2. The ability to energize a bus. If it is not possible to energize a bus during the test, the testing entity must affirm that the unit has the capability to energize a bus such as verifying that the breaker close coil relay can be energized with the voltage and frequency monitor controls disconnected from the synchronizing circuits.

7.3. The minimum duration of each of the required tests.

M7. Each Transmission Operator shall have documented Blackstart Resource testing requirements in accordance with Requirement R7.

R8. Each Transmission Operator shall include within its operations training program, annual System restoration training for its System Operators. This training program shall include training on the following: *[Violation Risk Factor = Medium] [Time Horizon = Operations Planning]*

8.1. System restoration plan including coordination with its Reliability Coordinator and Generator Operators included in the restoration plan.

8.2. Restoration priorities.

8.3. Building of cranking paths.

8.4. Synchronizing (re-energized sections of the System).

8.5. Transition of Demand and resource balance within its area to the Balancing Authority.

M8. Each Transmission Operator shall have an electronic or hard copy of the training program material provided for its System Operators for System restoration training in accordance with Requirement R8.

R9. Each Transmission Operator, each applicable Transmission Owner, and each applicable Distribution Provider shall provide a minimum of two hours of System restoration training every two calendar years to their field switching personnel identified as performing unique tasks associated with the Transmission Operator's restoration plan that are outside of their normal tasks. *[Violation Risk Factor = Medium] [Time Horizon = Operations Planning]*

M9. Each Transmission Operator, each applicable Transmission Owner, and each applicable Distribution Provider shall have an electronic or hard copy of the training program material provided to their field switching personnel for System restoration training and the corresponding training records including training dates and duration in accordance with Requirement R9.

R10. Each Transmission Operator shall participate in its Reliability Coordinator's restoration drills, exercises, or simulations as requested by its Reliability Coordinator. *[Violation Risk Factor = Medium] [Time Horizon = Operations Planning]*

M10. Each Transmission Operator shall have evidence that it participated in its Reliability Coordinator's restoration drills, exercises, or simulations as requested in accordance with Requirement R10.

R11. Each Transmission Operator and each Generator Operator with a Blackstart Resource shall have written Blackstart Resource Agreements or mutually agreed upon procedures or protocols, specifying the terms and conditions of their arrangement. Such Agreements shall include references to the Blackstart Resource testing requirements. *[Violation Risk Factor = Medium] [Time Horizon = Operations Planning]*

M11. Each Transmission Operator and Generator Operator with a Blackstart Resource shall have the dated Blackstart Resource Agreements or mutually agreed upon procedures or protocols in accordance with Requirement R11.

R12. Each Generator Operator with a Blackstart Resource shall have documented procedures for starting each Blackstart Resource and energizing a bus. *[Violation Risk Factor = Medium] [Time Horizon = Operations Planning]*

M12. Each Generator Operator with a Blackstart Resource shall have dated documented procedures on file for starting each unit and energizing a bus in accordance with Requirement R12.

R13. Each Generator Operator with a Blackstart Resource shall notify its Transmission Operator of any known changes to the capabilities of that Blackstart Resource affecting the ability to meet the Transmission Operator's restoration plan within 24 hours following such change. *[Violation Risk Factor = Medium] [Time Horizon = Operations Planning]*

M13. Each Generator Operator with a Blackstart Resource shall provide evidence, such as dated electronic receipts or registered mail receipts, showing that it notified its Transmission Operator of any known changes to its Blackstart Resource capabilities within 24 hours of such changes in accordance with Requirement R13.

R14. Each Generator Operator with a Blackstart Resource shall perform Blackstart Resource tests, and maintain records of such testing, in accordance with the testing requirements set by the Transmission Operator to verify that the Blackstart Resource can perform as specified in the restoration plan. *[Violation Risk Factor = Medium] [Time Horizon = Operations Planning]*

14.1. Testing records shall include at a minimum: name of the Blackstart Resource, unit tested, date of the test, duration of the test, time required to start the unit, an indication of any testing requirements not met under Requirement R7.

14.2. Each Generator Operator shall provide the blackstart test results within 30 calendar days following a request from its Reliability Coordinator or Transmission Operator.

M14. Each Generator Operator with a Blackstart Resource shall maintain dated documentation of its Blackstart Resource test results and shall have evidence such as e-mails with receipts or registered mail receipts, that it provided these records to its Reliability Coordinator and Transmission Operator when requested in accordance with Requirement R14.

R15. Each Generator Operator with a Blackstart Resource shall provide a minimum of two hours of training every two calendar years to each of its operating personnel responsible for the startup of its Blackstart Resource generation units and energizing a bus. The training program shall include training on the following: *[Violation Risk Factor = Medium] [Time Horizon = Operations Planning]*

15.1. System restoration plan including coordination with the Transmission Operator

15.2. The procedures documented in Requirement R12

M15. Each Generator Operator with a Blackstart Resource shall have an electronic or hard copy of the training program material provided to its operating personnel responsible for the startup, energizing a bus and synchronization of its Blackstart Resource generation units and a copy of its dated training records including training dates and durations showing that it has provided training in accordance with Requirement R15.

R16. Each Generator Operator shall participate in its Reliability Coordinator's restoration drills, exercises, or simulations as requested by its Reliability Coordinator. *[Violation Risk Factor = Medium] [Time Horizon = Operations Planning]*

M16. Each Generator Operator shall have evidence that it participated in its Reliability Coordinator's restoration drills, exercises, or simulations if requested to do so in accordance with Requirement R16.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: Regional Entity
"Compliance Enforcement Authority" means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention:
The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

The Transmission Operator shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation:

- Approved restoration plan and any restoration plans in effect since the last compliance audit for Requirement R1, Measure M1.
- Provided the entities identified in its approved restoration plan with a description of any changes to their roles and specific tasks prior to the effective date of the plan for the current calendar year and three prior calendar years for Requirement R2, Measure M2.
- Submission of the Transmission Operator's annually-reviewed restoration plan to its Reliability Coordinator for the current calendar year and three prior calendar years for Requirement R3, Measure M3.
- Submission of a revised restoration plan to its Reliability Coordinator for all versions for the current calendar year and the prior three calendar years for Requirement R4, Measure M4.
- The current restoration plan approved by its Reliability Coordinator and any restoration plans for the last three calendar years that was made available in its control rooms for Requirement R5, Measure M5.
- The verification results for the current, approved restoration plan and the previous approved restoration plan for Requirement R6, Measure M6.
- The verification process and results for the current Blackstart Resource testing requirements and the last previous Blackstart Resource testing requirements for Requirement R7, Measure M7.
- Training program materials or descriptions for three calendar years for Requirement R8, Measure M8.
- Records of participation in all requested Reliability Coordinator restoration drills, exercises, or simulations since its last compliance audit, as well as one previous compliance audit period for Requirement R10, Measure M10.

If a Transmission Operator is found non-compliant for any requirement, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time period specified above, whichever is longer. The Transmission Operator, applicable Transmission Owner, and applicable Distribution Provider shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation:

- Training program materials or descriptions and training records for three calendar years for Requirement R9, Measure M9.

If a Transmission Operator, applicable Transmission Owner, or applicable Distribution Provider is found non-compliant for any requirement, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time period specified above, whichever is longer. .

The Transmission Operator and Generator Operator with a Blackstart Resource shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation:

- Current Blackstart Resource Agreements and any Blackstart Resource Agreements or mutually agreed upon procedures or protocols in effect since its last compliance audit for Requirement R11, Measure M11.

The Generator Operator with a Blackstart Resource shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation:

- Current documentation and any documentation in effect since its last compliance audit on procedures to start each Blackstart Resource and for energizing a bus for Requirement R12, Measure M12.
- Notification to its Transmission Operator of any known changes to its Blackstart Resource capabilities over the last three calendar years for Requirement R13, Measure M13.
- The verification test results for the current set of requirements and one previous set for its Blackstart Resources for Requirement R14, Measure M14.
- Training program materials and training records for three calendar years for Requirement R15, Measure M15.

If a Generation Operator with a Blackstart Resource is found non-compliant for any requirement, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time period specified above, whichever is longer.

The Generator Operator shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation:

- Records of participation in all requested Reliability Coordinator restoration drills, exercises, or simulations since its last compliance audit for Requirement R16, Measure M16.

If a Generation Operator is found non-compliant for any requirement, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time period specified above, whichever is longer. The Compliance Enforcement Authority shall keep the last compliance audit records and all requested and submitted subsequent compliance audit records.

1.3. Compliance Monitoring and Enforcement Program

As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	The Transmission Operator has an approved plan but failed to comply with one of the requirement parts within Requirement R1.	The Transmission Operator has an approved plan but failed to comply with two of the requirement parts within Requirement R1.	The Transmission Operator has an approved plan but failed to comply with three or more of the requirement parts within Requirement R1.	The Transmission Operator does not have an approved restoration plan. OR The Transmission Operator has an approved restoration plan, but failed to implement the applicable requirement parts within Requirement R1.
R2.	The Transmission Operator failed to provide one of the entities identified in its approved restoration plan with a description of any changes to their roles and specific tasks prior to the effective date of the plan.	The Transmission Operator failed to provide two of the entities identified in its approved restoration plan with a description of any changes to their roles and specific tasks prior to the effective date of the plan.	The Transmission Operator failed to provide three of the entities identified in its approved restoration plan with a description of any changes to their roles and specific tasks prior to the effective date of the plan.	The Transmission Operator failed to provide four or more of the entities identified in its approved restoration plan with a description of any changes to their roles and specific tasks prior to the effective date of the plan. OR Transmission Operator failed to provide at least half of the entities identified in its

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				approved restoration plan with a description of any changes to their roles and specific tasks prior to the effective date.
R3.	The Transmission Operator submitted the reviewed restoration plan within 30 calendar days after the mutually-agreed, predetermined schedule.	The Transmission Operator submitted the reviewed restoration plan more than 30 and less than or equal to 60 calendar days after the mutually-agreed, predetermined schedule.	The Transmission Operator submitted the reviewed restoration plan more than 60 and less than or equal to 90 calendar days after the mutually-agreed, predetermined schedule.	The Transmission Operator submitted the reviewed restoration plan more than 90 calendar days after the mutually-agreed, predetermined schedule.
R4.	The Transmission Operator failed to submit its revised restoration plan to its Reliability Coordinator within 90 calendar days of an unplanned permanent System BES modification.	The Transmission Operator submitted its revised restoration plan to its Reliability Coordinator between 91 calendar days and 120 calendar days of an unplanned permanent System BES modification.	The Transmission Operator submitted its revised restoration plan to its Reliability Coordinator between 121 calendar days and 150 calendar days of an unplanned permanent System BES modification.	The Transmission Operator has failed to submit its revised restoration plan to its Reliability Coordinator within 150 calendar days of an unplanned permanent System BES modification. OR The Transmission Operator failed to submit its revised restoration plan to its Reliability Coordinator prior

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				to a planned permanent BES modification.
R5.	N/A	N/A	N/A	The Transmission Operator did not make the latest Reliability Coordinator approved restoration plan available in its primary and backup control rooms prior to its effective date.
R6.	The Transmission Operator performed the verification within the required timeframe but did not comply with one of the requirement parts.	The Transmission Operator performed the verification within the required timeframe but did not comply with two of the requirement parts.	The Transmission Operator performed the verification but did not complete it within the required time frame.	The Transmission Operator did not perform the verification or it took more than six calendar years to complete the verification. OR The Transmission Operator performed the verification within the required timeframe but did not comply with any of the requirement parts.
R7.	N/A	N/A	N/A	The Transmission Operator's Blackstart Resource testing requirements do not address

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				one or more of the requirement parts of Requirement R7.
R8.	The Transmission Operator's training does not address one of the requirement parts of Requirement R8.	The Transmission Operator's training does not address two of the requirement parts of Requirement R8.	The Transmission Operator's training does not address three or more of the requirement parts of Requirement R8.	The Transmission Operator has not included System restoration training in its operations training program.
R9.	The Transmission Operator, applicable Transmission Owner, or applicable Distribution Provider failed to train 5% or less of the personnel required by Requirement R9 within a two-calendar-year period.	The Transmission Operator, applicable Transmission Owner, or applicable Distribution Provider failed to train more than 5% and up to 10% of the personnel required by Requirement R9 within a two-calendar-year period.	The Transmission Operator, applicable Transmission Owner, or applicable Distribution Provider failed to train more than 10% and up to 15% of the personnel required by Requirement R9 two-calendar-year period.	The Transmission Operator, applicable Transmission Owner, or applicable Distribution Provider failed to train more than 15% of the personnel required by Requirement R9 within a two-calendar-year period.
R10.	N/A	N/A	N/A	The Transmission Operator has failed to comply with a request for its participation from its Reliability Coordinator.
R11.	N/A	The Transmission Operator and Generator Operator	N/A	The Transmission Operator and Generator Operator

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		with a Blackstart Resource do not reference Blackstart Resource Testing requirements in their written Blackstart Resource Agreements or mutually-agreed upon procedures or protocols.		with a Blackstart resource do not have a written Blackstart Resource Agreement or mutually-agreed upon procedure or protocol.
R12.	N/A	N/A	N/A	The Generator Operator does not have documented starting and bus energizing procedures for each Blackstart Resource.
R13.	The Generator Operator with a Blackstart Resource did not notify the Transmission Operator of a known change in Blackstart Resource capability affecting the ability to meet the Transmission Operator's restoration plan within 24 hours but did make the notification within 48 hours.	The Generator Operator with a Blackstart Resource did not notify the Transmission Operator of a known change in Blackstart Resource capability affecting the ability to meet the Transmission Operator's restoration plan within 48 hours but did make the notification within 72 hours.	The Generator Operator with a Blackstart Resource did not notify the Transmission Operator of a known change in Blackstart Resource capability affecting the ability to meet the Transmission Operator's restoration plan within 72 hours but did make the notification within 96 hours.	The Generator Operator with a Blackstart Resource did not notify the Transmission Operator of a known change in Blackstart Resource capability affecting the ability to meet the Transmission Operator's restoration plan for more than 96 hours.

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R14.	The Generator Operator with a Blackstart Resource performed tests and maintained records but the records did not include all of the items in Requirement R14, Part 14.1. OR The Generator Operator did not supply the Blackstart Resource testing records as requested for 31 to 60 calendar days after the request.	The Generator Operator with a Blackstart Resource performed tests and maintained records but did not supply the Blackstart Resource testing records as requested for 61 to 90 calendar days after the request.	The Generator Operator with a Blackstart Resource performed tests but either did not maintain records or did not supply the Blackstart Resource testing records as requested within 91 or more calendar days after the request.	The Generator Operator with a Blackstart Resource did not perform Blackstart Resource tests.
R15.	The Generator Operator with a Blackstart Resource did not train less than or equal to 10% of the personnel required by Requirement R15 within a two-calendar-year period.	The Generator Operator with a Blackstart Resource did not train more than 10% and less than or equal to 25% of the personnel required by Requirement R15 within a two-calendar-year period.	The Generator Operator with a Blackstart Resource did not train more than 25% and less than or equal to 50% of the personnel required by Requirement R15 within a two-calendar-year period.	The Generator Operator with a Blackstart Resource did not train more than 50% of the personnel required by Requirement R15 within a two-calendar-year period.
R16.	N/A	N/A	N/A	The Generator Operator failed to participate in its Reliability Coordinator's

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				restoration drills, exercises, or simulations as requested by its Reliability Coordinator.

D. Regional Variances

None.

E. Associated Documents

Link to the Implementation Plan and other important associated documents.

Version History

Version	Date	Action	Change Tracking
0	April 1, 2005	Effective Date	New
0	August 8, 2005	Removed “Proposed” from Effective Date	Errata
1	May 2, 2007	Approved by the Board of Trustees	Revised
2		Revisions pursuant to Project 2006-03	Updated testing requirements Incorporated Attachment 1 into the requirements. Updated Measures and Compliance to match new requirements
2	August 5, 2009	Adopted by Board of Trustees	Revised
2	March 17, 2011	Order issued by FERC approving EOP-005-2 (approval effective 5/23/11)	
2	February 7, 2013	R3.1 and associated elements approved by NERC Board of Trustees for retirement as part of the Paragraph 81 project (Project 2013-02) pending applicable regulatory approval	
2	July 1, 2013	Updated VRFs and VSLs based on June 24, 2013 approval	
2	November 21, 2013	R3.1 and associated elements approved by FERC for retirement as part of the Paragraph 81 project (Project 2013-02)	
3	February 9, 2017	Adopted by the NERC Board of Trustees	Revised

3	January 18, 2018	FERC order issued approving EOP-005-3. Docket No. RM17-12-000.	

Rationale

Rationale for Requirement R4: As previously written, Requirement R4 addressed (in one sentence) two restoration plan update items that a Transmission Operator must perform: (1) the restoration plan must be updated within 90 calendar days after identifying any unplanned permanent System modifications and (2) the restoration plan must be updated prior to implementing a planned BES modification. The phrase: "… that would change the implementation of its restoration plan" appeared to apply to both types of changes. There was no time frame specified for updating the restoration plan for a planned BES modification; although one could infer that "90 calendar days" is intended to be the same time frame for both unplanned and planned modifications. Furthermore, the distinction between "System modifications" for unplanned changes and "BES modifications" for planned changes has been seen as confusing to some Responsible Entities.

The references to permanent unplanned and planned BES modifications that will change the ability to implement the RC-approved restoration plan are intended to require a Responsible Entity to submit a revised restoration plan to the RC when the modification would substantively change the TOP's ability to implement the restoration plan or impact the RC's ability to monitor and direct restoration efforts. The intent is not to require a TOP to submit changes that do not substantively change the restoration plan or the RCs ability to monitor and direct the restoration efforts. Examples of instances that do not require update and submission of a restoration plan include element number changes, device changes, or administrative changes that have no significance to the implementation of the plan.

In addition, the timeframes referenced in Requirement R4, Part 4.2 for a permanent planned BES modification directs the Responsible Entity to EOP-006-2, Requirement R5.1 and EOP-006-3, Requirement R5, Part 5.1, which states that the RC shall approve or disapprove the TOPs submitted restoration plan within 30 days of receipt. This allows the Responsible Entity to coordinate submission with the RC based on the RCs specific requirements.

Rationale for Requirement R6: Dynamic simulations should simulate frequency and voltage response. It is the intent of the EOP SDT that the simulation provides for the feedback of the System performance as generation and Load are added.

Rationale for Requirement R8: The addition of Requirement 8, Part 8.5 allows operating personnel to gain experience on all stages of restoration, including coordination needed transferring Demand and resource balance operations, back to the Balancing Authority in accordance with Requirement R1, Part 1.9.

Rationale for Requirement R9: The intent of "unique tasks" are those tasks that are defined by the Transmission Operator, the Transmission Owner, and the Distribution Provider.

Appendix EOP-005-3-QC-1

Specific provisions applicable in Québec for standard EOP-005-3 – System Restoration from Blackstart Resources

This appendix establishes specific provisions for the application of the standard in Québec. Provisions of the standard and of this appendix must be read jointly for comprehension and interpretation purposes. Where the standard and appendix differ, the appendix shall prevail.

A. Introduction

1. Title: No specific provisions.

2. Number: No specific provisions.

3. Purpose: No specific provisions.

4. Applicability:

4.1. Functional Entities

No specific provisions.

5. Effective date:

5.1. Adoption of the standard by the Régie de l'énergie: November 22, 2019

5.2. Adoption of this appendix by the Régie de l'énergie: November 22, 2019

5.3. Effective date of the standard and of this appendix in Québec: January 1st, 2021

6. Standard-Only Definition:

No specific provisions.

B. Requirements and Measures

Specific provision applicable to Requirement R16:

Requirement R16 applies only to Generator Operators operating resources needed for system restoration and identified in the Transmission Operator's restoration plan.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

In Québec, "Compliance Enforcement Authority" means the Régie de l'énergie in its roles of monitoring and enforcing compliance with respect to the Reliability Standard and to this appendix.

1.2. Evidence Retention

No specific provisions.

1.3. Compliance Monitoring and Enforcement Program

The Régie de l'énergie establishes the monitoring processes used to evaluate data or information for the purpose of determining compliance or non-compliance with the Reliability Standard and with this appendix.

Violation Severity Levels

No specific provisions.

High VSL for Requirement 9, erratum correction: added "within a" in the following part of the sentence "the personnel required by Requirement R9 within a two-calendar-year period."

R9.	The Transmission Operator, applicable Transmission Owner, or applicable Distribution Provider failed to train 5% or less of the personnel required by Requirement R9 within a two-calendar-year period.	The Transmission Operator, applicable Transmission Owner, or applicable Distribution Provider failed to train more than 5% and up to 10% of the personnel required by Requirement R9 within a two-calendar-year period.	The Transmission Operator, applicable Transmission Owner, or applicable Distribution Provider failed to train more than 10% and up to 15% of the personnel required by Requirement R9 within a two-calendar-year period.	The Transmission Operator, applicable Transmission Owner, or applicable Distribution Provider failed to train more than 15% of the personnel required by Requirement R9 within a two-calendar-year period.

D. Regional Variances

No specific provisions.

E. Associated Documents

No specific provisions.

Version history

Version	Date	Action	Change tracking
1	November 22, 2019	New appendix	New

A. Introduction

1. **Title:** System Restoration Coordination

2. **Number:** EOP-006-3

3. **Purpose:** Ensure plans are established and personnel are prepared to enable effective coordination of the System restoration process to ensure reliability is maintained during restoration and priority is placed on restoring the Interconnection.

4. **Applicability:**

   4.1. Functional Entities:

   4.1.1. Reliability Coordinators

5. **Proposed Effective Date:** See the Implementation Plan for EOP-006-3.

6. **Standard-Only Definition:** None

B. Requirements and Measures

R1. Each Reliability Coordinator shall develop and implement a Reliability Coordinator Area restoration plan. The scope of the Reliability Coordinator's restoration plan starts when Blackstart Resources are utilized to re-energize a shutdown area of the Bulk Electric System (BES), or separation has occurred between neighboring Reliability Coordinators, or an energized island has been formed on the BES within the Reliability Coordinator Area. The scope of the Reliability Coordinator's restoration plan ends when all of its Transmission Operators are interconnected and its Reliability Coordinator Area is connected to all of its neighboring Reliability Coordinator Areas. The restoration plan shall include: *[Violation Risk Factor = High] [Time Horizon = Operations Planning, Real-time Operations]*

1.1. A description of the high-level strategy to be employed during restoration events for restoring the Interconnection, including minimum criteria for meeting the objectives of the Reliability Coordinator's restoration plan.

1.2. Criteria and conditions for re-establishing interconnections with other Transmission Operators within its Reliability Coordinator Area, with Transmission Operators in other Reliability Coordinator Areas, and with other Reliability Coordinators.

1.3. Reporting requirements for the entities within the Reliability Coordinator Area during a restoration event.

1.4. Criteria for sharing information regarding restoration with neighboring Reliability Coordinators and with Transmission Operators and Balancing Authorities within its Reliability Coordinator Area.

1.5. Identification of the Reliability Coordinator as the primary contact for disseminating information regarding restoration to neighboring Reliability

Coordinators, and to Transmission Operators, and Balancing Authorities within its Reliability Coordinator Area.

1.6. Criteria for transferring operations and authority back to the Balancing Authority.

M1. Each Reliability Coordinator shall have available a dated copy of its restoration plan and will have evidence, such as operator logs or other operating documentation, voice recordings, or other communication documentation to show that its restoration plan was implemented in accordance with Requirement R1.

R2. The Reliability Coordinator shall distribute its most recent Reliability Coordinator Area restoration plan to each of its Transmission Operators and neighboring Reliability Coordinators within 30 calendar days of creation or revision. *[Violation Risk Factor = Lower] [Time Horizon = Operations Planning]*

M2. Each Reliability Coordinator shall provide evidence such as electronic receipts, posting to a secure website with notification to affected entities, or registered mail receipts, that its most recent restoration plan has been distributed in accordance with Requirement R2.

R3. Each Reliability Coordinator shall review its restoration plan within 13 calendar months of the last review. *[Violation Risk Factor = Medium] [Time Horizon = Operations Planning]*

M3. Each Reliability Coordinator shall provide evidence such as a review signature sheet, or revision histories, that it has reviewed its restoration plan within 13 calendar months of the last review in accordance with Requirement R3.

R4. Each Reliability Coordinator shall review its neighboring Reliability Coordinator's restoration plans and provide written notification of any conflicts discovered during that review within 60 calendar days of receipt. *[Violation Risk Factor = Medium] [Time Horizon = Operations Planning]*

4.1. If a Reliability Coordinator finds conflicts between its restoration plans and any of its neighbors, the conflicts shall be resolved within 30 calendar days of receipt of written notification.

M4. Each Reliability Coordinator shall provide evidence such as dated review signature sheets or electronic receipt that it has reviewed its neighboring Reliability Coordinator's restoration plans and resolved any conflicts within the timing requirements of Requirement R4 and Requirement R4, Part 4.1.

R5. Each Reliability Coordinator shall review the restoration plans required by EOP-005 of the Transmission Operators within its Reliability Coordinator Area. *[Violation Risk Factor = Medium] [Time Horizon = Operations Planning]*

5.1. The Reliability Coordinator shall determine whether the Transmission Operator's restoration plan is coordinated and compatible with the Reliability Coordinator's restoration plan and other Transmission Operators' restoration plans within its

Reliability Coordinator Area. The Reliability Coordinator shall provide notification to the Transmission Operator of approval or disapproval, with stated reasons, of the Transmission Operator's submitted restoration plan within 30 calendar days following the receipt of the restoration plan from the Transmission Operator.

M5. Each Reliability Coordinator shall provide evidence such as a dated review signature sheet or electronic receipt that it has reviewed, approved or disapproved, and notified its Transmission Operators within 30 calendar days following the receipt of the restoration plan from the Transmission Operator in accordance with Requirement R5.

R6. Each Reliability Coordinator shall have a copy of its latest restoration plan and copies of the latest approved restoration plan of each Transmission Operator in its Reliability Coordinator Area within its primary and backup control rooms so that it is available to all of its System Operators prior to the effective date. *[Violation Risk Factor = Lower] [Time Horizon = Operations Planning]*

M6. Each Reliability Coordinator shall have documentation such as electronic receipts that it has made the latest copy of its restoration plan and copies of the latest approved restoration plan of each Transmission Operator in its Reliability Coordinator Area available in its primary and backup control rooms and to each of its System Operators prior to the effective date in accordance with Requirement R6.

R7. Each Reliability Coordinator shall include within its operations training program, annual System restoration training for its System Operators. This training program shall address the following: *[Violation Risk Factor = Medium] [Time Horizon = Operations Planning]*

7.1. The coordination role of the Reliability Coordinator; and

7.2. Re-establishing the Interconnection.

M7. Each Reliability Coordinator shall have an electronic copy or hard copy of its training records available showing that it has provided training in accordance with Requirement R7.

R8. Each Reliability Coordinator shall conduct two System restoration drills, exercises, or simulations per calendar year, which shall include the Transmission Operators and Generator Operators as dictated by the particular scope of the drill, exercise, or simulation that is being conducted. *[Violation Risk Factor = Medium] [Time Horizon = Operations Planning]*

8.1. Each Reliability Coordinator shall request each Transmission Operator identified in its restoration plan and each Generator Operator identified in the Transmission Operators' restoration plans to participate in a drill, exercise, or simulation at least once every two calendar years.

M8. Each Reliability Coordinator shall have evidence, such as dated electronic documents, that it conducted two System restoration drills, exercises, or simulations per calendar year in accordance with Requirement R8. And each Reliability Coordinator shall have

evidence that the Reliability Coordinator requested each applicable Transmission Operator and Generator Operator to participate per Requirement R8 and Requirement R8, Part 8.1.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority:
"Compliance Enforcement Authority" means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention:
The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

- The current restoration plan and any restoration plans in effect since the last compliance audit for Requirement R1, Measure M1.
- Distribution of its most recent restoration plan and any restoration plans in effect for the current calendar year and three prior calendar years for Requirement R2, Measure M2.
- It's reviewed restoration plan for the current review period and the last three prior review periods for Requirement R3, Measure M3.
- Reviewed copies of neighboring Reliability Coordinator restoration plans for the current calendar year and the three prior calendar years for Requirement R4, Measure M4.
- The reviewed restoration plans for the current calendar year and the last three prior calendar years for Requirement R5, Measure M5.
- The current, approved restoration plan and any restoration plans in effect for the last three calendar years was made available in its control rooms for Requirement R6, Measure M6.
- Actual training program materials or descriptions for three calendar years for Requirements R7, Measure M7.

- Records of all Reliability Coordinator restoration drills, exercises, or simulations since its last compliance audit, as well as one previous compliance audit period for Requirement R8, Measure M8.

If a Reliability Coordinator is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time period specified above, whichever is longer.

The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program

As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	The Reliability Coordinator failed to include one requirement part of Requirement R1 within its restoration plan.	The Reliability Coordinator failed to include two requirement parts of Requirement R1 within its restoration plan.	The Reliability Coordinator failed to include three of the requirements parts of Requirement R1 within its restoration plan.	The Reliability Coordinator failed to include four or more of the requirement parts within its restoration plan. OR The Reliability Coordinator had a restoration plan, but failed to implement it.
R2.	The Reliability Coordinator distributed the most recent Reliability Coordinator Area restoration plan to the entities identified in Requirement R2 but was more than 30 calendar days late but less than 60 calendar days late.	The Reliability Coordinator distributed the most recent Reliability Coordinator Area restoration plan to the entities identified in Requirement R2 but was 60 calendar days or more late, but less than 90 calendar days late.	The Reliability Coordinator distributed the most recent Reliability Coordinator Area restoration plan to the entities identified in Requirement R2 but was 90 or more calendar days late but less than 120 calendar days late.	The Reliability Coordinator distributed the most recent Reliability Coordinator Area restoration plan to entities identified in Requirement R2 but was 120 calendar days or more late.
R3.	N/A	N/A	N/A	The Reliability Coordinator did not review its restoration plan within 13 calendar months of the last review.

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R4.	The Reliability Coordinator reviewed the submitted restoration plans from its neighboring Reliability Coordinators within 60 calendar days of receipt, and resolved conflicts between 31 and 60 calendar days following written notification.	The Reliability Coordinator reviewed the submitted restoration plans from its neighboring Reliability Coordinators within 60 calendar days of receipt and resolved conflicts between 61 and 90 calendar days following written notification.	The Reliability Coordinator reviewed the submitted restoration plans from its neighboring Reliability Coordinators within 60 calendar days of receipt and resolved conflicts 91 or more calendar days following written notification.	The Reliability Coordinator did not review the submitted restoration plans from its neighboring Reliability Coordinators within 60 calendar days of receipt.
R5.	The Reliability Coordinator did not review and approve/disapprove the submitted restoration plans, with stated reasons for disapproval, from its Transmission Operators and neighboring Reliability Coordinators within 30 calendar days of receipt but did review and approve/disapprove the plans within 45 calendar days of receipt. OR	The Reliability Coordinator did not review and approve/disapprove the submitted restoration plans, with stated reasons for disapproval, from its Transmission Operators and neighboring Reliability Coordinators within 30 calendar days of receipt but did review and approve/disapprove the plans within 60 calendar days of receipt. OR	The Reliability Coordinator did not review and approve/disapprove the submitted restoration plans, with stated reasons for disapproval, from its Transmission Operators and neighboring Reliability Coordinators within 30 calendar days of receipt but did review and approve/disapprove the plans within 90 calendar days of receipt. OR	The Reliability Coordinator did not review and approve/disapprove the submitted restoration plans, with stated reasons for disapproval, from its Transmission Operators and neighboring Reliability Coordinators for more than 90 calendar days of receipt. OR The Reliability Coordinator failed to notify the Transmission Operator of its

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	The Reliability Coordinator failed to notify the Transmission Operator of its approval or disapproval with stated reasons for disapproval within 30 calendar days of receipt but did notify the Transmission Operator of its approval or disapproval with reasons within 45 calendar days of receipt.	The Reliability Coordinator failed to notify the Transmission Operator of its approval or disapproval with stated reasons for disapproval within 30 calendar days of receipt, but did notify the Transmission Operator of its approval or disapproval with reasons within 60 calendar days of receipt	The Reliability Coordinator failed to notify the Transmission Operator of its approval or disapproval with stated reasons for disapproval within 30 calendar days of receipt but did notify the Transmission Operator of its approval or disapproval with reasons within 90 calendar days of receipt.	approval or disapproval with stated reasons for disapproval for more than 90 calendar days of receipt.
R6.	N/A	N/A	The Reliability Coordinator did not have a copy of the latest approved restoration plan of all Transmission Operators in its Reliability Coordinator Area within its primary and backup control rooms prior to the effective date.	The Reliability Coordinator did not have a copy of its latest restoration plan within its primary and backup control rooms prior to the effective date.
R7.	N/A	N/A	The Reliability Coordinator included the annual System restoration training within its operations training program,	The Reliability Coordinator did not include the annual System restoration training

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			but did not address both of the requirement parts.	within its operations training program.
R8.	N/A	The Reliability Coordinator only held one restoration drill, exercise, or simulation during the calendar year. OR The Reliability Coordinator did not request each applicable Transmission Operator or Generator Operator identified in its restoration plan to participate in a drill, exercise, or simulation at least once every two calendar years.	N/A	The Reliability Coordinator did not hold a restoration drill, exercise, or simulation during the calendar year.

D. Regional Variances

None.

E. Associated Documents

Link to the Implementation Plan and other important associated documents.

Version History

Version	Date	Action	Change Tracking
0	April 1, 2005	Effective Date	New
0	August 8, 2005	Removed “Proposed” from Effective Date	Errata
1	Nov. 1, 2006	Adopted by Board of Trustees	Revised
2		Revisions pursuant to Project 2006-03	Updated Measures and Compliance to match new Requirements
2	August 5, 2009	Adopted by Board of Trustees	Revised
2	March 17, 2011	Order issued by FERC approving EOP-006-2 (approval effective 5/23/11)	
2	July 1, 2013	Updated VRFs and VSLs based on June 24, 2013 approval.	
3	February 9, 2017	Adopted by the NERC Board of Trustees	Revised
3	January 18, 2018	FERC order issued approving EOP-006-3. Docket No. RM17-12-000.	

Appendix EOP-006-3-QC-1

Specific provisions applicable in Québec for standard EOP-006-3 – System Restoration Coordination

This appendix establishes specific provisions for the application of the standard in Québec. Provisions of the standard and of this appendix must be read jointly for comprehension and interpretation purposes. Where the standard and appendix differ, the appendix shall prevail.

A. Introduction

1. Title: No specific provisions.

2. Number: No specific provisions.

3. Purpose: No specific provisions.

4. Applicability:

4.1. Functional Entities

No specific provisions.

5. Effective date:

5.1. Adoption of the standard by the Régie de l'énergie: November 22, 2019

5.2. Adoption of this appendix by the Régie de l'énergie: November 22, 2019

5.3. Effective date of the standard and of this appendix in Québec: January 1st, 2021

6. Standard-Only Definition:

No specific provisions.

B. Requirements and Measures

No specific provisions.

Requirement R4 and Measure M4, erratum correction: changed "Coordinator's" to "Coordinators'"

"**R4**. Each Reliability Coordinator shall review its neighboring Reliability Coordinators' restoration plans and provide written notification of any conflicts discovered during that review within 60 calendar days of receipt. *[Violation Risk Factor = Medium] [Time Horizon = Operations Planning]*

4.1. If a Reliability Coordinator finds conflicts between its restoration plans and any of its neighbors, the conflicts shall be resolved within 30 calendar days of receipt of written notification.

M4. Each Reliability Coordinator shall provide evidence such as dated review signature sheets or electronic receipt that it has reviewed its neighboring Reliability Coordinators' restoration plans and resolved any conflicts within the timing requirements of Requirement R4 and Requirement R4, Part 4.1."

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

In Québec, "Compliance Enforcement Authority" means the Régie de l'énergie in its roles of monitoring and enforcing compliance with respect to the Reliability Standard and to this appendix.

1.2. Evidence Retention

No specific provisions.

1.3. Compliance Monitoring and Enforcement Program

The Régie de l'énergie establishes the monitoring processes used to evaluate data or information for the purpose of determining compliance or non-compliance with the Reliability Standard and with this appendix.

Violation Severity Levels

No specific provisions.

D. Regional Variances

No specific provisions.

E. Associated Documents

No specific provisions.

Version history

Version	Date	Action	Change tracking
1	November 22, 2019	New appendix	New

A. Introduction

1. **Title:** Loss of Control Center Functionality
2. **Number:** EOP-008-2
3. **Purpose:** Ensure continued reliable operations of the Bulk Electric System (BES) in the event that a control center becomes inoperable.
4. **Applicability:**
   - **4.1. Functional Entities:**
     - **4.1.1.** Reliability Coordinator
     - **4.1.2.** Transmission Operator
     - **4.1.3.** Balancing Authority
5. **Effective Date:** See the Implementation Plan for EOP-008-2.
6. **Standard-Only Definition:** None

B. Requirements and Measures

R1. Each Reliability Coordinator, Balancing Authority, and Transmission Operator shall have a current Operating Plan describing the manner in which it continues to meet its functional obligations with regard to the reliable operations of the BES in the event that its primary control center functionality is lost. This Operating Plan for backup functionality shall include: *[Violation Risk Factor = Medium] [Time Horizon = Operations Planning]*

- **1.1.** The location and method of implementation for providing backup functionality.
- **1.2.** A summary description of the elements required to support the backup functionality. These elements shall include:
  - **1.2.1.** Tools and applications to ensure that System Operators have situational awareness of the BES.
  - **1.2.2.** Data exchange capabilities.
  - **1.2.3.** Interpersonal Communications.
  - **1.2.4.** Power source(s).
  - **1.2.5.** Physical and cyber security.
- **1.3.** An Operating Process for keeping the backup functionality consistent with the primary control center.
- **1.4.** Operating Procedures, including decision authority, for use in determining when to implement the Operating Plan for backup functionality.
- **1.5.** A transition period between the loss of primary control center functionality and the time to fully implement the backup functionality that is less than or equal to two hours.

1.6. An Operating Process describing the actions to be taken during the transition period between the loss of primary control center functionality and the time to fully implement backup functionality elements identified in Requirement R1, Part 1.2. The Operating Process shall include:

1.6.1. A list of all entities to notify when there is a change in operating locations.

1.6.2. Actions to manage the risk to the BES during the transition from primary to backup functionality, as well as during outages of the primary or backup functionality.

1.6.3. Identification of the roles for personnel involved during the initiation and implementation of the Operating Plan for backup functionality.

M1. Each Reliability Coordinator, Balancing Authority, and Transmission Operator shall have a dated, current, and in effect Operating Plan for backup functionality in accordance with Requirement R1, in electronic or hardcopy format.

R2. Each Reliability Coordinator, Balancing Authority, and Transmission Operator shall have a copy of its current Operating Plan for backup functionality available at its primary control center and at the location providing backup functionality. *[Violation Risk Factor = Lower] [Time Horizon = Operations Planning]*

M2. Each Reliability Coordinator, Balancing Authority, and Transmission Operator shall have a dated, current, and in effect copy of its Operating Plan for backup functionality in accordance with Requirement R2, in electronic or hardcopy format, available at its primary control center and at the location providing backup functionality.

R3. Each Reliability Coordinator shall have a backup control center facility (provided through its own dedicated backup facility or at another entity's control center staffed with certified Reliability Coordinator operators when control has been transferred to the backup facility) that provides the functionality required for maintaining compliance with all Reliability Standards are applicable to the primary control center functionality. To avoid requiring a tertiary facility, a backup facility is not required during: *[Violation Risk Factor = High] [Time Horizon = Operations Planning]*

- Planned outages of the primary or backup facilities of two weeks or less
- Unplanned outages of the primary or backup facilities

M3. Each Reliability Coordinator shall provide dated evidence that it has a backup control center facility (provided through its own dedicated backup facility or at another entity's control center staffed with certified Reliability Coordinator operators when control has been transferred to the backup facility) that provides the functionality required for maintaining compliance with all Reliability Standards that are applicable to the primary control center functionality in accordance with Requirement R3.

R4. Each Balancing Authority and Transmission Operator shall have backup functionality (provided either through a facility or contracted services staffed by applicable certified operators when control has been transferred to the backup functionality

location) that includes monitoring, control, logging, and alarming sufficient for maintaining compliance with all Reliability Standards that are applicable to a Balancing Authority's and Transmission Operator's primary control center functionality. To avoid requiring tertiary functionality, backup functionality is not required during: *[Violation Risk Factor = High] [Time Horizon = Operations Planning]*

- Planned outages of the primary or backup functionality of two weeks or less
- Unplanned outages of the primary or backup functionality

M4. Each Balancing Authority and Transmission Operator shall provide dated evidence that its backup functionality (provided either through a facility or contracted services staffed by applicable certified operators when control has been transferred to the backup functionality location) includes monitoring, control, logging, and alarming sufficient for maintaining compliance with all Reliability Standards that are applicable to a Balancing Authority's or Transmission Operator's primary control center functionality in accordance with Requirement R4.

R5. Each Reliability Coordinator, Balancing Authority, and Transmission Operator, shall annually review and approve its Operating Plan for backup functionality. *[Violation Risk Factor = Medium] [Time Horizon = Operations Planning]*

5.1. An update and approval of the Operating Plan for backup functionality shall take place within sixty calendar days of any changes to any part of the Operating Plan described in Requirement R1.

M5. Each Reliability Coordinator, Balancing Authority, and Transmission Operator shall have evidence that its dated, current, and in effect Operating Plan for backup functionality, in electronic or hardcopy format, has been reviewed and approved annually and that it has been updated within sixty calendar days of any changes to any part of the Operating Plan described in Requirement R1 in accordance with Requirement R5.

R6. Each Reliability Coordinator, Balancing Authority, and Transmission Operator shall have primary and backup functionality that do not depend on each other for the control center functionality required to maintain compliance with Reliability Standards. *[Violation Risk Factor = Medium] [Time Horizon = Operations Planning]*

M6. Each Reliability Coordinator, Balancing Authority, and Transmission Operator shall have dated evidence that its primary and backup functionality do not depend on each other for the control center functionality required to maintain compliance with Reliability Standards in accordance with Requirement R6.

R7. Each Reliability Coordinator, Balancing Authority, and Transmission Operator shall conduct and document results of an annual test of its Operating Plan that demonstrates: *[Violation Risk Factor = Medium] [Time Horizon = Operations Planning]*

7.1. The transition time between the simulated loss of primary control center functionality and the time to fully implement the backup functionality.

7.2. The backup functionality for a minimum of two continuous hours.

M7. Each Reliability Coordinator, Balancing Authority, and Transmission Operator shall provide evidence such as dated records, that it has completed and documented its annual test of its Operating Plan for backup functionality, in accordance with Requirement R7.

R8. Each Reliability Coordinator, Balancing Authority, and Transmission Operator that has experienced a loss of its primary or backup functionality and that anticipates that the loss of primary or backup functionality will last for more than six calendar months shall provide a plan to its Regional Entity within six calendar months of the date when the functionality is lost, showing how it will re-establish primary or backup functionality. *[Violation Risk Factor = Medium] [Time Horizon = Operations Planning]*

M8. Each Reliability Coordinator, Balancing Authority, and Transmission Operator that has experienced a loss of their primary or backup functionality and that anticipates that the loss of primary or backup functionality will last for more than six calendar months shall provide evidence that a plan has been submitted to its Regional Entity within six calendar months of the date when the functionality is lost showing how it will re-establish primary or backup functionality in accordance with Requirement R8.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority:

"Compliance Enforcement Authority" means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention:

The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

- Each Reliability Coordinator, Balancing Authority, and Transmission Operator shall retain its dated, current, in effect Operating Plan for backup functionality plus all issuances of the Operating Plan for backup functionality since its last compliance audit in accordance with Measurement M1.
- Each Reliability Coordinator, Balancing Authority, and Transmission Operator shall retain a dated, current, in effect copy of its Operating Plan for backup functionality, with evidence of its last issue, available at its primary control center and at the location providing backup functionality, for the current year, in accordance with Measurement M2.
- Each Reliability Coordinator shall retain dated evidence for the time period since its last compliance audit, that it has demonstrated that it has a backup control center facility (provided through its own dedicated backup facility or at another entity's control center staffed with certified Reliability Coordinator operators when control has been transferred to the backup facility) in accordance with Requirement R3 that provides the functionality required for maintaining compliance with all Reliability Standards that are applicable to the primary control center functionality in accordance with Measurement M3.
- Each Balancing Authority and Transmission Operator shall retain dated evidence for the time period since its last compliance audit, that it has demonstrated that it's backup functionality (provided either through a facility or contracted services staffed by applicable certified operators

when control has been transferred to the backup functionality location) in accordance with Requirement R4 includes monitoring, control, logging, and alarming sufficient for maintaining compliance with all Reliability Standards that are applicable to a Balancing Authority's and Transmission Operator's primary control center functionality in accordance with Measurement M4.

- Each Reliability Coordinator, Balancing Authority, and Transmission Operator, shall retain evidence for the time period since its last compliance audit, that its dated, current, in effect Operating Plan for backup functionality, has been reviewed and approved annually and that it has been updated within sixty calendar days of any changes to any part of the Operating Plan described in Requirement R1 in accordance with Measurement M5.
- Each Reliability Coordinator, Balancing Authority, and Transmission Operator shall retain dated evidence for the current year and for any Operating Plan for backup functionality in effect since its last compliance audit, that its primary and backup functionality do not depend on each other for the control center functionality required to maintain compliance with Reliability Standards in accordance with Measurement M6.
- Each Reliability Coordinator, Balancing Authority, and Transmission Operator shall retain evidence for the current calendar year and the previous calendar years, such as dated records, that it has tested its Operating Plan for backup functionality, in accordance with Measurement M7.
- Each Reliability Coordinator, Balancing Authority, and Transmission Operator that has experienced a loss of their primary or backup functionality and that anticipates that the loss of primary or backup functionality would last for more than six calendar months shall retain evidence for the current in effect document and any such documents in effect since its last compliance audit that a plan has been submitted to its Regional Entity within six calendar months of the date when the functionality is lost showing how it will re-establish primary or backup functionality in accordance with Measurement M8.

1.3. Compliance Monitoring and Enforcement Program

As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	The responsible entity had a current Operating Plan for backup functionality, but the plan was missing one of the requirement's six parts (Requirement R1, Parts 1.1 through 1.6).	The responsible entity had a current Operating Plan for backup functionality, but the plan was missing two of the requirement's six parts (Requirement R1, Parts 1.1 through 1.6).	The responsible entity had a current Operating Plan for backup functionality, but the plan was missing three of the requirement's six parts (Requirement R1, Parts 1.1 through 1.6).	The responsible entity had a current Operating Plan for backup functionality, but the plan was missing four or more of the requirement's six parts (Requirement R1, Parts 1.1 through 1.6) OR The responsible entity did not have a current Operating Plan for backup functionality.
R2.	N/A	The responsible entity did not have a copy of its current Operating Plan for backup functionality available in at least one of its control locations.	N/A	The responsible entity did not have a copy of its current Operating Plan for backup functionality at any of its locations.
R3.	N/A	N/A	N/A	The Reliability Coordinator does not have a backup control center facility (provided through its own dedicated backup facility or at another entity's control

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				center staffed with certified Reliability Coordinator operators when control has been transferred to the backup facility) that provides the functionality required for maintaining compliance with all Reliability Standards that are applicable to the primary control center functionality.
R4.	N/A	N/A	N/A	The responsible entity does not have backup functionality (provided either through a facility or contracted services staffed by applicable certified operators when control has been transferred to the backup functionality location) that includes monitoring, control, logging, and alarming sufficient for maintaining compliance with all Reliability Standards that are applicable to a Balancing Authority's and Transmission Operator's

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				primary control center functionality.
R5.	The responsible entity did not update and approve its Operating Plan for backup functionality for more than 60 calendar days and less than or equal to 70 calendar days after a change to any part of the Operating Plan described in Requirement R1.	The responsible entity did not update and approve its Operating Plan for backup functionality for more than 70 calendar days and less than or equal to 80 calendar days after a change to any part of the Operating Plan described in Requirement R1.	The responsible entity did not update and approve its Operating Plan for backup functionality for more than 80 calendar days and less than or equal to 90 calendar days after a change to any part of the Operating Plan described in Requirement R1.	The responsible entity did not have evidence that its Operating Plan for backup functionality was annually reviewed and approved. OR, The responsible entity did not update and approve its Operating Plan for backup functionality for more than 90 calendar days after a change to any part of the Operating Plan described in Requirement R1.
R6.	N/A	N/A	N/A	The responsible entity has primary and backup functionality that do depend on each other for the control center functionality required to maintain compliance with Reliability Standards.
R7.	The responsible entity conducted an annual test of	The responsible entity conducted an annual test of	The responsible entity conducted an annual test of	The responsible entity did not conduct an annual test

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	its Operating Plan for backup functionality, but it did not document the results. OR, The responsible entity conducted an annual test of its Operating Plan for backup functionality, but the test was for less than two continuous hours but more than or equal to 1.5 continuous hours.	its Operating Plan for backup functionality, but the test was for less than 1.5 continuous hours but more than or equal to 1 continuous hour.	its Operating Plan for backup functionality, but the test did not assess the transition time between the simulated loss of its primary control center and the time to fully implement the backup functionality OR, The responsible entity conducted an annual test of its Operating Plan for backup functionality, but the test was for less than 1 continuous hour but more than or equal to 0.5 continuous hours.	of its Operating Plan for backup functionality. OR, The responsible entity conducted an annual test of its Operating Plan for backup functionality, but the test was for less than 0.5 continuous hours.
R8.	The responsible entity experienced a loss of its primary or backup functionality and anticipated that the loss of primary or backup functionality would last for more than six calendar months and provided a plan to its	The responsible entity experienced a loss of its primary or backup functionality and anticipated that the loss of primary or backup functionality would last for more than six calendar months provided a plan to its Regional Entity	The responsible entity experienced a loss of its primary or backup functionality and anticipated that the loss of primary or backup functionality would last for more than six calendar months provided a plan to its Regional Entity	The responsible entity experienced a loss of its primary or backup functionality and anticipated that the loss of primary or backup functionality would last for more than six calendar months, but did not submit a plan to its Regional

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	Regional Entity showing how it will re-establish primary or backup functionality but the plan was submitted more than six calendar months but less than or equal to seven calendar months after the date when the functionality was lost.	showing how it will re-establish primary or backup functionality but the plan was submitted in more than seven calendar months but less than or equal to eight calendar months after the date when the functionality was lost.	showing how it will re-establish primary or backup functionality but the plan was submitted in more than eight calendar months but less than or equal to nine calendar months after the date when the functionality was lost.	Entity showing how it will re-establish primary or backup functionality for more than nine calendar months after the date when the functionality was lost.

D. Regional Variances

None.

E. Associated Documents

Link to the Implementation Plan and other important associated documents.

Version History

Version	Date	Action	Change Tracking
1	2009 - 2010	Project 2006-04: Revisions	Major re-write to accommodate changes noted in project file
1	August 5, 2010	Project 2006-04: Adopted by the Board	
1	April 21, 2011	Project 2006-04: FERC Order issued approving EOP-008-1 (approval effective June 27, 2011)	
1	July 1, 2013	Project 2006-04: Updated VRFs and VSLs based on June 24, 2013 approval	
2	July 9, 2017	Adopted by the NERC Board of Trustees	Revised
2	January 18, 2018	FERC order issued approving EOP-008-2. Docket No. RM17-12-000.	

Rationale

Rationale for Requirement R1: The phrase "data exchange capabilities" is replacing “data communications in Requirement R1, Part 1.2.2 for the following reasons:

COM-001-1 (no longer enforceable) covered telecommunications, which could be viewed as covering both voice and data. COM-001-2.1 (currently enforceable) focuses on "Interpersonal Communication" and does not address data.

The topic of data exchange has historically been covered in the IRO / TOP Standards. Most recently the revisions to the standards that came out of Project 2014-03 Revisions to TOP and IRO Standards use the phrase "data exchange capabilities." The rationale included in the IRO-002-4 standard discusses the need to retain the topic of data exchange, as it is not addressed in the COM standards.

Appendix EOP-008-2-QC-1

Specific provisions applicable in Québec for standard EOP-008-2 – Loss of Control Center Functionality

This appendix establishes specific provisions for the application of the standard in Québec. Provisions of the standard and of this appendix must be read jointly for comprehension and interpretation purposes. Where the standard and appendix differ, the appendix shall prevail.

A. Introduction

1. Title: No specific provisions.

2. Number: No specific provisions.

3. Purpose: No specific provisions.

4. Applicability:

4.1. Functional Entities

No specific provisions.

5. Effective date:

5.1. Adoption of the standard by the Régie de l'énergie: November 22, 2019

5.2. Adoption of this appendix by the Régie de l'énergie: November 22, 2019

5.3. Effective date of the standard and of this appendix in Québec: January 1st, 2021

6. Standard-Only Definition:

No specific provisions.

B. Requirements and Measures

Replace "BES" by "RTP" in this section.

Requirement 3, erratum correction: added the word "that" in the following part of the sentence "all Reliability Standards that are applicable to the primary control center functionality "

"Each Reliability Coordinator shall have a backup control center facility (provided through its own dedicated backup facility or at another entity's control center staffed with certified Reliability Coordinator operators when control has been transferred to the backup facility) that provides the functionality required for maintaining compliance with all Reliability Standards that are applicable to the primary control center functionality. To avoid requiring a tertiary facility, a backup facility is not required during: *[Violation Risk Factor = High] [Time Horizon = Operations Planning]*

- Planned outages of the primary or backup facilities of two weeks or less
- Unplanned outages of the primary or backup facilities"

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

In Québec, "Compliance Enforcement Authority" means the Régie de l'énergie in its roles of monitoring and enforcing compliance with respect to the Reliability Standard and to this appendix.

1.2. Evidence Retention

No specific provisions.

1.3. Compliance Monitoring and Enforcement Program

The Régie de l'énergie establishes the monitoring processes used to evaluate data or information for the purpose of determining compliance or non-compliance with the Reliability Standard and with this appendix.

Violation Severity Levels

No specific provisions.

D. Regional Variances

No specific provisions.

E. Associated Documents

No specific provisions.

Version history

Version	Date	Action	Change tracking
1	November 22, 2019	New appendix	New

A. Introduction

1. **Title: Geomagnetic Disturbance Operations**

2. **Number:** EOP-010-1

3. **Purpose:** To mitigate the effects of geomagnetic disturbance (GMD) events by implementing Operating Plans, Processes, and Procedures.

4. **Applicability:**

   4.1. Functional Entities:

   4.1.1 Reliability Coordinator

   4.1.2 Transmission Operator with a Transmission Operator Area that includes a power transformer with a high side wye-grounded winding with terminal voltage greater than 200 kV

5. **Background:**

Geomagnetic disturbance (GMD) events have the potential to adversely impact the reliable operation of interconnected transmission systems. During a GMD event, geomagnetically-induced currents (GIC) may cause transformer hot-spot heating or damage, loss of Reactive Power sources, increased Reactive Power demand, and Protection System Misoperation, the combination of which may result in voltage collapse and blackout.

6. **Effective Date:**

The first day of the first calendar quarter that is six months after the date that this standard is approved by an applicable governmental authority or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective on the first day of the first calendar quarter that is six months after the date this standard is adopted by the NERC Board of Trustees or as otherwise provided for in that jurisdiction.

B. Requirements and Measures

R1. Each Reliability Coordinator shall develop, maintain, and implement a GMD Operating Plan that coordinates GMD Operating Procedures or Operating Processes within its Reliability Coordinator Area. At a minimum, the GMD Operating Plan shall include: *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning, Operations Planning, Same-day Operations, Real-time Operations]*

1.1 A description of activities designed to mitigate the effects of GMD events on the reliable operation of the interconnected transmission system within the Reliability Coordinator Area.

1.2 A process for the Reliability Coordinator to review the GMD Operating Procedures or Operating Processes of Transmission Operators within its Reliability Coordinator Area.

M1. Each Reliability Coordinator shall have a current GMD Operating Plan meeting all the provisions of Requirement R1; evidence such as a review or revision history to indicate that the GMD Operating Plan has been maintained; and evidence to show that the plan was implemented as called for in its GMD Operating Plan, such as dated operator logs, voice recordings, or voice transcripts.

R2. Each Reliability Coordinator shall disseminate forecasted and current space weather information to functional entities identified as recipients in the Reliability Coordinator's GMD Operating Plan. *[Violation Risk Factor: Medium] [Time Horizon: Same-day Operations, Real-time Operations]*

M2. Each Reliability Coordinator shall have evidence such as dated operator logs, voice recordings, transcripts, or electronic communications to indicate that forecasted and current space weather information was disseminated as stated in its GMD Operating Plan.

R3. Each Transmission Operator shall develop, maintain, and implement a GMD Operating Procedure or Operating Process to mitigate the effects of GMD events on the reliable operation of its respective system. At a minimum, the Operating Procedure or Operating Process shall include: *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning, Operations Planning, Same-day Operations, Real-Time Operations]*

3.1. Steps or tasks to receive space weather information.

3.2. System Operator actions to be initiated based on predetermined conditions.

3.3. The conditions for terminating the Operating Procedure or Operating Process.

M3. Each Transmission Operator shall have a GMD Operating Procedure or Operating Process meeting all the provisions of Requirement R3; evidence such as a review or revision history to indicate that the GMD Operating Procedure or Operating Process has been maintained; and evidence to show that the Operating Procedure or Operating Process was implemented as called for in its GMD Operating Procedure or Operating Process, such as dated operator logs, voice recordings, or voice transcripts.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since

the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Reliability Coordinator and Transmission Operator shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

The responsible entities shall retain documentation as evidence for three years.

If a responsible entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.

The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audit

Self-Certification

Spot Check

Compliance Investigation

Self-Reporting

Complaint

1.4. Additional Compliance Information

None

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	Long-term Planning, Operations Planning, Same-day Operations, Real-time Operations	Medium	The Reliability Coordinator had a GMD Operating Plan, but failed to maintain it.	N/A	The Reliability Coordinator's GMD Operating Plan failed to include one of the required elements as listed in Requirement R1, parts 1.1 or 1.2.	The Reliability Coordinator did not have a GMD Operating Plan OR The Reliability Coordinator failed to implement a GMD Operating Plan within its Reliability Coordinator Area.
R2	Same-day Operations, Real-time Operations	Medium	N/A	N/A	N/A	The Reliability Coordinator failed to disseminate forecasted and current space weather information to all functional entities identified as recipients in the Reliability Coordinator's GMD Operating Plan.
R3	Long-term Planning, Operations Planning,	Medium	The Transmission Operator had a GMD Operating Procedure or Operating Process,	The Transmission Operator's GMD Operating Procedure or Operating Process	The Transmission Operator's GMD Operating Procedure or Operating Process	The Transmission Operator did not have a GMD Operating Procedure or Operating

	Same-day Operations, Real-time Operations		but failed to maintain it.	failed to include one of the required elements as listed in Requirement R3, parts 3.1 through 3.3.	failed to include two or more of the required elements as listed in Requirement R3, parts 3.1 through 3.3.	Process OR The Transmission Operator failed to implement its GMD Operating Procedure or Operating Process.

D. Regional Variances

None.

E. Interpretations

None.

F. Guideline and Technical Basis

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for R1:

An Operating Plan is implemented by carrying out its stated actions.

Coordination is intended to ensure that Operating Procedures are not in conflict with one another. An Operating Plan is maintained when it is kept relevant by taking into consideration system configuration, conditions, or operating experience, as needed to accomplish its purpose.

Elements of Requirement R1 take place in various time horizons. Development of the GMD Operating Plan occurs in the Long-Term Planning Time Horizon. Maintenance of the GMD Operating Plan occurs in the Operations Planning Time Horizon. Implementation of the GMD Operating Plan occurs in the Operations Planning, Same-Day and Real-Time Time Horizons.

Rationale for R2:

Requirement R2 replaces IRO-005-3.1a, Requirement R3. IRO-005-4 has been adopted by the NERC Board and filed with FERC, and will retire IRO-005-3.1a Requirement R3. If EOP-010-1 becomes effective prior to the retirement of IRO-005-3.1a, Requirement R2 shall become effective on the first day following retirement of IRO-005-3.1a.

Space weather forecast information can be used for situational awareness and safe posturing of the system. Current space weather information can be used for monitoring progress of a GMD event.

The Reliability Coordinator is responsible for disseminating space weather information to ensure coordination and consistent awareness in its Reliability Coordinator Area.

Rationale for R3:

In developing an Operating Procedure or Operating Process, an entity may consider entity-specific factors such as geography, geology, and system topology.

An Operating Procedure or Operating Process is maintained when it is kept relevant by taking into consideration system configuration, conditions, or operating experience, as needed to accomplish its purpose.

Version History

Version	Date	Action	Change Tracking
1	11/07/2013	Adopted by the NERC Board of Trustees	
1	6/19/2014	FERC Order issued approving EOP-010-1	

Appendix QC-EOP-010-1
Provisions specific to the standard EOP-010-1 applicable in Québec

This appendix establishes specific provisions for the application of the standard in Québec. Provisions of the standard and of its appendix must be read together for the purposes of understanding and interpretation. Where the standard and appendix differ, the appendix shall prevail.

A. Introduction

1. Title: **Geomagnetic Disturbance Operation**

2. Number: EOP-010-1

3. Purpose: No specific provision

4. Applicability:

No specific provisions

5. Background:

No specific provisions

6. Effective Date:

6.1. Adoption of the standard by the Régie de l'énergie: September 30, 2016

6.2. Adoption of the appendix by the Régie de l'énergie: February 17, 2021

6.3. Effective date of the standard and its appendix in Québec:

Requirement	Effective date in Québec
R1, R3	January 1, 2017
R2	April 1st, 2021

B. Requirements and Measures

No specific provision

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

The Régie de l'énergie is responsible, in Québec, for compliance monitoring with respect to the reliability standard and its appendix that it adopts.

1.2. Evidence Retention

No specific provision

1.3. Compliance Monitoring and Assessment Processes

No specific provision

1.4. Additional Compliance Information

No specific provisions

Table of Compliance Elements

No specific provision

D. Regional Differences

No specific provision

E. Interpretation

No specific provision

F. Guideline and Technical Basis

No specific provisions

Revision History

Revision	Adoption Date	Action	Change Tracking
0	September 30, 2016	New Appendix	New
1	February 17, 2021	Modified effective date of Requirement R2 in decision D-2021-015 under filing R-4123-2020.	Revision

A. Introduction

1. **Title:** **Emergency Preparedness and Operations**

2. **Number:** **EOP-011-2**

3. **Purpose:** To address the effects of operating emergencies by ensuring each Transmission Operator, Balancing Authority, and Generator Owner has developed plan(s) to mitigate operating Emergencies and that those plans are implemented and coordinated within the Reliability Coordinator Area as specified within the requirements.

4. **Applicability:**

   4.1. Functional Entities:

   4.1.1 Balancing Authority

   4.1.2 Reliability Coordinator

   4.1.3 Transmission Operator

   3.1.4 Generator Owner

   3.1.5 Generator Operator

   4.2. Facilities

   4.2.1 For the purpose of this standard, the term “generating unit” means all Bulk Electric System generators.

5. **Effective Date:** See Implementation Plan for Project 2019-06.

B. Requirements and Measures

R1. Each Transmission Operator shall develop, maintain, and implement one or more Reliability Coordinator-reviewed Operating Plan(s) to mitigate operating Emergencies in its Transmission Operator Area. The Operating Plan(s) shall include the following, as applicable: *[Violation Risk Factor: High] [Time Horizon: Real-Time Operations, Operations Planning, Long-term Planning]*

1.1. Roles and responsibilities for activating the Operating Plan(s);

1.2. Processes to prepare for and mitigate Emergencies including:

1.2.1. Notification to its Reliability Coordinator, to include current and projected conditions, when experiencing an operating Emergency;

1.2.2. Cancellation or recall of Transmission and generation outages;

1.2.3. Transmission system reconfiguration;

1.2.4. Redispatch of generation request;

1.2.5. Provisions for operator-controlled manual Load shedding that minimizes the overlap with automatic Load shedding and are capable of being implemented in a timeframe adequate for mitigating the Emergency; and

1.2.6. Provisions to determine reliability impacts of:

1.2.6.1. cold weather conditions; and

1.2.6.2. extreme weather conditions.

M1. Each Transmission Operator will have a dated Operating Plan(s) developed in accordance with Requirement R1 and reviewed by its Reliability Coordinator; evidence such as a review or revision history to indicate that the Operating Plan(s) has been maintained; and will have as evidence, such as operator logs or other operating documentation, voice recordings or other communication documentation to show that its Operating Plan(s) was implemented for times when an Emergency has occurred, in accordance with Requirement R1.

R2. Each Balancing Authority shall develop, maintain, and implement one or more Reliability Coordinator-reviewed Operating Plan(s) to mitigate Capacity Emergencies and Energy Emergencies within its Balancing Authority Area. The Operating Plan(s) shall include the following, as applicable: *[Violation Risk Factor: High] [Time Horizon: Real-Time Operations, Operations Planning, Long-term Planning]*

2.1. Roles and responsibilities for activating the Operating Plan(s);

2.2. Processes to prepare for and mitigate Emergencies including:

2.2.1. Notification to its Reliability Coordinator, to include current and projected conditions when experiencing a Capacity Emergency or Energy Emergency;

2.2.2. Requesting an Energy Emergency Alert, per Attachment 1;

2.2.3. Managing generating resources in its Balancing Authority Area to address:

2.2.3.1. capability and availability;

2.2.3.2. fuel supply and inventory concerns;

2.2.3.3. fuel switching capabilities; and

2.2.3.4. environmental constraints.

2.2.4. Public appeals for voluntary Load reductions;

2.2.5. Requests to government agencies to implement their programs to achieve necessary energy reductions;

2.2.6. Reduction of internal utility energy use;

2.2.7. Use of Interruptible Load, curtailable Load and demand response;

2.2.8. Provisions for operator-controlled manual Load shedding that minimizes the overlap with automatic Load shedding and are capable of being implemented in a timeframe adequate for mitigating the Emergency; and

2.2.9. Provisions to determine reliability impacts of:

2.2.9.1. cold weather conditions; and

2.2.9.2. extreme weather conditions.

M2. Each Balancing Authority will have a dated Operating Plan(s) developed in accordance with Requirement R2 and reviewed by its Reliability Coordinator; evidence such as a review or revision history to indicate that the Operating Plan(s) has been maintained; and will have as evidence, such as operator logs or other operating documentation, voice recordings, or other communication documentation to show that its Operating Plan(s) was implemented for times when an Emergency has occurred, in accordance with Requirement R2.

R3. The Reliability Coordinator shall review the Operating Plan(s) to mitigate operating Emergencies submitted by a Transmission Operator or a Balancing Authority regarding any reliability risks that are identified between Operating Plans. *[Violation Risk Factor: High] [Time Horizon: Operations Planning]*

3.1. Within 30 calendar days of receipt, the Reliability Coordinator shall:

3.1.1. Review each submitted Operating Plan(s) on the basis of compatibility and inter-dependency with other Balancing Authorities' and Transmission Operators' Operating Plans;

3.1.2. Review each submitted Operating Plan(s) for coordination to avoid risk to Wide Area reliability; and

3.1.3. Notify each Balancing Authority and Transmission Operator of the results of its review, specifying any time frame for resubmittal of its Operating Plan(s) if revisions are identified.

M3. The Reliability Coordinator will have documentation, such as dated e-mails or other correspondences that it reviewed Transmission Operator and Balancing Authority Operating Plans within 30 calendar days of submittal in accordance with Requirement R3.

R4. Each Transmission Operator and Balancing Authority shall address any reliability risks identified by its Reliability Coordinator pursuant to Requirement R3 and resubmit its Operating Plan(s) to its Reliability Coordinator within a time period specified by its Reliability Coordinator. *[Violation Risk Factor: High] [Time Horizon: Operation Planning]*

M4. The Transmission Operator and Balancing Authority will have documentation, such as dated emails or other correspondence, with an Operating Plan(s) version history showing that it responded and updated the Operating Plan(s) within the timeframe identified by its Reliability Coordinator in accordance with Requirement R4.

R5. Each Reliability Coordinator that receives an Emergency notification from a Transmission Operator or Balancing Authority within its Reliability Coordinator Area shall notify, within 30 minutes from the time of receiving notification, other Balancing Authorities and Transmission Operators in its Reliability Coordinator Area, and

neighboring Reliability Coordinators. *[Violation Risk Factor: High] [Time Horizon: Real-Time Operations]*

M5. Each Reliability Coordinator that receives an Emergency notification from a Balancing Authority or Transmission Operator within its Reliability Coordinator Area will have, and provide upon request, evidence that could include, but is not limited to, operator logs, voice recordings or transcripts of voice recordings, electronic communications, or equivalent evidence that will be used to determine if the Reliability Coordinator communicated, in accordance with Requirement R5, with other Balancing Authorities and Transmission Operators in its Reliability Coordinator Area, and neighboring Reliability Coordinators .

R6. Each Reliability Coordinator that has a Balancing Authority experiencing a potential or actual Energy Emergency within its Reliability Coordinator Area shall declare an Energy Emergency Alert, as detailed in Attachment 1. *[Violation Risk Factor: High] [Time Horizon: Real-Time Operations]*

M6. Each Reliability Coordinator, with a Balancing Authority experiencing a potential or actual Energy Emergency within its Reliability Coordinator Area, will have, and provide upon request, evidence that could include, but is not limited to, operator logs, voice recordings or transcripts of voice recordings, electronic communications, or equivalent evidence that it declared an Energy Emergency Alert, as detailed in Attachment 1, in accordance with Requirement R6.

R7. Each Generator Owner shall implement and maintain one or more cold weather preparedness plan(s) for its generating units. The cold weather preparedness plan(s) shall include the following, at a minimum: [*Violation Risk Factor: High*] [*Time Horizon: Operations Planning and Real-Time Operations*]

7.1. Generating unit(s) freeze protection measures based on geographical location and plant configuration;

7.2. Annual inspection and maintenance of generating unit(s) freeze protection measures;

7.3. Generating unit(s) cold weather data, to include:

7.3.1. Generating unit(s) operating limitations in cold weather to include:

7.3.1.1. capability and availability;

7.3.1.2. fuel supply and inventory concerns;

7.3.1.3. fuel switching capabilities; and

7.3.1.4. environmental constraints.

7.3.2. Generating unit(s) minimum:

7.3.2.1. design temperature; or

7.3.2.2. historical operating temperature; or

7.3.1.3. current cold weather performance temperature determined by an engineering analysis.

M7. Each Generator Owner will have evidence documenting that its cold weather preparedness plan(s) was implemented and maintained in accordance with Requirement R7.

R8. Each Generator Owner in conjunction with its Generator Operator shall identify the entity responsible for providing the generating unit-specific training, and that identified entity shall provide the training to its maintenance or operations personnel responsible for implementing cold weather preparedness plan(s) developed pursuant to Requirement R7. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning, Operations Planning]*

M8. Each Generator Operator or Generator Owner will have documented evidence that the applicable personnel completed training of the Generator Owner's cold weather preparedness plan(s). This evidence may include, but is not limited to, documents such as personnel training records, training materials, date of training, agendas or learning objectives, attendance at pre-work briefings, review of work order tasks, tailboards, attendance logs for classroom training, and completion records for computer-based training in fulfillment of Requirement R8.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

"Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with the mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention

The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

- The Transmission Operator shall retain the current Operating Plan(s), evidence of review or revision history plus each version issued since the last audit and evidence of compliance since the last audit for Requirements R1 and R4 and Measures M1 and M4.
- The Balancing Authority shall retain the current Operating Plan(s), evidence of review or revision history plus each version issued since the last audit and

evidence of compliance since the last audit for Requirements R2 and R4, and Measures M2 and M4.

- The Reliability Coordinator shall maintain evidence of compliance since the last audit for Requirements R3, R5, and R6 and Measures M3, M5, and M6.
- The Generator Owner shall retain the cold weather preparedness plan(s), evidence of review or revision history plus each version issued since the last audit and evidence of compliance since the last audit for Requirement R7 and Measure M7.

1.3. The Generator Owner or Generator Operator shall keep data or evidence to show compliance for three years or since its last compliance audit, whichever timeframe is greater, unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation, for Requirement R8 and Measure M8. **Compliance Monitoring and Enforcement Program:**

As defined in the NERC Rules of Procedure; "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	Real-time Operations, Operations Planning, Long-term Planning	High	N/A	The Transmission Operator developed a Reliability Coordinator-reviewed Operating Plan(s) to mitigate operating Emergencies in its Transmission Operator Area but failed to maintain it.	The Transmission Operator developed an Operating Plan(s) to mitigate operating Emergencies in its Transmission Operator Area but failed to have it reviewed by its Reliability Coordinator.	The Transmission Operator failed to develop an Operating Plan(s) to mitigate operating Emergencies in its Transmission Operator Area. OR The Transmission Operator developed a Reliability Coordinator-reviewed Operating Plan(s) to mitigate operating Emergencies in its Transmission s Operator Area but failed to implement it.
R2	Real-time Operations, Operations	High	N/A	The Balancing Authority developed a Reliability Coordinator-	The Balancing Authority developed an Operating Plan(s) to mitigate operating	The Balancing Authority failed to develop an

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
	Planning, Long-term Planning			reviewed Operating Plan(s) to mitigate operating Emergencies within its Balancing Authority Area but failed to maintain it.	Emergencies within its Balancing Authority Area but failed to have it reviewed by its Reliability Coordinator.	Operating Plan(s) to mitigate operating Emergencies within its Balancing Authority Area. OR The Balancing Authority developed a Reliability Coordinator-reviewed Operating Plan(s) to mitigate operating Emergencies within its Balancing Authority Area but failed to implement it.
R3	Operations Planning	High	N/A	N/A	The Reliability Coordinator identified a reliability risk but failed to notify the Balancing Authority or Transmission	The Reliability Coordinator identified a reliability risk but failed to notify the Balancing Authority or Transmission Operator.

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					Operator within 30 calendar days.	
R4	Operations Planning	High	N/A	N/A	The Transmission Operator or Balancing Authority failed to update and resubmit tis Operating Plan(s) to its Reliability Coordinator within the timeframe specified by its Reliability Coordinator.	The Transmission Operator or Balancing Authority failed to update and resubmit its Operating Plan(s) to its Reliability Coordinator.
R5	Real-time Operations	High	N/A	N/A	The Reliability Coordinator that received an Emergency notification from a Transmission Operator or Balancing Authority did notify neighboring Reliability Coordinators, Balancing Authorities	The Reliability Coordinator that received an Emergency notification from a Transmission Operator or Balancing Authority failed to notify neighboring Reliability Coordinators, Balancing Authorities

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					and Transmission Operators but failed to notify within 30 minutes from the time of receiving notification.	and Transmission Operators.
R6	Real-time Operations	High	N/A	N/A	N/A	The Reliability Coordinator that had a Balancing Authority experiencing a potential or actual Energy Emergency within its Reliability Coordinator Area failed to declare an Energy Emergency Alert.
R7	Operations Planning and Real-time Operations	High	The Generator Owner implemented a cold weather preparedness plan(s) but failed to maintain it.	The Generator Owner's cold weather preparedness plan failed to include one of the applicable requirement Parts within Requirement R7.	The Generator Owner had and maintained a cold weather preparedness plan(s) but failed to fully implement it. OR	The Generator Owner does not have a cold weather preparedness plan. OR The Generator Owner has a cold

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					The Generator Owner's cold weather preparedness plan failed to include two of the applicable requirement Parts within Requirement R7.	weather preparedness plan, but failed to include any of the applicable requirement Parts within Requirement R7.
R8	Operations Planning and Real-time Operations	Medium	The Generator Owner or Generator Operator failed to provide generating unit-specific training as described in Requirement R8 to the greater of: • one applicable personnel at a single generating unit; or • 5% or less of its total applicable personnel.	The Generator Owner or Generator Operator failed to provide generating unit-specific training as described in Requirement R8 to the greater of: • two applicable personnel at a single generating unit; or • more than 5% or less than or equal to 10% of its total applicable personnel.	The Generator Owner or Generator Operator failed to provide generating unit-specific training as described in Requirement R8 to the greater of: • three applicable personnel at a single generating unit; or • more than 10% or less than or equal to 15% of its total applicable personnel.	The Generator Owner or Generator Operator failed to provide generating unit-specific training as described in Requirement R8 to the greater of: • four applicable personnel at a single generating unit; or • more than 15% of its total applicable personnel.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	November 13, 2014	Adopted by Board of Trustees	Merged EOP-001-2.1b, EOP-002-3.1 and EOP-003-2.
1	November 19, 2015	FERC approved EOP-011-1. Docket Nos. RM15-7-000, RM15-12-000, and RM15-13-000. Order No. 818	
2	June 11,2021	Adopted by the Board of Trustees	Revised under Project 2019-06
2	August 24,2021	FERC approved EOP-011-2. Docket Number RD21-5-000	
2	August 24,2021	April 1, 2023	Effective Date

Attachment 1-EOP-011-2
Energy Emergency Alerts

Introduction

This Attachment provides the process and descriptions of the levels used by the Reliability Coordinator in which it communicates the condition of a Balancing Authority which is experiencing an Energy Emergency.

A. General Responsibilities

1. **Initiation by Reliability Coordinator.** An Energy Emergency Alert (EEA) may be initiated only by a Reliability Coordinator at 1) the Reliability Coordinator's own request, or 2) upon the request of an energy deficient Balancing Authority.
2. **Notification**. A Reliability Coordinator who declares an EEA shall notify all Balancing Authorities and Transmission Operators in its Reliability Coordinator Area. The Reliability Coordinator shall also notify all neighboring Reliability Coordinators.

B. EEA Levels

Introduction

To ensure that all Reliability Coordinators clearly understand potential and actual Energy Emergencies in the Interconnection, NERC has established three levels of EEAs. The Reliability Coordinators will use these terms when communicating Energy Emergencies to each other. An EEA is an Emergency procedure, not a daily operating practice, and is not intended as an alternative to compliance with NERC Reliability Standards.

The Reliability Coordinator may declare whatever alert level is necessary, and need not proceed through the alerts sequentially.

1. **EEA 1 — All available generation resources in use.**

Circumstances:

- The Balancing Authority is experiencing conditions where all available generation resources are committed to meet firm Load, firm transactions, and reserve commitments, and is concerned about sustaining its required Contingency Reserves.
- Non-firm wholesale energy sales (other than those that are recallable to meet reserve requirements) have been curtailed.

2. **EEA 2 — Load management procedures in effect**.

Circumstances:

- The Balancing Authority is no longer able to provide its expected energy requirements and is an energy deficient Balancing Authority.
- An energy deficient Balancing Authority has implemented its Operating Plan(s) to mitigate Emergencies.

- An energy deficient Balancing Authority is still able to maintain minimum Contingency Reserve requirements.

During EEA 2, Reliability Coordinators and energy deficient Balancing Authorities have the following responsibilities:

2.1 Notifying other Balancing Authorities **and market participants**. The energy deficient Balancing Authority shall communicate its needs to other Balancing Authorities and market participants. Upon request from the energy deficient Balancing Authority, the respective Reliability Coordinator shall post the declaration of the alert level, along with the name of the energy deficient Balancing Authority on the RCIS website.

2.2 Declaration period. The energy deficient Balancing Authority shall update its Reliability Coordinator of the situation at a minimum of every hour until the EEA 2 is terminated. The Reliability Coordinator shall update the energy deficiency information posted on the RCIS website as changes occur and pass this information on to the neighboring Reliability Coordinators, Balancing Authorities and Transmission Operators**.**

2.3 Sharing information on resource availability. Other Reliability Coordinators of Balancing Authorities with available resources shall coordinate, as appropriate, with the Reliability Coordinator that has an energy deficient Balancing Authority.

2.4 Evaluating and mitigating Transmission limitations. The Reliability Coordinator shall review Transmission outages and work with the Transmission Operator(s) to see if it's possible to return to service any Transmission Elements that may relieve the loading on System Operating Limits (SOLs) or Interconnection Reliability Operating Limits (IROLs).

2.5 Requesting Balancing Authority actions. Before requesting an EEA 3, the energy deficient Balancing Authority must make use of all available resources; this includes, but is not limited to:

2.5.1 All available generation units are on line. All generation capable of being on line in the time frame of the Emergency is on line.

2.5.2 Demand-Side Management. Activate Demand-Side Management within provisions of any applicable agreements.

3. EEA 3 —Firm Load interruption is imminent or in progress.

Circumstances:

- The energy deficient Balancing Authority is unable to meet minimum Contingency Reserve requirements.

During EEA 3, Reliability Coordinators and Balancing Authorities have the following responsibilities:

3.1 Continue actions from EEA 2. The Reliability Coordinators and the energy deficient Balancing Authority shall continue to take all actions initiated during EEA 2.

3.2 Declaration Period. The energy deficient Balancing Authority shall update its Reliability Coordinator of the situation at a minimum of every hour until the EEA 3 is terminated. The Reliability Coordinator shall update the energy deficiency information posted on the RCIS website as changes occur and pass this information on to the neighboring Reliability Coordinators, Balancing Authorities, and Transmission Operators.

3.3 Reevaluating and revising SOLs and IROLs. The Reliability Coordinator shall evaluate the risks of revising SOLs and IROLs for the possibility of delivery of energy to the energy deficient Balancing Authority. Reevaluation of SOLs and IROLs shall be coordinated with other Reliability Coordinators and only with the agreement of the Transmission Operator whose Transmission Owner (TO) equipment would be affected. SOLs and IROLs shall only be revised as long as an EEA 3 condition exists, or as allowed by the Transmission Owner whose equipment is at risk. The following are minimum requirements that must be met before SOLs or IROLs are revised:

3.3.1 Energy deficient Balancing Authority obligations. The energy deficient Balancing Authority, upon notification from its Reliability Coordinator of the situation, it will immediately take whatever actions are necessary to mitigate any undue risk to the Interconnection. These actions may include Load shedding.

3.4 Returning to pre-Emergency conditions. Whenever energy is made available to an energy deficient Balancing Authority such that the Systems can be returned to its pre-Emergency SOLs or IROLs condition, the energy deficient Balancing Authority shall request the Reliability Coordinator to downgrade the alert level.

3.4.1 Notification of other parties. Upon notification from the energy deficient Balancing Authority that an alert has been downgraded, the Reliability Coordinator shall notify the neighboring Reliability Coordinators (via the RCIS), Balancing Authorities and Transmission Operators that its Systems can be returned to its normal limits.

Alert 0 - Termination. When the energy deficient Balancing Authority is able to meet its Load and Operating Reserve requirements, it shall request its Reliability Coordinator to terminate the EEA**.**

3.4.2 Notification. The Reliability Coordinator shall notify all other Reliability Coordinators via the RCIS of the termination. The Reliability Coordinator shall also notify the neighboring Balancing Authorities and Transmission Operators.

Appendix QC-EOP-011-2
Specific provisions applicable in Québec for standard EOP-011-2
Standard EOP-011-2 — Emergency Preparedness and Operations

This appendix establishes specific provisions for the application of the standard in Québec. Provisions of the standard and of its appendix must be read together for the purposes of understanding and interpretation. Where the standard and appendix differ, the appendix shall prevail.

A. Introduction

1. Title: No specific provisions.

2. Number: No specific provisions.

3. Purpose: No specific provisions.

4. Applicability:

4.1. Functions:

No specific provisions.

4.2. Facilities:

For the purpose of this standard, the term “generating unit” means all Main Transmission System (RTP) generators.

5. Effective Date:

5.1. Adoption of the standard by the Régie de l’énergie: March 30 , 2023

5.2. Adoption of the appendix by the Régie de l’énergie: March 30 , 2023

5.3. Effective date of the standard and its appendix in Québec: October 1, 2024

B. Requirements and Measures

No specific provisions.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

The Régie de l’énergie is responsible, in Québec, for compliance monitoring with respect to the Reliability Standard and its appendix that it adopts.

1.2. Evidence Retention

Erratum correction: In addition to the information detailed in this subsection of the Reliability Standard, the following data or evidence shall also be kept: The Generator Owner or Generator Operator shall keep data or evidence to show compliance for three years or since its last compliance audit, whichever timeframe is greater, unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation, for Requirement R8 and Measure M8.

1.3. Compliance Monitoring and Enforcement Program

The Régie de l'énergie establishes the monitoring processes used to evaluate data or information for the purpose of determining compliance or non-compliance with the Reliability Standard and with this appendix.

Erratum correction: The first sentence of this section in the Reliability Standard should be removed as it refers to data or evidence to be kept in subsection C1.2 "Evidence Retention".

Violation Severity Levels

No specific provisions.

D. Regional Differences

No specific provisions.

E. Interpretation

No specific provisions.

F. Associated Documents

No specific provisions.

Attachment 1 -EOP-011-2

No specific provisions.

Revision History

Version	Date	Action	Change Tracking
1	March 30 , 2023	New appendix as per decision D-2023-040.	New

A. Introduction

1. **Title:** **Facility Interconnection Requirements**

2. **Number:** FAC-001-4

3. **Purpose:** To avoid adverse impacts on the reliability of the Bulk Electric System, Transmission Owners and applicable Generator Owners must document and make Facility interconnection requirements available so that entities seeking to interconnect will have the necessary information.

4. **Applicability:**

   4.1. Functional Entities:

   4.1.1. Transmission Owner

   4.1.2. Applicable Generator Owner

   4.1.2.1. Generator Owner with a fully executed Agreement to conduct a study on the reliability impact of interconnecting a third party Facility to the Generator Owner's existing Facility that is used to interconnect to the Transmission system.

5. **Effective Date:** See Implementation Plan for Project 2020-05.

B. Requirements and Measures

R1. Each Transmission Owner shall document Facility interconnection requirements, update them as needed, and make them available upon request. Each Transmission Owner's Facility interconnection requirements shall address interconnection requirements for: *[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*

1.1. generation Facilities;

1.2. transmission Facilities; and

1.3. end-user Facilities.

M1. Each Transmission Owner shall have evidence (such as dated, documented Facility interconnection requirements) that it met all requirements in Requirement R1.

R2. Each applicable Generator Owner shall document Facility interconnection requirements and make them available upon request within 45 calendar days of full execution of an Agreement to conduct a study on the reliability impact of interconnecting a third party Facility to the Generator Owner's existing Facility that is used to interconnect to the Transmission system. *[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*

M2. Each applicable Generator Owner shall have evidence (such as dated, documented Facility interconnection requirements) that it met all requirements in Requirement R2.

R3. Each Transmission Owner shall address the following items in its Facility interconnection requirements: *[Violation Risk Factor: Lower] [Time Horizon: Long-Term Planning]*

3.1. Procedures for coordinated studies for new interconnections or existing interconnections seeking to make a qualified change as defined by the Planning Coordinator and their impacts on affected systems.

3.2. Procedures for notifying those responsible for the reliability of affected system(s) of new interconnections or existing interconnections seeking to make a qualified change.

3.3. Procedures for confirming with those responsible for the reliability of affected systems that new Facilities or existing Facilities seeking to make a qualified change are within a Balancing Authority Area.

M3. Each Transmission Owner shall have evidence (such as dated, documented Facility interconnection requirements addressing the procedures) that it met all requirements in Requirement R3.

R4. Each applicable Generator Owner shall address the following items in its Facility interconnection requirements: *[Violation Risk Factor: Lower] [Time Horizon: Long-Term Planning]*

4.1. Procedures for coordinated studies of new interconnections and their impacts on affected system(s).

4.2. Procedures for notifying those responsible for the reliability of affected system(s) of new interconnections.

4.3. Procedures for confirming with those responsible for the reliability of affected systems that new Facilities or existing Facilities seeking to make a qualified change as defined by the Planning Coordinator are within a Balancing Authority Area.

M4. Each applicable Generator Owner shall have evidence (such as dated, documented Facility interconnection requirements addressing the procedures) that it met all requirements in Requirement R4.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: "Compliance Enforcement Authority" means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

- The responsible entities shall retain documentation as evidence for three years.
- If a responsible entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	Long-term Planning	Lower	N/A	The Transmission Owner documented Facility interconnection requirements and updated them as needed, but failed to make them available upon request. OR The Transmission Owner documented Facility interconnection requirements and made them available upon request, but failed to update them as needed. OR The Transmission Owner documented Facility interconnection requirements,	The Transmission Owner documented Facility interconnection requirements, but failed to update them as needed and failed to make them available upon request. OR The Transmission Owner documented Facility interconnection requirements, updated them as needed, and made them available upon request, but failed to address interconnection requirements for two of the Facilities as	The Transmission Owner did not document Facility interconnection requirements.

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				updated them as needed, and made them available upon request, but failed to address interconnection requirements for one of the Facilities as specified in R1, Parts 1.1, 1.2, or 1.3.	specified in R1, Parts 1.1, 1.2, or 1.3.	
R2.	Long-term Planning	Lower	The applicable Generator Owner failed to document Facility interconnection requirements and make them available upon request until more than 45 calendar days but less than or equal to 60 calendar days after full execution of an Agreement to conduct a study on the reliability impact of interconnecting a third	The applicable Generator Owner failed to document Facility interconnection requirements and make them available upon request until more than 60 calendar days but less than or equal to 70 calendar days after full execution of an Agreement to conduct a study on the reliability impact of interconnecting a third	The applicable Generator Owner failed to document Facility interconnection requirements and make them available upon request until more than 70 calendar days but less than or equal to 80 calendar days after full execution of an Agreement to conduct a study on the reliability impact of interconnecting a third	The applicable Generator Owner failed to document Facility interconnection requirements and make them available upon request until more than 80 calendar days after full execution of an Agreement to conduct a study on the reliability impact of interconnecting a third party Facility to the Generator Owner's

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			party Facility to the Generator Owner's existing Facility that is used to interconnect to the Transmission system.	party Facility to the Generator Owner's existing Facility that is used to interconnect to the Transmission system.	party Facility to the Generator Owner's existing Facility that is used to interconnect to the Transmission system.	existing Facility that is used to interconnect to the Transmission system.
R3.	Long-term Planning	Lower	N/A	The Transmission Owner failed to address one part of Requirement R3 (Part 3.1 through Part 3.3).	The Transmission Owner failed to address two parts of Requirement R3 (Part 3.1 through Part 3.3).	The Transmission Owner failed to address three parts of Requirement R3 (Part 3.1 through Part 3.3).
R4.	Long-term Planning	Lower	N/A	The Generator Owner failed to address one part of Requirement R4 (Part 4.1 through Part 4.3).	The Generator Owner failed to address two parts of Requirement R4 (Part 4.1 through Part 4.3).	The Generator Owner failed to address three parts of Requirement R4 (Part 4.1 through Part 4.3).

D. Regional Variances

None.

E. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
0	April 1, 2005	Effective Date	New
1		Added requirements for Generator Owner and brought overall standard format up to date.	Revision under Project 2010-07
1	February 9, 2012	Adopted by the Board of Trustees	
1	September 19, 2013	A FERC order was issued on September 19, 2013, approving FAC-001-1. This standard became enforceable on November 25, 2013 for Transmission Owners. For Generator Owners, the standard becomes enforceable on January 1, 2015.	
2		Revisions to implement the recommendations of the FAC Five-Year Review Team.	Revision under Project 2010-02
2	August 14, 2014	Adopted by the Board of Trustees	
2	November 6, 2014	FERC letter order issued approving FAC-001-2.	
3	February 11, 2016	Adopted by the Board of Trustees	Moved BAL-005-0.2b Requirement R1 into FAC-001-3 Requirements R3 and R4
3	September 20, 2017	FERC Order No. 836 issued approving FAC-001-3	
3	February 19, 2021	FERC letter Order issued approving FAC-001-3 Errata	
4	May 12, 2022	Adopted by the Board of Trustees	Revisions under Project 2020-05
4	November 17,2022	FERC Order RD22-5-000 issued approving FAC-001-4	
4	December 2, 2022	Effective Date	1/1/2024

Appendix FAC-001-4-QC-1
Specific provisions applicable in Québec for standard FAC-001-4 — Facility Interconnection Requirements

This appendix establishes specific provisions for the application of the standard in Québec. Provisions of the standard and of this appendix must be read jointly for comprehension and interpretation purposes. Where the standard and appendix differ, the appendix shall prevail.

A. Introduction

1. Title: No specific provision.

2. Number: No specific provision.

3. Purpose: No specific provision.

4. Applicability:

4.1. Functional Entities

No specific provision.

5. Effective Date:

5.1. Adoption of the standard by the Régie: September 14, 2023

5.2. Adoption of the appendix by the Régie: September 14, 2023

5.3. Effective date of the standard and its appendix in Québec: October 1, 2024

Requirements	Applicability	Date of implementation in Québec
R1 and R2		October 1, 2024
R3 and R4	To the extent a change is considered a "qualified change" under the definition developed by the PC under FAC-002-4 Requirement R6 but was not considered a "material modification" under FAC-001-3 or FAC-002-3.	October 1, 2025

B. Requirements and Measures

No specific provision.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

In Québec, "Compliance Enforcement Authority" means the Régie de l'énergie in its roles of monitoring and enforcing compliance with respect to the Reliability Standard and to this appendix.

1.2. Evidence Retention

No specific provision.

1.3. Compliance Monitoring and Enforcement Program

The Régie de l'énergie establishes the monitoring processes used to evaluate data or information for the purpose of determining compliance or non-compliance with the Reliability Standard and with this appendix.

Violation Severity Levels

No specific provision.

D. Regional Variances

No specific provision.

E. Associated Documents

No specific provision.

Version history

Version	Date	Action	Change Tracking
1	September 14, 2023	New appendix as per decision D-2023-107.	New

A. Introduction

1. **Title:** **Facility Interconnection Studies**

2. **Number:** FAC-002-4

3. **Purpose:** To study the impact of interconnecting new or changed Facilities on the Bulk Electric System.

4. **Applicability:**

   4.1. Functional Entities:

   4.1.1. Planning Coordinator

   4.1.2. Transmission Planner

   4.1.3. Transmission Owner

   4.1.4. Distribution Provider

   4.1.5. Generator Owner

   4.1.6. Applicable Generator Owner

   4.1.6.1. Generator Owner with a fully executed Agreement to conduct a study on the reliability impact of interconnecting a third party Facility to the Generator Owner's existing Facility that is used to interconnect to the Transmission system.

5. **Effective Date:** See Implementation Plan for Project 2020-05.

B. Requirements and Measures

R1. Each Transmission Planner and each Planning Coordinator shall study the reliability impact of: (i) interconnecting new generation, transmission, or electricity end-user Facilities and (ii) existing interconnections of generation, transmission, or electricity end-user Facilities seeking to make a qualified change as defined by the Planning Coordinator under Requirement R6. The following shall be studied: *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

1.1. The reliability impact of the new interconnection, or existing interconnection seeking to make a qualified change as defined by the Planning Coordinator under Requirement R6, on affected system(s);

1.2. Adherence to applicable NERC Reliability Standards; regional and Transmission Owner planning criteria; and Facility interconnection requirements;

1.3. Steady-state, short-circuit, and dynamics studies, as necessary, to evaluate system performance under both normal and contingency conditions; and

1.4. Study assumptions, system performance, alternatives considered, and coordinated recommendations. While these studies may be performed independently, the results shall be evaluated and coordinated by the entities involved.

M1. Each Transmission Planner or each Planning Coordinator shall have evidence (such as study reports, including documentation of reliability issues) that it met all requirements in Requirement R1.

R2. Each Generator Owner seeking to interconnect new generation Facilities, or existing interconnections of generation Facilities seeking to make a qualified change as defined by the Planning Coordinator under Requirement R6, shall coordinate and cooperate on studies with its Transmission Planner or Planning Coordinator, including but not limited to the provision of data as described in R1, Parts 1.1-1.4. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

M2. Each Generator Owner shall have evidence (such as documents containing the data provided in response to the requests of the Transmission Planner or Planning Coordinator) that it met all requirements in Requirement R2.

R3. Each Transmission Owner and each Distribution Provider seeking to interconnect new transmission Facilities or electricity end-user Facilities, or existing interconnections of transmission Facilities or electricity end-user Facilities seeking to make a qualified change as defined by the Planning Coordinator under Requirement R6, shall coordinate and cooperate on studies with its Transmission Planner or Planning Coordinator, including but not limited to the provision of data as described in R1, Parts 1.1-1.4. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

M3. Each Transmission Owner and each Distribution Provider shall have evidence (such as documents containing the data provided in response to the requests of the

Transmission Planner or Planning Coordinator) that it met all requirements in Requirement R3.

R4. Each Transmission Owner shall coordinate and cooperate with its Transmission Planner or Planning Coordinator on studies regarding requested new or existing interconnections seeking to make a qualified change as defined by the Planning Coordinator under Requirement R6, to its Facilities, including but not limited to the provision of data as described in R1, Parts 1.1-1.4. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

M4. Each Transmission Owner shall have evidence (such as documents containing the data provided in response to the requests of the Transmission Planner or Planning Coordinator) that it met all requirements in Requirement R4.

R5. Each applicable Generator Owner shall coordinate and cooperate with its Transmission Planner or Planning Coordinator on studies regarding requested interconnections to its Facilities, including but not limited to the provision of data as described in R1, Parts 1.1-1.4. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

M5. Each applicable Generator Owner shall have evidence (such as documents containing the data provided in response to the requests of the Transmission Planner or Planning Coordinator) that it met all requirements in Requirement R5.

R6. Each Planning Coordinator shall maintain a publicly available definition of qualified change for the purposes of facility interconnection. *[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*

M6. Each Planning Coordinator shall have evidence that it has maintained a publicly available definition of qualified change.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: "Compliance Enforcement Authority" means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

The Planning Coordinator, Transmission Planner, Transmission Owner, Distribution Provider, Generator Owner and applicable Generator Owner shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

The responsible entities shall retain documentation as evidence for three years.

If a responsible entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.

The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	Long-term Planning	Medium	The Transmission Planner or Planning Coordinator studied the reliability impact of: (i) interconnecting new generation, transmission, or electricity end-user Facilities, and (ii) existing interconnections of generation, transmission, or electricity end-user Facilities seeking to make a qualified change as defined by the Planning Coordinator under Requirement R6, but failed to study one of the Parts (R1, 1.1-1.4).	The Transmission Planner or Planning Coordinator studied the reliability impact of: (i) interconnecting new generation, transmission, or electricity end-user Facilities, and (ii) existing interconnections of generation, transmission, or electricity end-user Facilities seeking to make a qualified change as defined by the Planning Coordinator under Requirement R6, but failed to study two of the Parts (R1, 1.1-1.4).	The Transmission Planner or Planning Coordinator studied the reliability impact of: (i) interconnecting new generation, transmission, or electricity end-user Facilities, and (ii) existing interconnections of generation, transmission, or electricity end-user Facilities seeking to make a qualified change as defined by the Planning Coordinator under Requirement R6, but failed to study three of the Parts (R1, 1.1-1.4).	The Transmission Planner or Planning Coordinator failed to study the reliability impact of: interconnecting new generation, transmission, or electricity end-user Facilities, and (ii) existing interconnections of, generation, transmission, or electricity end-user Facilities seeking to make a qualified change as defined by the Planning Coordinator under Requirement R6.
R2.	Long-term Planning	Medium	The Generator Owner seeking to interconnect new generation Facilities,	The Generator Owner seeking to interconnect new generation Facilities,	The Generator Owner seeking to interconnect new generation Facilities,	The Generator Owner seeking to interconnect new generation Facilities,

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			or existing interconnections of generation Facilities seeking to make a qualified change as defined by the Planning Coordinator under Requirement R6, coordinated and cooperated on studies with its Transmission Planner or Planning Coordinator, but failed to provide data necessary to perform studies as described in one of the Parts (R1, 1.1-1.4).	or existing interconnections of generation Facilities seeking to make a qualified change as defined by the Planning Coordinator under Requirement R6, coordinated and cooperated on studies with its Transmission Planner or Planning Coordinator, but failed to provide data necessary to perform studies as described in two of the Parts (R1, 1.1-1.4).	or existing interconnections of generation Facilities seeking to make a qualified change as defined by the Planning Coordinator under Requirement R6, coordinated and cooperated on studies with its Transmission Planner or Planning Coordinator, but failed to provide data necessary to perform studies as described in three of the Parts (R1, 1.1-1.4).	or existing interconnections of generation Facilities seeking to make a qualified change as defined by the Planning Coordinator under Requirement R6, failed to coordinate and cooperate on studies with its Transmission Planner or Planning Coordinator.
R3.	Long-term Planning	Medium	The Transmission Owner or Distribution Provider seeking to interconnect new transmission Facilities or electricity end-user Facilities, or existing interconnections of transmission Facilities	The Transmission Owner, or Distribution Provider seeking to interconnect new transmission Facilities or electricity end-user Facilities, or existing interconnections of transmission Facilities	The Transmission Owner or Distribution Provider seeking to interconnect new transmission Facilities or electricity end-user Facilities, or existing interconnections of transmission Facilities	The Transmission Owner, or Distribution Provider seeking to interconnect new transmission Facilities or electricity end-user Facilities, or existing interconnections of transmission Facilities

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			seeking to make a qualified change as defined by the Planning Coordinator under Requirement R6, or electricity end-user Facilities, coordinated and cooperated on studies with its Transmission Planner or Planning Coordinator, but failed to provide data necessary to perform studies as described in one of the Parts (R1, 1.1-1.4).	seeking to make a qualified change as defined by the Planning Coordinator under Requirement R6, or electricity end-user Facilities, coordinated and cooperated on studies with its Transmission Planner or Planning Coordinator, but failed to provide data necessary to perform studies as described in two of the Parts (R1, 1.1-1.4).	seeking to make a qualified change as defined by the Planning Coordinator under Requirement R6, or electricity end-user Facilities, coordinated and cooperated on studies with its Transmission Planner or Planning Coordinator, but failed to provide data necessary to perform studies as described in three of the Parts (R1, 1.1-1.4).	seeking to make a qualified change as defined by the Planning Coordinator under Requirement R6, or electricity end-user Facilities, failed to coordinate and cooperate on studies with its Transmission Planner or Planning Coordinator.
R4.	Long-term Planning	Medium	The Transmission Owner coordinated and cooperated on studies with its Transmission Planner or Planning Coordinator regarding requested new or existing interconnections	The Transmission Owner coordinated and cooperated on studies with its Transmission Planner or Planning Coordinator regarding requested new or existing interconnections	The Transmission Owner coordinated and cooperated on studies with its Transmission Planner or Planning Coordinator regarding requested new or existing interconnections	The Transmission Owner failed to coordinate and cooperate on studies with its Transmission Planner or Planning Coordinator regarding requested new or existing interconnections

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			seeking to make a qualified change as defined by the Planning Coordinator under Requirement R6to its Facilities, but failed to provide data necessary to perform studies as described in one of the Parts (R1, 1.1-1.4).	seeking to make a qualified change as defined by the Planning Coordinator under Requirement R6to its Facilities, but failed to provide data necessary to perform studies as described in two of the Parts (R1, 1.1-1.4).	seeking to make a qualified change as defined by the Planning Coordinator under Requirement R6to its Facilities, but failed to provide data necessary to perform studies as described in three of the Parts (R1, 1.1-1.4).	seeking to make a qualified change as defined by the Planning Coordinator under Requirement R6to its Facilities.
R5.	Long-term Planning	Medium	The applicable Generator Owner coordinated and cooperated on studies with its Transmission Planner or Planning Coordinator regarding requested interconnections to its Facilities, but failed to provide data necessary to perform studies as described in one of the Parts (R1, 1.1-1.4).	The applicable Generator Owner coordinated and cooperated on studies with its Transmission Planner or Planning Coordinator regarding requested interconnections to its Facilities, but failed to provide data necessary to perform studies as described in two of the Parts (R1, 1.1-1.4).	The applicable Generator Owner coordinated and cooperated on studies with its Transmission Planner or Planning Coordinator regarding requested interconnections to its Facilities, but failed to provide data necessary to perform studies as described in three of the Parts (R1, 1.1-1.4).	The applicable Generator Owner failed to coordinate and cooperate on studies with its Transmission Planner or Planning Coordinator regarding requested interconnections to its Facilities.

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R6.	Long-term Planning	Lower	N/A	N/A	N/A	The Planning Coordinator did not maintain a publicly available definition of qualified change for the purposes of facility interconnection.

D. Regional Variances

None.

E. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
0	April 1, 2005	Effective Date	New
0	January 13, 2006	Removed duplication of "Regional Reliability Organizations(s).	Errata
1	August 5, 2010	Modified to address Order No. 693 Directives contained in paragraph 693. Adopted by the NERC Board of Trustees.	Revised
1	February 7, 2013	R2 and associated elements approved by NERC Board of Trustees for retirement as part of the Paragraph 81 project (Project 2013-02) pending applicable regulatory approval.	
1	November 21, 2013	R2 and associated elements approved by FERC for retirement as part of the Paragraph 81 project (Project 2013-02)	
2		Revisions to implement the recommendations of the FAC Five-Year Review Team.	Revision under Project 2010-02
2	August 14, 2014	Adopted by the Board of Trustees.	
2	November 6, 2014	FERC letter order issued approving FAC-002-2.	
3	February 6, 2020	Adopted by NERC Board of Trustees.	Revisions under Project 2017-07
4	May 12, 2022	Adopted by NERC Board of Trustees.	Revisions under Project 2020-05
4	November 17,2022	FERC Order RD22-5-000 issued approving FAC-002-4	
4	December 2, 2022	Effective Date	1/1/2024

Appendix FAC-002-4-QC-1
Specific provisions applicable in Québec for standard FAC-002-4 — Facility Interconnection Studies

This appendix establishes specific provisions for the application of the standard in Québec. Provisions of the standard and of this appendix must be read jointly for comprehension and interpretation purposes. Where the standard and appendix differ, the appendix shall prevail.

A. Introduction

1. Title: No specific provision.

2. Number: No specific provision.

3. Purpose: No specific provision.

4. Applicability:

4.1. Functional Entities

No specific provision.

Facilities

For the purposes of the standard, Transmission facilities, Generation facilities and End-user facilities are defined as follow:

Transmission facilities:

- Transmission System operated at 44 kV or above ;
- Any lines from the Transmission System operated at 44 kV or above ;
- Transmission facility operated at 44 kV and above, connected to the Main Transmission System (RTP).

Generation facilities:

- Any generation facility with an installed capacity of 50 MVA or greater ;
- Any generation facility connected to the Main Transmission System (RTP).

End-user facilities:

- Addition of a line feeder at 25 kV in a Distribution substation ;
- New connection of an Industrial Customer operated at 44 kV and above, connected to the Main Transmission System (RTP).

5. Effective Date:

5.1. Adoption of the standard by the Régie de l'énergie: September 14, 2023

5.2. Adoption of the appendix by the Régie de l'énergie: September 14, 2023

5.3. Effective date of the standard and of its appendix in Québec: October 1, 2024

Requirements	Applicability	Date of implementation in Québec
R5 and R6		October 1, 2024

Requirements	Applicability	Date of implementation in Québec
R1 to R4	To the extent a change is considered a "qualified change" under the definition developed by the PC under FAC-002-4 Requirement R6 but was not considered a "material modification" under FAC-001-3 or FAC-002-3.	October 1, 2025

B. Requirements and Measures

No specific provision.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

In Québec, "Compliance Enforcement Authority" means the Régie de l'énergie in its role of monitoring and enforcing compliance with respect to the Reliability Standard and to this appendix.

1.2. Evidence Retention

No specific provision.

1.3. Compliance Monitoring and Enforcement Program

The Régie de l'énergie establishes the monitoring processes used to evaluate data or information for the purpose of determining compliance or non-compliance with the Reliability Standard and with this appendix.

Violation Severity Levels

No specific provision.

D. Regional Variances

No specific provision.

E. Associated Documents

No specific provision.

Version History

Version	Date	Action	Change Tracking
1	September 14, 2023	New appendix as per decision D-2023-107.	New

A. Introduction

1. **Title:** **Transmission Vegetation Management**

2. **Number:** **FAC-003-4**

3. **Purpose:** **To maintain a reliable electric transmission system by using a defense-in-depth strategy to manage vegetation located on transmission rights of way (ROW) and minimize encroachments from vegetation located adjacent to the ROW, thus preventing the risk of those vegetation-related outages that could lead to Cascading.**

4. **Applicability:**

   4.1. Functional Entities:

   4.1.1. Applicable Transmission Owners

   4.1.1.1. Transmission Owners that own Transmission Facilities defined in 4.2.

   4.1.2. Applicable Generator Owners

   4.1.2.1. Generator Owners that own generation Facilities defined in 4.3.

   4.2. Transmission Facilities: Defined below (referred to as "applicable lines"), including but not limited to those that cross lands owned by federal[1], state, provincial, public, private, or tribal entities:

   4.2.1. Each overhead transmission line operated at 200kV or higher.

   4.2.2. Each overhead transmission line operated below 200kV identified as an element of an IROL under NERC Standard FAC-014 by the Planning Coordinator.

   4.2.3. Each overhead transmission line operated below 200 kV identified as an element of a Major WECC Transfer Path in the Bulk Electric System by WECC.

   4.2.4. Each overhead transmission line identified above (4.2.1. through 4.2.3.) located outside the fenced area of the switchyard, station or substation and any portion of the span of the transmission line that is crossing the substation fence.

   4.3. Generation Facilities: Defined below (referred to as "applicable lines"), including but not limited to those that cross lands owned by federal[2], state, provincial, public, private, or tribal entities:

[1] EPAct 2005 section 1211c: *"Access approvals by Federal agencies."*

[2] *Id.*

4.3.1. Overhead transmission lines that (1) extend greater than one mile or 1.609 kilometers beyond the fenced area of the generating station switchyard to the point of interconnection with a Transmission Owner's Facility or (2) do not have a clear line of sight[3] from the generating station switchyard fence to the point of interconnection with a Transmission Owner's Facility and are:

4.3.1.1. Operated at 200kV or higher; or

4.3.1.2. Operated below 200kV identified as an element of an IROL under NERC Standard FAC-014 by the Planning Coordinator; or

4.3.1.3. Operated below 200 kV identified as an element of a Major WECC Transfer Path in the Bulk Electric System by WECC.

5. Effective Date: See Implementation Plan

6. Background: This standard uses three types of requirements to provide layers of protection to prevent vegetation related outages that could lead to Cascading:

a) Performance-based defines a particular reliability objective or outcome to be achieved. In its simplest form, a results-based requirement has four components: *who, under what conditions (if any), shall perform what action, to achieve what particular bulk power system performance result or outcome?*

b) Risk-based preventive requirements to reduce the risks of failure to acceptable tolerance levels. A risk-based reliability requirement should be framed as: *who, under what conditions (if any), shall perform what action, to achieve what particular result or outcome that reduces a stated risk to the reliability of the bulk power system?*

c) Competency-based defines a minimum set of capabilities an entity needs to have to demonstrate it is able to perform its designated reliability functions. A competency-based reliability requirement should be framed as: *who, under what conditions (if any), shall have what capability, to achieve what particular result or outcome to perform an action to achieve a result or outcome or to reduce a risk to the reliability of the bulk power system?*

The defense-in-depth strategy for reliability standards development recognizes that each requirement in a NERC reliability standard has a role in preventing system failures, and that these roles are complementary and reinforcing. Reliability standards should not be viewed as a body of unrelated requirements, but rather should be viewed as part of a portfolio of requirements designed to achieve an overall defense-in-depth strategy and comport with the quality objectives of a reliability standard.

[3] "Clear line of sight" means the distance that can be seen by the average person without special instrumentation (e.g., binoculars, telescope, spyglasses, etc.) on a clear day.

This standard uses a defense-in-depth approach to improve the reliability of the electric Transmission system by:

- Requiring that vegetation be managed to prevent vegetation encroachment inside the flash-over clearance (R1 and R2);
- Requiring documentation of the maintenance strategies, procedures, processes and specifications used to manage vegetation to prevent potential flash-over conditions including consideration of 1) conductor dynamics and 2) the interrelationships between vegetation growth rates, control methods and the inspection frequency (R3);
- Requiring timely notification to the appropriate control center of vegetation conditions that could cause a flash-over at any moment (R4);
- Requiring corrective actions to ensure that flash-over distances will not be violated due to work constrains such as legal injunctions (R5);
- Requiring inspections of vegetation conditions to be performed annually (R6); and
- Requiring that the annual work needed to prevent flash-over is completed (R7).

For this standard, the requirements have been developed as follows:

- Performance-based: Requirements 1 and 2
- Competency-based: Requirement 3
- Risk-based: Requirements 4, 5, 6 and 7

R3 serves as the first line of defense by ensuring that entities understand the problem they are trying to manage and have fully developed strategies and plans to manage the problem. R1, R2, and R7 serve as the second line of defense by requiring that entities carry out their plans and manage vegetation. R6, which requires inspections, may be either a part of the first line of defense (as input into the strategies and plans) or as a third line of defense (as a check of the first and second lines of defense). R4 serves as the final line of defense, as it addresses cases in which all the other lines of defense have failed.

Major outages and operational problems have resulted from interference between overgrown vegetation and transmission lines located on many types of lands and ownership situations. Adherence to the standard requirements for applicable lines on any kind of land or easement, whether they are Federal Lands, state or provincial lands, public or private lands, franchises, easements or lands owned in fee, will reduce and manage this risk. For the purpose of the standard the term “public lands” includes municipal lands, village lands, city lands, and a host of other governmental entities.

This standard addresses vegetation management along applicable overhead lines and does not apply to underground lines, submarine lines or to line sections inside an electric station boundary.

This standard focuses on transmission lines to prevent those vegetation related outages that could lead to Cascading. It is not intended to prevent customer outages due to tree contact with lower voltage distribution system lines. For example, localized customer service might be disrupted if vegetation were to make contact with a 69kV transmission line supplying power to a 12kV distribution station. However, this standard is not written to address such isolated situations which have little impact on the overall electric transmission system.

Since vegetation growth is constant and always present, unmanaged vegetation poses an increased outage risk, especially when numerous transmission lines are operating at or near their Rating. This can present a significant risk of consecutive line failures when lines are experiencing large sags thereby leading to Cascading. Once the first line fails the shift of the current to the other lines and/or the increasing system loads will lead to the second and subsequent line failures as contact to the vegetation under those lines occurs. Conversely, most other outage causes (such as trees falling into lines, lightning, animals, motor vehicles, etc.) are not an interrelated function of the shift of currents or the increasing system loading. These events are not any more likely to occur during heavy system loads than any other time. There is no cause-effect relationship which creates the probability of simultaneous occurrence of other such events. Therefore these types of events are highly unlikely to cause large-scale grid failures. Thus, this standard places the highest priority on the management of vegetation to prevent vegetation grow-ins.

B. Requirements and Measures

R1. Each applicable Transmission Owner and applicable Generator Owner shall manage vegetation to prevent encroachments into the Minimum Vegetation Clearance Distance (MVCD) of its applicable line(s) which are either an element of an IROL, or an element of a Major WECC Transfer Path; operating within their Rating and all Rated Electrical Operating Conditions of the types shown below[4] *[Violation Risk Factor: High] [Time Horizon: Real-time]*:

[4] This requirement does not apply to circumstances that are beyond the control of an applicable Transmission Owner or applicable Generator Owner subject to this reliability standard, including natural disasters such as earthquakes, fires, tornados, hurricanes, landslides, wind shear, fresh gale, major storms as defined either by the applicable Transmission Owner or applicable Generator Owner or an applicable regulatory body, ice storms, and floods; human or animal activity such as logging, animal severing tree, vehicle contact with tree, or installation, removal, or digging of vegetation. Nothing in this footnote should be construed to limit the Transmission Owner's or applicable Generator Owner's right to exercise its full legal rights on the ROW.

1.1. An encroachment into the MVCD as shown in FAC-003-Table 2, observed in Real-time, absent a Sustained Outage,[5]

1.2. An encroachment due to a fall-in from inside the ROW that caused a vegetation-related Sustained Outage,[6]

1.3. An encroachment due to the blowing together of applicable lines and vegetation located inside the ROW that caused a vegetation-related Sustained Outage[7],

1.4. An encroachment due to vegetation growth into the MVCD that caused a vegetation-related Sustained Outage.[8]

M1. Each applicable Transmission Owner and applicable Generator Owner has evidence that it managed vegetation to prevent encroachment into the MVCD as described in R1. Examples of acceptable forms of evidence may include dated attestations, dated reports containing no Sustained Outages associated with encroachment types 2 through 4 above, or records confirming no Real-time observations of any MVCD encroachments. (R1)

R2. Each applicable Transmission Owner and applicable Generator Owner shall manage vegetation to prevent encroachments into the MVCD of its applicable line(s) which are not either an element of an IROL, or an element of a Major WECC Transfer Path; operating within its Rating and all Rated Electrical Operating Conditions of the types shown below[9] *[Violation Risk Factor: High] [Time Horizon: Real-time]*:

2.1. An encroachment into the MVCD, observed in Real-time, absent a Sustained Outage,[10]

2.2. An encroachment due to a fall-in from inside the ROW that caused a vegetation-related Sustained Outage,[11]

2.3. An encroachment due to the blowing together of applicable lines and vegetation located inside the ROW that caused a vegetation-related Sustained Outage,[12]

2.4. An encroachment due to vegetation growth into the line MVCD that caused a vegetation-related Sustained Outage.[13]

---

[5] If a later confirmation of a Fault by the applicable Transmission Owner or applicable Generator Owner shows that a vegetation encroachment within the MVCD has occurred from vegetation within the ROW, this shall be considered the equivalent of a Real-time observation.

[6] Multiple Sustained Outages on an individual line, if caused by the same vegetation, will be reported as one outage regardless of the actual number of outages within a 24-hour period.

[7] *Id.*

[8] *Id.*

[9] See footnote 4.

[10] See footnote 5.

[11] See footnote 6.

[12] *Id.*

[13] *Id.*

M2. Each applicable Transmission Owner and applicable Generator Owner has evidence that it managed vegetation to prevent encroachment into the MVCD as described in R2. Examples of acceptable forms of evidence may include dated attestations, dated reports containing no Sustained Outages associated with encroachment types 2 through 4 above, or records confirming no Real-time observations of any MVCD encroachments. (R2)

R3. Each applicable Transmission Owner and applicable Generator Owner shall have documented maintenance strategies or procedures or processes or specifications it uses to prevent the encroachment of vegetation into the MVCD of its applicable lines that accounts for the following: *[Violation Risk Factor: Lower] [Time Horizon: Long Term Planning]:*

3.1. Movement of applicable line conductors under their Rating and all Rated Electrical Operating Conditions;

3.2. Inter-relationships between vegetation growth rates, vegetation control methods, and inspection frequency.

M3. The maintenance strategies or procedures or processes or specifications provided demonstrate that the applicable Transmission Owner and applicable Generator Owner can prevent encroachment into the MVCD considering the factors identified in the requirement. (R3)

R4. Each applicable Transmission Owner and applicable Generator Owner, without any intentional time delay, shall notify the control center holding switching authority for the associated applicable line when the applicable Transmission Owner and applicable Generator Owner has confirmed the existence of a vegetation condition that is likely to cause a Fault at any moment *[Violation Risk Factor: Medium] [Time Horizon: Real-time].*

M4. Each applicable Transmission Owner and applicable Generator Owner that has a confirmed vegetation condition likely to cause a Fault at any moment will have evidence that it notified the control center holding switching authority for the associated transmission line without any intentional time delay. Examples of evidence may include control center logs, voice recordings, switching orders, clearance orders and subsequent work orders. (R4)

R5. When an applicable Transmission Owner and an applicable Generator Owner are constrained from performing vegetation work on an applicable line operating within its Rating and all Rated Electrical Operating Conditions, and the constraint may lead to a vegetation encroachment into the MVCD prior to the implementation of the next annual work plan, then the applicable Transmission Owner or applicable Generator Owner shall take corrective action to ensure continued vegetation management to prevent encroachments [*Violation Risk Factor: Medium*] [*Time Horizon: Operations Planning*].

M5. Each applicable Transmission Owner and applicable Generator Owner has evidence of the corrective action taken for each constraint where an applicable transmission line was put at potential risk. Examples of acceptable forms of evidence may include initially-planned work orders, documentation of constraints from landowners, court orders, inspection records of increased monitoring, documentation of the de-rating of lines, revised work orders, invoices, or evidence that the line was de-energized. (R5)

R6. Each applicable Transmission Owner and applicable Generator Owner shall perform a Vegetation Inspection of 100% of its applicable transmission lines (measured in units of choice - circuit, pole line, line miles or kilometers, etc.) at least once per calendar year and with no more than 18 calendar months between inspections on the same ROW[14] [*Violation Risk Factor: Medium*] [*Time Horizon: Operations Planning*].

M6. Each applicable Transmission Owner and applicable Generator Owner has evidence that it conducted Vegetation Inspections of the transmission line ROW for all applicable lines at least once per calendar year but with no more than 18 calendar months between inspections on the same ROW. Examples of acceptable forms of evidence may include completed and dated work orders, dated invoices, or dated inspection records. (R6)

R7. Each applicable Transmission Owner and applicable Generator Owner shall complete 100% of its annual vegetation work plan of applicable lines to ensure no vegetation encroachments occur within the MVCD. Modifications to the work plan in response to changing conditions or to findings from vegetation inspections may be made (provided they do not allow encroachment of vegetation into the MVCD) and must be documented. The percent completed calculation is based on the number of units actually completed divided by the number of units in the final amended plan (measured in units of choice - circuit, pole line, line miles or kilometers, etc.). Examples of reasons for modification to annual plan may include [*Violation Risk Factor: Medium*] [*Time Horizon: Operations Planning*]:

7.1. Change in expected growth rate/environmental factors

7.2. Circumstances that are beyond the control of an applicable Transmission Owner or applicable Generator Owner[15]

7.3. Rescheduling work between growing seasons

7.4. Crew or contractor availability/Mutual assistance agreements

[14] When the applicable Transmission Owner or applicable Generator Owner is prevented from performing a Vegetation Inspection within the timeframe in R6 due to a natural disaster, the TO or GO is granted a time extension that is equivalent to the duration of the time the TO or GO was prevented from performing the Vegetation Inspection.

[15] Circumstances that are beyond the control of an applicable Transmission Owner or applicable Generator Owner include but are not limited to natural disasters such as earthquakes, fires, tornados, hurricanes, landslides, ice storms, floods, or major storms as defined either by the TO or GO or an applicable regulatory body.

7.5. Identified unanticipated high priority work

7.6. Weather conditions/Accessibility

7.7. Permitting delays

7.8. Land ownership changes/Change in land use by the landowner

7.9. Emerging technologies

M7. Each applicable Transmission Owner and applicable Generator Owner has evidence that it completed its annual vegetation work plan for its applicable lines. Examples of acceptable forms of evidence may include a copy of the completed annual work plan (as finally modified), dated work orders, dated invoices, or dated inspection records. (R7)

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority:
"Compliance Enforcement Authority" means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention:
The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

- The applicable Transmission Owner and applicable Generator Owner retains data or evidence to show compliance with Requirements R1, R2, R3, R5, R6 and R7, for three calendar years.
- The applicable Transmission Owner and applicable Generator Owner retains data or evidence to show compliance with Requirement R4, Measure M4 for most recent 12 months of operator logs or most recent 3 months of voice recordings or transcripts of voice recordings, unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

- If an applicable Transmission Owner or applicable Generator Owner is found non-compliant, it shall keep information related to the non-compliance until found compliant or for the time period specified above, whichever is longer.

1.3. Compliance Monitoring and Enforcement Program

As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

1.4. Additional Compliance Information

Periodic Data Submittal: The applicable Transmission Owner and applicable Generator Owner will submit a quarterly report to its Regional Entity, or the Regional Entity's designee, identifying all Sustained Outages of applicable lines operated within their Rating and all Rated Electrical Operating Conditions as determined by the applicable Transmission Owner or applicable Generator Owner to have been caused by vegetation, except as excluded in footnote 2, and including as a minimum the following:

- The name of the circuit(s), the date, time and duration of the outage; the voltage of the circuit; a description of the cause of the outage; the category associated with the Sustained Outage; other pertinent comments; and any countermeasures taken by the applicable Transmission Owner or applicable Generator Owner.

  A Sustained Outage is to be categorized as one of the following:

- Category 1A — Grow-ins: Sustained Outages caused by vegetation growing into applicable lines, that are identified as an element of an IROL or Major WECC Transfer Path, by vegetation inside and/or outside of the ROW;
- Category 1B — Grow-ins: Sustained Outages caused by vegetation growing into applicable lines, but are not identified as an element of an IROL or Major WECC Transfer Path, by vegetation inside and/or outside of the ROW;
- Category 2A — Fall-ins: Sustained Outages caused by vegetation falling into applicable lines that are identified as an element of an IROL or Major WECC Transfer Path, from within the ROW;
- Category 2B — Fall-ins: Sustained Outages caused by vegetation falling into applicable lines, but are not identified as an element of an IROL or Major WECC Transfer Path, from within the ROW;
- Category 3 — Fall-ins: Sustained Outages caused by vegetation falling into applicable lines from outside the ROW;
- Category 4A — Blowing together: Sustained Outages caused by vegetation and applicable lines that are identified as an element of an IROL or Major WECC Transfer Path, blowing together from within the ROW;

- Category 4B — Blowing together: Sustained Outages caused by vegetation and applicable lines, but are not identified as an element of an IROL or Major WECC Transfer Path, blowing together from within the ROW.

  The Regional Entity will report the outage information provided by applicable Transmission Owners and applicable Generator Owners, as per the above, quarterly to NERC, as well as any actions taken by the Regional Entity as a result of any of the reported Sustained Outages.

Violation Severity Levels (Table 1)

R #	Table 1: Violation Severity Levels (VSL)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.			The responsible entity failed to manage vegetation to prevent encroachment into the MVCD of a line identified as an element of an IROL or Major WECC transfer path and encroachment into the MVCD as identified in FAC-003-4-Table 2 was observed in real time absent a Sustained Outage.	The responsible entity failed to manage vegetation to prevent encroachment into the MVCD of a line identified as an element of an IROL or Major WECC transfer path and a vegetation-related Sustained Outage was caused by one of the following: • *A fall-in from inside the active transmission line ROW* • *Blowing together of applicable lines and vegetation located inside the active transmission line ROW* • *A grow-in*
R2.			The responsible entity failed to manage vegetation to prevent encroachment into the MVCD of a line not identified as an element of	The responsible entity failed to manage vegetation to prevent encroachment into the MVCD of a line not identified as an element of

			an IROL or Major WECC transfer path and encroachment into the MVCD as identified in FAC-003-4-Table 2 was observed in real time absent a Sustained Outage.	an IROL or Major WECC transfer path and a vegetation-related Sustained Outage was caused by one of the following: • *A fall-in from inside the active transmission line ROW* • *Blowing together of applicable lines and vegetation located inside the active transmission line ROW* • *A grow-in*
R3.		The responsible entity has maintenance strategies or documented procedures or processes or specifications but has not accounted for the inter-relationships between vegetation growth rates, vegetation control methods, and inspection frequency, for the responsible entity's applicable lines. (Requirement R3, Part 3.2.)	The responsible entity has maintenance strategies or documented procedures or processes or specifications but has not accounted for the movement of transmission line conductors under their Rating and all Rated Electrical Operating Conditions, for the responsible entity's applicable lines. (Requirement R3, Part 3.1.)	The responsible entity does not have any maintenance strategies or documented procedures or processes or specifications used to prevent the encroachment of vegetation into the MVCD, for the responsible entity's applicable lines.
R4.			The responsible entity experienced a confirmed	The responsible entity experienced a confirmed

			vegetation threat and notified the control center holding switching authority for that applicable line, but there was intentional delay in that notification.	vegetation threat and did not notify the control center holding switching authority for that applicable line.
R5.				The responsible entity did not take corrective action when it was constrained from performing planned vegetation work where an applicable line was put at potential risk.
R6.	The responsible entity failed to inspect 5% or less of its applicable lines (measured in units of choice - circuit, pole line, line miles or kilometers, etc.)	The responsible entity failed to inspect more than 5% up to and including 10% of its applicable lines (measured in units of choice - circuit, pole line, line miles or kilometers, etc.).	The responsible entity failed to inspect more than 10% up to and including 15% of its applicable lines (measured in units of choice - circuit, pole line, line miles or kilometers, etc.).	The responsible entity failed to inspect more than 15% of its applicable lines (measured in units of choice - circuit, pole line, line miles or kilometers, etc.).
R7.	The responsible entity failed to complete 5% or less of its annual vegetation work plan for its applicable lines (as finally modified).	The responsible entity failed to complete more than 5% and up to and including 10% of its annual vegetation work plan for its applicable lines (as finally modified).	The responsible entity failed to complete more than 10% and up to and including 15% of its annual vegetation work plan for its applicable lines (as finally modified).	The responsible entity failed to complete more than 15% of its annual vegetation work plan for its applicable lines (as finally modified).

D. Regional Variances

None.

E. Associated Documents

- FAC-003-4 Implementation Plan

Version History

Version	Date	Action	Change Tracking
1	January 20, 2006	1. Added "Standard Development Roadmap." 2. Changed "60" to "Sixty" in section A, 5.2. 3. Added "Proposed Effective Date: April 7, 2006" to footer. 4. Added "Draft 3: November 17, 2005" to footer.	New
1	April 4, 2007	Regulatory Approval - Effective Date	New
2	November 3, 2011	Adopted by the NERC Board of Trustees	New
2	March 21, 2013	FERC Order issued approving FAC-003-2 (Order No. 777) FERC Order No. 777 was issued on March 21, 2013 directing NERC to "conduct or contract testing to obtain empirical data and submit a report to the Commission providing the results of the testing."[16]	Revisions

[16] *Revisions to Reliability Standard for Transmission Vegetation Management, Order No. 777,* 142 FERC ¶ 61,208 (2013)

2	May 9, 2013	Board of Trustees adopted the modification of the VRF for Requirement R2 of FAC-003-2 by raising the VRF from “Medium” to “High.”	Revisions
3	May 9, 2013	FAC-003-3 adopted by Board of Trustees	Revisions
3	September 19, 2013	A FERC order was issued on September 19, 2013, approving FAC-003-3. This standard became enforceable on July 1, 2014 for Transmission Owners. For Generator Owners, R3 became enforceable on January 1, 2015 and all other requirements (R1, R2, R4, R5, R6, and R7) became enforceable on January 1, 2016.	Revisions
3	November 22, 2013	Updated the VRF for R2 from “Medium” to “High” per a Final Rule issued by FERC	Revisions
3	July 30, 2014	Transferred the effective dates section from FAC-003-2 (for Transmission Owners) into FAC-003-3, per the FAC-003-3 implementation plan	Revisions
4	February 11, 2016	Adopted by Board of Trustees. Adjusted MVCD values in Table 2 for alternating current systems, consistent with findings reported in report filed on August 12, 2015 in Docket No. RM12-4-002 consistent with FERC’s directive in Order No. 777, and based on empirical testing results for flashover distances between conductors and vegetation.	Revisions
4	March 9, 2016	Corrected subpart 7.10 to M7, corrected value of .07 to .7	Errata
4	April 26, 2016	FERC Letter Order approving FAC-003-4. Docket No. RD16-4-000.	

FAC-003 — TABLE 2 — Minimum Vegetation Clearance Distances (MVCD)[17]

For **Alternating Current** Voltages (feet)

(AC) Nominal System Voltage (KV)[+]	(AC) Maximum System Voltage (kV)[18]	MVCD (feet) Over sea level up to 500 ft	MVCD feet Over 500 ft up to 1000 ft	MVCD feet Over 1000 ft up to 2000 ft	MVCD feet Over 2000 ft up to 3000 ft	MVCD feet Over 3000 ft up to 4000 ft	MVCD feet Over 4000 ft up to 5000 ft	MVCD feet Over 5000 ft up to 6000 ft	MVCD feet Over 6000 ft up to 7000 ft	MVCD feet Over 7000 ft up to 8000 ft	MVCD feet Over 8000 ft up to 9000 ft	MVCD feet Over 9000 ft up to 10000 ft	MVCD feet Over 10000 ft up to 11000 ft	MVCD feet Over 11000 ft up to 12000 ft	MVCD feet Over 12000 ft up to 13000 ft	MVCD feet Over 13000 ft up to 14000 ft	MVCD feet Over 14000 ft up to 15000 ft
765	800	11.6ft	11.7ft	11.9ft	12.1ft	12.2ft	12.4ft	12.6ft	12.8ft	13.0ft	13.1ft	13.3ft	13.5ft	13.7ft	13.9ft	14.1ft	14.3ft
500	550	7.0ft	7.1ft	7.2ft	7.4ft	7.5ft	7.6ft	7.8ft	7.9ft	8.1ft	8.2ft	8.3ft	8.5ft	8.6ft	8.8ft	8.9ft	9.1ft
345	362[19]	4.3ft	4.3ft	4.4ft	4.5ft	4.6ft	4.7ft	4.8ft	4.9ft	5.0ft	5.1ft	5.2ft	5.3ft	5.4ft	5.5ft	5.6ft	5.7ft
287	302	5.2ft	5.3ft	5.4ft	5.5ft	5.6ft	5.7ft	5.8ft	5.9ft	6.1ft	6.2ft	6.3ft	6.4ft	6.5ft	6.6ft	6.8ft	6.9ft
230	242	4.0ft	4.1ft	4.2ft	4.3ft	4.3ft	4.4ft	4.5ft	4.6ft	4.7ft	4.8ft	4.9ft	5.0ft	5.1ft	5.2ft	5.3ft	5.4ft
161*	169	2.7ft	2.7ft	2.8ft	2.9ft	2.9ft	3.0ft	3.0ft	3.1ft	3.2ft	3.3ft	3.3ft	3.4ft	3.5ft	3.6ft	3.7ft	3.8ft
138*	145	2.3ft	2.3ft	2.4ft	2.4ft	2.5ft	2.5ft	2.6ft	2.7ft	2.7ft	2.8ft	2.8ft	2.9ft	3.0ft	3.0ft	3.1ft	3.2ft
115*	121	1.9ft	1.9ft	1.9ft	2.0ft	2.0ft	2.1ft	2.1ft	2.2ft	2.2ft	2.3ft	2.3ft	2.4ft	2.5ft	2.5ft	2.6ft	2.7ft
88*	100	1.5ft	1.5ft	1.6ft	1.6ft	1.7ft	1.7ft	1.8ft	1.8ft	1.8ft	1.9ft	1.9ft	2.0ft	2.0ft	2.1ft	2.2ft	2.2ft
69*	72	1.1ft	1.1ft	1.1ft	1.2ft	1.2ft	1.2ft	1.2ft	1.3ft	1.3ft	1.3ft	1.4ft	1.4ft	1.4ft	1.5ft	1.6ft	1.6ft

* Such lines are applicable to this standard only if PC has determined such per FAC-014 (refer to the Applicability Section above)

[+] *Table 2 – Table of MVCD values at a 1.0 gap factor (in U.S. customary units), which is located in the EPRI report filed with FERC on August 12, 2015. (The 14000-15000 foot values were subsequently provided by EPRI in an updated Table 2 on December 1, 2015, filed with the FAC-003-4 Petition at FERC)*

[17] The distances in this Table are the minimums required to prevent Flash-over; however prudent vegetation maintenance practices dictate that substantially greater distances will be achieved at time of vegetation maintenance.

[18] Where applicable lines are operated at nominal voltages other than those listed, the applicable Transmission Owner or applicable Generator Owner should use the maximum system voltage to determine the appropriate clearance for that line.

[19] The change in transient overvoltage factors in the calculations are the driver in the decrease in MVCDs for voltages of 345 kV and above. Refer to pp.29-31 in the Supplemental Materials for additional information.

TABLE 2 (CONT) — Minimum Vegetation Clearance Distances (MVCD)[20]

For **Alternating Current** Voltages (meters)

(AC) Nominal System Voltage (KV)+	(AC) Maximum System Voltage (kV)[21]	MVCD meters Over sea level up to 153 m	MVCD meters Over 153m up to 305m	MVCD meters Over 305m up to 610m	MVCD meters Over 610m up to 915m	MVCD meters Over 915m up to 1220m	MVCD meters Over 1220m up to 1524m	MVCD meters Over 1524m up to 1829m	MVCD meters Over 1829m up to 2134m	MVCD meters Over 2134m up to 2439m	MVCD meters Over 2439m up to 2744m	MVCD meters Over 2744m up to 3048m	MVCD meters Over 3048m up to 3353m	MVCD meters Over 3353m up to 3657m	MVCD meters Over 3657m up to 3962m	MVCD meters Over 3962 m up to 4268 m	MVCD meters Over 4268m up to 4572m
765	800	3.6m	3.6m	3.6m	3.7m	3.7m	3.8m	3.8m	3.9m	4.0m	4.0m	4.1m	4.1m	4.2m	4.2m	4.3m	4.4m
500	550	2.1m	2.2m	2.2m	2.3m	2.3m	2.3m	2.4m	2.4m	2.5m	2..5m	2.5m	2.6m	2.6m	2.7m	2.7m	2.7m
345	362[22]	1.3m	1.3m	1.3m	1.4m	1.4m	1.4m	1.5m	1.5m	1.5m	1.6m	1.6m	1.6m	1.6m	1.7m	1.7m	1.8m
287	302	1.6m	1.6m	1.7m	1.7m	1.7m	1.7m	1.8m	1.8m	1.9m	1.9m	1.9m	2.0m	2.0m	2.0m	2.1m	2.1m
230	242	1.2m	1.3m	1.3m	1.3m	1.3m	1.3m	1.4m	1.4m	1.4m	1.5m	1.5m	1.5m	1.6m	1.6m	1.6m	1.6m
161*	169	0.8m	0.8m	0.9m	0.9m	0.9m	0.9m	0.9m	1.0m	1.0m	1.0m	1.0m	1.0m	1.1m	1.1m	1.1m	1.1m
138*	145	0.7m	0.7m	0.7m	0.7m	0.7m	0.7m	0.8m	0.8m	0.8m	0.9m	0.9m	0.9m	0.9m	0.9m	1.0m	1.0m
115*	121	0.6m	0.6m	0.6m	0.6m	0.6m	0.6m	0.6m	0.7m	0.7m	0.7m	0.7m	0.7m	0.8m	0.8m	0.8m	0.8m
88*	100	0.4m	0.4m	0.5m	0.5m	0.5m	0.5m	0.6m	0.6m	0.6m	0.6m	0.6m	0.6m	0.6m	0.6m	0.7m	0.7m
69*	72	0.3m	0.3m	0.3m	0.4m	0.4m	0.4m	0.4m	0.4m	0.4m	0.4m	0.4m	0.4m	0.4m	0.5m	0.5m	0.5m

* Such lines are applicable to this standard only if PC has determined such per FAC-014 (refer to the Applicability Section above)

+ *Table 2 – Table of MVCD values at a 1.0 gap factor (in U.S. customary units), which is located in the EPRI report filed with FERC on August 12, 2015. (The 14000-15000 foot values were subsequently provided by EPRI in an updated Table 2 on December 1, 2015, filed with the FAC-003-4 Petition at FERC)*

[20] The distances in this Table are the minimums required to prevent Flash-over; however prudent vegetation maintenance practices dictate that substantially greater distances will be achieved at time of vegetation maintenance.

[21] Where applicable lines are operated at nominal voltages other than those listed, the applicable Transmission Owner or applicable Generator Owner should use the maximum system voltage to determine the appropriate clearance for that line.

[22] The change in transient overvoltage factors in the calculations are the driver in the decrease in MVCDs for voltages of 345 kV and above. Refer to pp.29-31 in the supplemental materials for additional information.

TABLE 2 (CONT) — Minimum Vegetation Clearance Distances (MVCD)[23]

For **Direct Current** Voltages feet (meters)

(DC) Nominal Pole to Ground Voltage (kV)	MVCD meters Over sea level up to 500 ft (Over sea level up to 152.4 m)	MVCD meters Over 500 ft up to 1000 ft (Over 152.4 m up to 304.8 m	MVCD meters Over 1000 ft up to 2000 ft (Over 304.8 m up to 609.6m)	MVCD meters Over 2000 ft up to 3000 ft (Over 609.6m up to 914.4m	MVCD meters Over 3000 ft up to 4000 ft (Over 914.4m up to 1219.2m	MVCD meters Over 4000 ft up to 5000 ft (Over 1219.2m up to 1524m	MVCD meters Over 5000 ft up to 6000 ft (Over 1524 m up to 1828.8 m)	MVCD meters Over 6000 ft up to 7000 ft (Over 1828.8m up to 2133.6m)	MVCD meters Over 7000 ft up to 8000 ft (Over 2133.6m up to 2438.4m)	MVCD meters Over 8000 ft up to 9000 ft (Over 2438.4m up to 2743.2m)	MVCD meters Over 9000 ft up to 10000 ft (Over 2743.2m up to 3048m)	MVCD meters Over 10000 ft up to 11000 ft (Over 3048m up to 3352.8m)
±750	14.12ft (4.30m)	14.31ft (4.36m)	14.70ft (4.48m)	15.07ft (4.59m)	15.45ft (4.71m)	15.82ft (4.82m)	16.2ft (4.94m)	16.55ft (5.04m)	16.91ft (5.15m)	17.27ft (5.26m)	17.62ft (5.37m)	17.97ft (5.48m)
±600	10.23ft (3.12m)	10.39ft (3.17m)	10.74ft (3.26m)	11.04ft (3.36m)	11.35ft (3.46m)	11.66ft (3.55m)	11.98ft (3.65m)	12.3ft (3.75m)	12.62ft (3.85m)	12.92ft (3.94m)	13.24ft (4.04m)	13.54ft (4.13m)
±500	8.03ft (2.45m)	8.16ft (2.49m)	8.44ft (2.57m)	8.71ft (2.65m)	8.99ft (2.74m)	9.25ft (2.82m)	9.55ft (2.91m)	9.82ft (2.99m)	10.1ft (3.08m)	10.38ft (3.16m)	10.65ft (3.25m)	10.92ft (3.33m)
±400	6.07ft (1.85m)	6.18ft (1.88m)	6.41ft (1.95m)	6.63ft (2.02m)	6.86ft (2.09m)	7.09ft (2.16m)	7.33ft (2.23m)	7.56ft (2.30m)	7.80ft (2.38m)	8.03ft (2.45m)	8.27ft (2.52m)	8.51ft (2.59m)
±250	3.50ft (1.07m)	3.57ft (1.09m)	3.72ft (1.13m)	3.87ft (1.18m)	4.02ft (1.23m)	4.18ft (1.27m)	4.34ft (1.32m)	4.5ft (1.37m)	4.66ft (1.42m)	4.83ft (1.47m)	5.00ft (1.52m)	5.17ft (1.58m)

[23] The distances in this Table are the minimums required to prevent Flash-over; however prudent vegetation maintenance practices dictate that substantially greater distances will be achieved at time of vegetation maintenance.

Guideline and Technical Basis

Effective dates:

The Compliance section is standard language used in most NERC standards to cover the general effective date and covers the vast majority of situations. A special case covers effective dates for (1) lines initially becoming subject to the Standard, (2) lines changing in applicability within the standard.

The special case is needed because the Planning Coordinators may designate lines below 200 kV to become elements of an IROL or Major WECC Transfer Path in a future Planning Year (PY). For example, studies by the Planning Coordinator in 2015 may identify a line to have that designation beginning in PY 2025, ten years after the planning study is performed. It is not intended for the Standard to be immediately applicable to, or in effect for, that line until that future PY begins. The effective date provision for such lines ensures that the line will become subject to the standard on January 1 of the PY specified with an allowance of at least 12 months for the applicable Transmission Owner or applicable Generator Owner to make the necessary preparations to achieve compliance on that line. A line operating below 200kV designated as an element of an IROL or Major WECC Transfer Path may be removed from that designation due to system improvements, changes in generation, changes in loads or changes in studies and analysis of the network.

Date that Planning Study is completed	PY the line will become an IROL element	Date 1	Date 2	Effective Date The later of Date 1 or Date 2
05/15/2011	2012	05/15/2012	01/01/2012	05/15/2012
05/15/2011	2013	05/15/2012	01/01/2013	01/01/2013
05/15/2011	2014	05/15/2012	01/01/2014	01/01/2014
05/15/2011	2021	05/15/2012	01/01/2021	01/01/2021

Defined Terms:

Explanation for revising the definition of ROW:
The current NERC glossary definition of Right of Way has been modified to include Generator Owners and to address the matter set forth in Paragraph 734 of FERC Order 693. The Order pointed out that Transmission Owners may in some cases own more property or rights than are needed to reliably operate transmission lines. This definition represents a slight but significant departure from the strict legal definition of “right of way” in that this definition is based on engineering and construction considerations that establish the width of a corridor from a technical basis. The pre-2007 maintenance records are included in the current definition to allow the use of such vegetation widths if there were no engineering or construction standards that

referenced the width of right of way to be maintained for vegetation on a particular line but the evidence exists in maintenance records for a width that was in fact maintained prior to this standard becoming mandatory. Such widths may be the only information available for lines that had limited or no vegetation easement rights and were typically maintained primarily to ensure public safety. This standard does not require additional easement rights to be purchased to satisfy a minimum right of way width that did not exist prior to this standard becoming mandatory.

Explanation for revising the definition of Vegetation Inspection:
The current glossary definition of this NERC term was modified to include Generator Owners and to allow both maintenance inspections and vegetation inspections to be performed concurrently. This allows potential efficiencies, especially for those lines with minimal vegetation and/or slow vegetation growth rates.

Explanation of the derivation of the MVCD:
The MVCD is a calculated minimum distance that is derived from the Gallet equation. This is a method of calculating a flash over distance that has been used in the design of high voltage transmission lines. Keeping vegetation away from high voltage conductors by this distance will prevent voltage flash-over to the vegetation. See the explanatory text below for Requirement R3 and associated Figure 1. Table 2 of the Standard provides MVCD values for various voltages and altitudes. The table is based on empirical testing data from EPRI as requested by FERC in Order No. 777.

Project 2010-07.1 Adjusted MVCDs per EPRI Testing:
In Order No. 777, FERC directed NERC to undertake testing to gather empirical data validating the appropriate gap factor used in the Gallet equation to calculate MVCDs, specifically the gap factor for the flash-over distances between conductors and vegetation. See, Order No. 777, at P 60. NERC engaged industry through a collaborative research project and contracted EPRI to complete the scope of work. In January 2014, NERC formed an advisory group to assist with developing the scope of work for the project. This team provided subject matter expertise for developing the test plan, monitoring testing, and vetting the analysis and conclusions to be submitted in a final report. The advisory team was comprised of NERC staff, arborists, and industry members with wide-ranging expertise in transmission engineering, insulation coordination, and vegetation management. The testing project commenced in April 2014 and continued through October 2014 with the final set of testing completed in May 2015. Based on these testing results conducted by EPRI, and consistent with the report filed in FERC Docket No. RM12-4-000, the gap factor used in the Gallet equation required adjustment from 1.3 to 1.0. This resulted in increased MVCD values for all alternating current system voltages identified. The adjusted MVCD values, reflecting the 1.0 gap factor, are included in Table 2 of version 4 of FAC-003.

The air gap testing completed by EPRI per FERC Order No. 777 established that trees with large spreading canopies growing directly below energized high voltage conductors create the

greatest likelihood of an air gap flash over incident and was a key driver in changing the gap factor to a more conservative value of 1.0 in version 4 of this standard.

Requirements R1 and R2:
R1 and R2 are performance-based requirements. The reliability objective or outcome to be achieved is the management of vegetation such that there are no vegetation encroachments within a minimum distance of transmission lines. Content-wise, R1 and R2 are the same requirements; however, they apply to different Facilities. Both R1 and R2 require each applicable Transmission Owner or applicable Generator Owner to manage vegetation to prevent encroachment within the MVCD of transmission lines. R1 is applicable to lines that are identified as an element of an IROL or Major WECC Transfer Path. R2 is applicable to all other lines that are not elements of IROLs, and not elements of Major WECC Transfer Paths.

The separation of applicability (between R1 and R2) recognizes that inadequate vegetation management for an applicable line that is an element of an IROL or a Major WECC Transfer Path is a greater risk to the interconnected electric transmission system than applicable lines that are not elements of IROLs or Major WECC Transfer Paths. Applicable lines that are not elements of IROLs or Major WECC Transfer Paths do require effective vegetation management, but these lines are comparatively less operationally significant.

Requirements R1 and R2 state that if inadequate vegetation management allows vegetation to encroach within the MVCD distance as shown in Table 2, it is a violation of the standard. Table 2 distances are the minimum clearances that will prevent spark-over based on the Gallet equations. These requirements assume that transmission lines and their conductors are operating within their Rating. If a line conductor is intentionally or inadvertently operated beyond its Rating and Rated Electrical Operating Condition (potentially in violation of other standards), the occurrence of a clearance encroachment may occur solely due to that condition. For example, emergency actions taken by an applicable Transmission Owner or applicable Generator Owner or Reliability Coordinator to protect an Interconnection may cause excessive sagging and an outage. Another example would be ice loading beyond the line's Rating and Rated Electrical Operating Condition. Such vegetation-related encroachments and outages are not violations of this standard.

Evidence of failures to adequately manage vegetation include real-time observation of a vegetation encroachment into the MVCD (absent a Sustained Outage), or a vegetation-related encroachment resulting in a Sustained Outage due to a fall-in from inside the ROW, or a vegetation-related encroachment resulting in a Sustained Outage due to the blowing together of the lines and vegetation located inside the ROW, or a vegetation-related encroachment resulting in a Sustained Outage due to a grow-in. Faults which do not cause a Sustained outage and which are confirmed to have been caused by vegetation encroachment within the MVCD are considered the equivalent of a Real-time observation for violation severity levels.

With this approach, the VSLs for R1 and R2 are structured such that they directly correlate to the severity of a failure of an applicable Transmission Owner or applicable Generator Owner to manage vegetation and to the corresponding performance level of the Transmission Owner's

vegetation program's ability to meet the objective of "preventing the risk of those vegetation related outages that could lead to Cascading." Thus violation severity increases with an applicable Transmission Owner's or applicable Generator Owner's inability to meet this goal and its potential of leading to a Cascading event. The additional benefits of such a combination are that it simplifies the standard and clearly defines performance for compliance. A performance-based requirement of this nature will promote high quality, cost effective vegetation management programs that will deliver the overall end result of improved reliability to the system.

Multiple Sustained Outages on an individual line can be caused by the same vegetation. For example initial investigations and corrective actions may not identify and remove the actual outage cause then another outage occurs after the line is re-energized and previous high conductor temperatures return. Such events are considered to be a single vegetation-related Sustained Outage under the standard where the Sustained Outages occur within a 24 hour period.

If the applicable Transmission Owner or applicable Generator Owner has applicable lines operated at nominal voltage levels not listed in Table 2, then the applicable TO or applicable GO should use the next largest clearance distance based on the next highest nominal voltage in the table to determine an acceptable distance.

Requirement R3:
R3 is a competency based requirement concerned with the maintenance strategies, procedures, processes, or specifications, an applicable Transmission Owner or applicable Generator Owner uses for vegetation management.

An adequate transmission vegetation management program formally establishes the approach the applicable Transmission Owner or applicable Generator Owner uses to plan and perform vegetation work to prevent transmission Sustained Outages and minimize risk to the transmission system. The approach provides the basis for evaluating the intent, allocation of appropriate resources, and the competency of the applicable Transmission Owner or applicable Generator Owner in managing vegetation. There are many acceptable approaches to manage vegetation and avoid Sustained Outages. However, the applicable Transmission Owner or applicable Generator Owner must be able to show the documentation of its approach and how it conducts work to maintain clearances.

An example of one approach commonly used by industry is ANSI Standard A300, part 7. However, regardless of the approach a utility uses to manage vegetation, any approach an applicable Transmission Owner or applicable Generator Owner chooses to use will generally contain the following elements:

1. *the maintenance strategy used (such as minimum vegetation-to-conductor distance or maximum vegetation height) to ensure that MVCD clearances are never violated*

2. *the work methods that the applicable Transmission Owner or applicable Generator Owner uses to control vegetation*
3. *a stated Vegetation Inspection frequency*
4. *an annual work plan*

The conductor's position in space at any point in time is continuously changing in reaction to a number of different loading variables. Changes in vertical and horizontal conductor positioning are the result of thermal and physical loads applied to the line. Thermal loading is a function of line current and the combination of numerous variables influencing ambient heat dissipation including wind velocity/direction, ambient air temperature and precipitation. Physical loading applied to the conductor affects sag and sway by combining physical factors such as ice and wind loading. The movement of the transmission line conductor and the MVCD is illustrated in Figure 1 below.

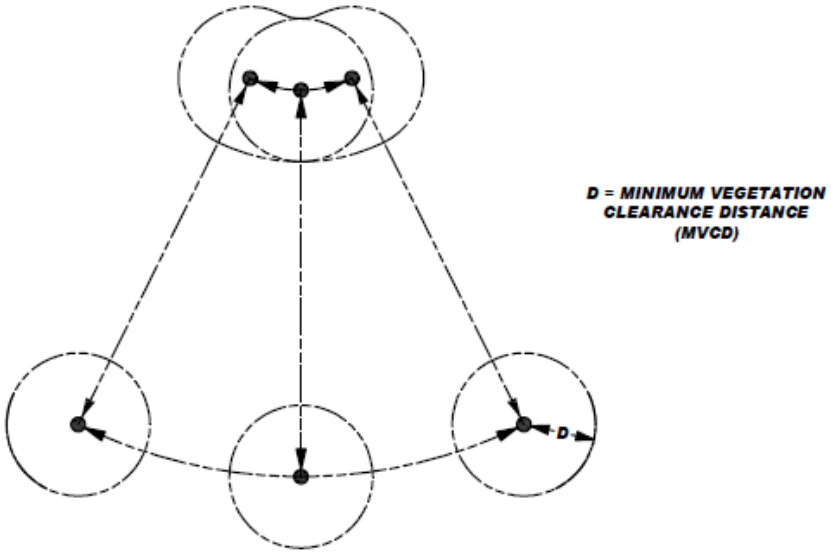


Figure 1

A cross-section view of a single conductor at a given point along the span is shown with six possible conductor positions due to movement resulting from thermal and mechanical loading.

Requirement R4:
R4 is a risk-based requirement. It focuses on preventative actions to be taken by the applicable Transmission Owner or applicable Generator Owner for the mitigation of Fault risk when a vegetation threat is confirmed. R4 involves the notification of potentially threatening vegetation conditions, without any intentional delay, to the control center holding switching authority for that specific transmission line. Examples of acceptable unintentional delays may

include communication system problems (for example, cellular service or two-way radio disabled), crews located in remote field locations with no communication access, delays due to severe weather, etc.

Confirmation is key that a threat actually exists due to vegetation. This confirmation could be in the form of an applicable Transmission Owner or applicable Generator Owner employee who personally identifies such a threat in the field. Confirmation could also be made by sending out an employee to evaluate a situation reported by a landowner.

Vegetation-related conditions that warrant a response include vegetation that is near or encroaching into the MVCD (a grow-in issue) or vegetation that could fall into the transmission conductor (a fall-in issue). A knowledgeable verification of the risk would include an assessment of the possible sag or movement of the conductor while operating between no-load conditions and its rating.

The applicable Transmission Owner or applicable Generator Owner has the responsibility to ensure the proper communication between field personnel and the control center to allow the control center to take the appropriate action until or as the vegetation threat is relieved. Appropriate actions may include a temporary reduction in the line loading, switching the line out of service, or other preparatory actions in recognition of the increased risk of outage on that circuit. The notification of the threat should be communicated in terms of minutes or hours as opposed to a longer time frame for corrective action plans (see R5).

All potential grow-in or fall-in vegetation-related conditions will not necessarily cause a Fault at any moment. For example, some applicable Transmission Owners or applicable Generator Owners may have a danger tree identification program that identifies trees for removal with the potential to fall near the line. These trees would not require notification to the control center unless they pose an immediate fall-in threat.

Requirement R5:
R5 is a risk-based requirement. It focuses upon preventative actions to be taken by the applicable Transmission Owner or applicable Generator Owner for the mitigation of Sustained Outage risk when temporarily constrained from performing vegetation maintenance. The intent of this requirement is to deal with situations that prevent the applicable Transmission Owner or applicable Generator Owner from performing planned vegetation management work and, as a result, have the potential to put the transmission line at risk. Constraints to performing vegetation maintenance work as planned could result from legal injunctions filed by property owners, the discovery of easement stipulations which limit the applicable Transmission Owner's or applicable Generator Owner's rights, or other circumstances.

This requirement is not intended to address situations where the transmission line is not at potential risk and the work event can be rescheduled or re-planned using an alternate work methodology. For example, a land owner may prevent the planned use of herbicides to control incompatible vegetation outside of the MVCD, but agree to the use of mechanical clearing. In

this case the applicable Transmission Owner or applicable Generator Owner is not under any immediate time constraint for achieving the management objective, can easily reschedule work using an alternate approach, and therefore does not need to take interim corrective action.

However, in situations where transmission line reliability is potentially at risk due to a constraint, the applicable Transmission Owner or applicable Generator Owner is required to take an interim corrective action to mitigate the potential risk to the transmission line. A wide range of actions can be taken to address various situations. General considerations include:

- Identifying locations where the applicable Transmission Owner or applicable Generator Owner is constrained from performing planned vegetation maintenance work which potentially leaves the transmission line at risk.
- Developing the specific action to mitigate any potential risk associated with not performing the vegetation maintenance work as planned.
- Documenting and tracking the specific action taken for the location.
- In developing the specific action to mitigate the potential risk to the transmission line the applicable Transmission Owner or applicable Generator Owner could consider location specific measures such as modifying the inspection and/or maintenance intervals. Where a legal constraint would not allow any vegetation work, the interim corrective action could include limiting the loading on the transmission line.
- The applicable Transmission Owner or applicable Generator Owner should document and track the specific corrective action taken at each location. This location may be indicated as one span, one tree or a combination of spans on one property where the constraint is considered to be temporary.

Requirement R6:
R6 is a risk-based requirement. This requirement sets a minimum time period for completing Vegetation Inspections. The provision that Vegetation Inspections can be performed in conjunction with general line inspections facilitates a Transmission Owner's ability to meet this requirement. However, the applicable Transmission Owner or applicable Generator Owner may determine that more frequent vegetation specific inspections are needed to maintain reliability levels, based on factors such as anticipated growth rates of the local vegetation, length of the local growing season, limited ROW width, and local rainfall. Therefore it is expected that some transmission lines may be designated with a higher frequency of inspections.

The VSLs for Requirement R6 have levels ranked by the failure to inspect a percentage of the applicable lines to be inspected. To calculate the appropriate VSL the applicable Transmission Owner or applicable Generator Owner may choose units such as: circuit, pole line, line miles or kilometers, etc.

For example, when an applicable Transmission Owner or applicable Generator Owner operates 2,000 miles of applicable transmission lines this applicable Transmission Owner or applicable

Generator Owner will be responsible for inspecting all the 2,000 miles of lines at least once during the calendar year. If one of the included lines was 100 miles long, and if it was not inspected during the year, then the amount failed to inspect would be 100/2000 = 0.05 or 5%. The "Low VSL" for R6 would apply in this example.

Requirement R7:
R7 is a risk-based requirement. The applicable Transmission Owner or applicable Generator Owner is required to complete its annual work plan for vegetation management to accomplish the purpose of this standard. Modifications to the work plan in response to changing conditions or to findings from vegetation inspections may be made and documented provided they do not put the transmission system at risk. The annual work plan requirement is not intended to necessarily require a "span-by-span", or even a "line-by-line" detailed description of all work to be performed. It is only intended to require that the applicable Transmission Owner or applicable Generator Owner provide evidence of annual planning and execution of a vegetation management maintenance approach which successfully prevents encroachment of vegetation into the MVCD.

When an applicable Transmission Owner or applicable Generator Owner identifies 1,000 miles of applicable transmission lines to be completed in the applicable Transmission Owner's or applicable Generator Owner's annual plan, the applicable Transmission Owner or applicable Generator Owner will be responsible completing those identified miles. If an applicable Transmission Owner or applicable Generator Owner makes a modification to the annual plan that does not put the transmission system at risk of an encroachment the annual plan may be modified. If 100 miles of the annual plan is deferred until next year the calculation to determine what percentage was completed for the current year would be: 1000 – 100 (deferred miles) = 900 modified annual plan, or 900 / 900 = 100% completed annual miles. If an applicable Transmission Owner or applicable Generator Owner only completed 875 of the total 1000 miles with no acceptable documentation for modification of the annual plan the calculation for failure to complete the annual plan would be: 1000 – 875 = 125 miles failed to complete then, 125 miles (not completed) / 1000 total annual plan miles = 12.5% failed to complete.

The ability to modify the work plan allows the applicable Transmission Owner or applicable Generator Owner to change priorities or treatment methodologies during the year as conditions or situations dictate. For example recent line inspections may identify unanticipated high priority work, weather conditions (drought) could make herbicide application ineffective during the plan year, or a major storm could require redirecting local resources away from planned maintenance. This situation may also include complying with mutual assistance agreements by moving resources off the applicable Transmission Owner's or applicable Generator Owner's system to work on another system. Any of these examples could result in acceptable deferrals or additions to the annual work plan provided that they do not put the transmission system at risk of a vegetation encroachment.
In general, the vegetation management maintenance approach should use the full extent of the applicable Transmission Owner's or applicable Generator Owner's easement, fee simple and

other legal rights allowed. A comprehensive approach that exercises the full extent of legal rights on the ROW is superior to incremental management because in the long term it reduces the overall potential for encroachments, and it ensures that future planned work and future planned inspection cycles are sufficient.

When developing the annual work plan the applicable Transmission Owner or applicable Generator Owner should allow time for procedural requirements to obtain permits to work on federal, state, provincial, public, tribal lands. In some cases the lead time for obtaining permits may necessitate preparing work plans more than a year prior to work start dates. Applicable Transmission Owners or applicable Generator Owners may also need to consider those special landowner requirements as documented in easement instruments.

This requirement sets the expectation that the work identified in the annual work plan will be completed as planned. Therefore, deferrals or relevant changes to the annual plan shall be documented. Depending on the planning and documentation format used by the applicable Transmission Owner or applicable Generator Owner, evidence of successful annual work plan execution could consist of signed-off work orders, signed contracts, printouts from work management systems, spreadsheets of planned versus completed work, timesheets, work inspection reports, or paid invoices. Other evidence may include photographs, and walk-through reports.

Notes:

The SDT determined that the use of IEEE 516-2003 in version 1 of FAC-003 was a misapplication. The SDT consulted specialists who advised that the Gallet equation would be a technically justified method. The explanation of why the Gallet approach is more appropriate is explained in the paragraphs below.

The drafting team sought a method of establishing minimum clearance distances that uses realistic weather conditions and realistic maximum transient over-voltages factors for in-service transmission lines.

The SDT considered several factors when looking at changes to the minimum vegetation to conductor distances in FAC-003-1:

- avoid the problem associated with referring to tables in another standard (IEEE-516-2003)
- transmission lines operate in non-laboratory environments (wet conditions)
- transient over-voltage factors are lower for in-service transmission lines than for inadvertently re-energized transmission lines with trapped charges.

FAC-003-1 used the minimum air insulation distance (MAID) without tools formula provided in IEEE 516-2003 to determine the minimum distance between a transmission line conductor and vegetation. The equations and methods provided in IEEE 516 were developed by an IEEE Task Force in 1968 from test data provided by thirteen independent laboratories. The distances provided in IEEE 516 Tables 5 and 7 are based on the withstand voltage of a dry rod-rod air gap,

or in other words, dry laboratory conditions. Consequently, the validity of using these distances in an outside environment application has been questioned.

FAC-003-1 allowed Transmission Owners to use either Table 5 or Table 7 to establish the minimum clearance distances. Table 7 could be used if the Transmission Owner knew the maximum transient over-voltage factor for its system. Otherwise, Table 5 would have to be used. Table 5 represented minimum air insulation distances under the worst possible case for transient over-voltage factors. These worst case transient over-voltage factors were as follows: 3.5 for voltages up to 362 kV phase to phase; 3.0 for 500 - 550 kV phase to phase; and 2.5 for 765 to 800 kV phase to phase. These worst case over-voltage factors were also a cause for concern in this particular application of the distances.

In general, the worst case transient over-voltages occur on a transmission line that is inadvertently re-energized immediately after the line is de-energized and a trapped charge is still present. The intent of FAC-003 is to keep a transmission line that is in service from becoming de-energized (i.e. tripped out) due to spark-over from the line conductor to nearby vegetation. Thus, the worst case transient overvoltage assumptions are not appropriate for this application. Rather, the appropriate over voltage values are those that occur only while the line is energized.

Typical values of transient over-voltages of in-service lines are not readily available in the literature because they are negligible compared with the maximums. A conservative value for the maximum transient over-voltage that can occur anywhere along the length of an in-service ac line was approximately 2.0 per unit. This value was a conservative estimate of the transient over-voltage that is created at the point of application (e.g. a substation) by switching a capacitor bank without pre-insertion devices (e.g. closing resistors). At voltage levels where capacitor banks are not very common (e.g. Maximum System Voltage of 362 kV), the maximum transient over-voltage of an in-service ac line are created by fault initiation on adjacent ac lines and shunt reactor bank switching. These transient voltages are usually 1.5 per unit or less.

Even though these transient over-voltages will not be experienced at locations remote from the bus at which they are created, in order to be conservative, it is assumed that all nearby ac lines are subjected to this same level of over-voltage. Thus, a maximum transient over-voltage factor of 2.0 per unit for transmission lines operated at 302 kV and below was considered to be a realistic maximum in this application. Likewise, for ac transmission lines operated at Maximum System Voltages of 362 kV and above a transient over-voltage factor of 1.4 per unit was considered a realistic maximum.

The Gallet equations are an accepted method for insulation coordination in tower design. These equations are used for computing the required strike distances for proper transmission line insulation coordination. They were developed for both wet and dry applications and can be used with any value of transient over-voltage factor. The Gallet equation also can take into account various air gap geometries. This approach was used to design the first 500 kV and 765 kV lines in North America.

If one compares the MAID using the IEEE 516-2003 Table 7 (table D.5 for English values) with the critical spark-over distances computed using the Gallet wet equations, for each of the nominal voltage classes and identical transient over-voltage factors, the Gallet equations yield a more conservative (larger) minimum distance value.

Distances calculated from either the IEEE 516 (dry) formulas or the Gallet "wet" formulas are not vastly different when the same transient overvoltage factors are used; the "wet" equations will consistently produce slightly larger distances than the IEEE 516 equations when the same transient overvoltage is used. While the IEEE 516 equations were only developed for dry conditions the Gallet equations have provisions to calculate spark-over distances for both wet and dry conditions.

Since no empirical data for spark over distances to live vegetation existed at the time version 3 was developed, the SDT chose a proven method that has been used in other EHV applications. The Gallet equations relevance to wet conditions and the selection of a Transient Overvoltage Factor that is consistent with the absence of trapped charges on an in-service transmission line make this methodology a better choice.

The following table is an example of the comparison of distances derived from IEEE 516 and the Gallet equations.

Comparison of spark-over distances computed using Gallet wet equations vs.

IEEE 516-2003 MAID distances

(AC) Nom System Voltage (kV)	**(AC) Max System Voltage (kV)**	**Transient Over-voltage Factor (T)**	**Clearance (ft.) Gallet (wet) @ Alt. 3000 feet**	Table 7 (Table D.5 for feet) **IEEE 516-2003 MAID (ft) @ Alt. 3000 feet**
765	800	2.0	14.36	13.95
500	550	2.4	11.0	10.07
345	362	3.0	8.55	7.47
230	242	3.0	5.28	4.2
115	121	3.0	2.46	2.1

Rationale:
During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for Applicability (section 4.2.4):
The areas excluded in 4.2.4 were excluded based on comments from industry for reasons summarized as follows:

1) There is a very low risk from vegetation in this area. Based on an informal survey, no TOs reported such an event.
2) Substations, switchyards, and stations have many inspection and maintenance activities that are necessary for reliability. Those existing process manage the threat. As such, the formal steps in this standard are not well suited for this environment.
3) Specifically addressing the areas where the standard does and does not apply makes the standard clearer.

Rationale for Applicability (section 4.3):
Within the text of NERC Reliability Standard FAC-003-3, "transmission line(s)" and "applicable line(s)" can also refer to the generation Facilities as referenced in 4.3 and its subsections.

Rationale for R1 and R2:
Lines with the highest significance to reliability are covered in R1; all other lines are covered in R2.

Rationale for the types of failure to manage vegetation which are listed in order of increasing degrees of severity in non-compliant performance as it relates to a failure of an applicable Transmission Owner's or applicable Generator Owner's vegetation maintenance program:

1. This management failure is found by routine inspection or Fault event investigation, and is normally symptomatic of unusual conditions in an otherwise sound program.
2. This management failure occurs when the height and location of a side tree within the ROW is not adequately addressed by the program.
3. This management failure occurs when side growth is not adequately addressed and may be indicative of an unsound program.
4. This management failure is usually indicative of a program that is not addressing the most fundamental dynamic of vegetation management, (i.e. a grow-in under the line). If this type of failure is pervasive on multiple lines, it provides a mechanism for a Cascade.

Rationale for R3:
The documentation provides a basis for evaluating the competency of the applicable Transmission Owner's or applicable Generator Owner's vegetation program. There may be many acceptable approaches to maintain clearances. Any approach must demonstrate that the

applicable Transmission Owner or applicable Generator Owner avoids vegetation-to-wire conflicts under all Ratings and all Rated Electrical Operating Conditions.

Rationale for R4:

This is to ensure expeditious communication between the applicable Transmission Owner or applicable Generator Owner and the control center when a critical situation is confirmed.

Rationale for R5:

Legal actions and other events may occur which result in constraints that prevent the applicable Transmission Owner or applicable Generator Owner from performing planned vegetation maintenance work.

In cases where the transmission line is put at potential risk due to constraints, the intent is for the applicable Transmission Owner and applicable Generator Owner to put interim measures in place, rather than do nothing.

The corrective action process is not intended to address situations where a planned work methodology cannot be performed but an alternate work methodology can be used.

Rationale for R6:

Inspections are used by applicable Transmission Owners and applicable Generator Owners to assess the condition of the entire ROW. The information from the assessment can be used to determine risk, determine future work and evaluate recently-completed work. This requirement sets a minimum Vegetation Inspection frequency of once per calendar year but with no more than 18 months between inspections on the same ROW. Based upon average growth rates across North America and on common utility practice, this minimum frequency is reasonable. Transmission Owners should consider local and environmental factors that could warrant more frequent inspections.

Rationale for R7:

This requirement sets the expectation that the work identified in the annual work plan will be completed as planned. It allows modifications to the planned work for changing conditions, taking into consideration anticipated growth of vegetation and all other environmental factors, provided that those modifications do not put the transmission system at risk of a vegetation encroachment.

Appendix QC-FAC-003-4
Provisions specific to the standard FAC-003-4 applicable in Québec

This appendix establishes specific provisions for the application of the standard in Québec. Provisions of the standard and of its appendix must be read together for the purposes of understanding and interpretation. Where the standard and appendix differ, the appendix shall prevail.

A. Introduction

1. Title: Transmission Vegetation Management

2. Number: FAC-003-4

3. Purpose: No specific provision

4. Applicability: No specific provision

5. Effective Date:

5.1. Adoption of the standard by the Régie: June 8, 2020

5.2. Adoption of the appendix by the Régie: June 8, 2020

5.3. Effective date of the standard and its appendix in Québec: April 1, 2021

6. Background: No specific provision

B. Requirements and Measures

Only requirement R6 and measure M6 were modified as follow:

R6. Each applicable Transmission Owner and applicable Generator Owner shall perform a Vegetation Inspection of 100% of its applicable transmission lines (measured in units of choice - circuit, pole line, line miles or kilometers, etc.)[1]

- at least once per calendar year, with no more than 18 calendar months between inspections on the same ROW, except the lines that have been designated for at least 12 months as having a vegetation control cycle of 5 years or more.
- at least once per 2 calendar years, with no more than 30 calendar months between inspections on the same ROW, for the lines that have been designated for at least 12 months as having a vegetation control cycle of 5 years or more. The Transmission Owner or Generator Owner can designate a line as having a vegetation control cycle of 5 years or more, but this designation must have an insignificant impact on the risk of MVCD encroachment, considering, for the last 6 years, both the results of the of Vegetation Inspections and vegetation management interventions as well as the relevant geographical, meteorological and vegetation data.

[1] When the applicable Transmission Owner or applicable Generator Owner is prevented from performing a Vegetation Inspection within the timeframe in R6 due to a natural disaster, the TO or GO is granted a time extension that is equivalent to the duration of the time the TO or GO was prevented from performing the Vegetation Inspection.

M6. Each applicable Transmission Owner and applicable Generator Owner has evidence that it conducted the inspections specified in R6. Examples of acceptable forms of evidence may include completed and dated work orders, dated invoices, or dated inspection records (R6).

Each applicable Transmission Owner and applicable Generator Owner that has designated lines as having a vegetation control cycle of 5 years, has a report with, for each line, a designation date and, for the past 6 years, the results of Vegetation Inspections and vegetation management interventions as well as the relevant geographical, meteorological and vegetation data.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

The Régie de l'énergie is responsible, in Québec, for compliance enforcement with respect to the reliability standard and its appendix that it adopts.

1.2. Evidence Retention

No specific provision

1.3. Compliance Monitoring and Enforcement Program

The Québec Reliability Standards Compliance Monitoring and Enforcement Program (QCMEP) of the Régie de l'énergie identifies the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

1.4. Additional Compliance Information

The periodic data is submitted to the Régie de l'énergie. The Régie de l'énergie will report the information provided quarterly to NERC.

Violation Severity Levels (Table 1)

The violation severity level for requirement R6 is replaced as follow:

R#	Table 1: Violation Severity Levels (VSL)			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
R6	The responsible entity has an inspection coverage of 95% or more.	The responsible entity has an inspection coverage of more than 90% and less than 95%.	The responsible entity has an inspection coverage of more than 85% and less than 90%.	The responsible entity has an inspection coverage of less than 85%.

The inspection coverage is defined as the ratio of all applicable lines inspected and all applicable lines (measured in units of choice – circuit, pole line, line miles or kilometers, etc.)

If the entity has not designated lines as having a vegetation control cycle of 5 years or more, "all applicable lines inspected" is the lines whose inspections respect Requirement 6, bullet 1.

If the entity has designated lines as having a vegetation control cycle of 5 years or more, the "all applicable lines inspected" is calculated as follows:

- Add all lines whose inspections respect Requirement 6 - first bullet (whether designated or not)

- Add all designated lines that do not respect Requirement 6 - first bullet, that respect Requirement 6 - second bullet and have a complete, correct justification.

- Add half of each designated line that does not respect Requirement 6 - first bullet but which has a partial justification (for example, a piece of evidence is missing or a conclusion is flawed).

Consequently, the "all applicable lines inspected" has no contribution from

- designated lines that do not respect Requirement 6, first bullet and whose justification for designation is absent or seriously flawed;
- designated lines that do not respect Requirement 6 – second bullet and
- non-designated lines that do not respect Requirement 6 – first bullet.

D. Regional Differences

No specific provision

E. Associated Documents

No specific provision

FAC-003—TABLE 2—Minimum Vegetation Clearance Distances (MVCD)

No specific provision

Guidelines and Technical Basis

No specific provision

Revision History

Revision	Date	Action	Change Tracking
0	June 8, 2020	New appendix	New

A. Introduction

1. **Title:** Facility Ratings

2. **Number:** FAC-008-5

3. **Purpose:** To ensure that Facility Ratings used in the reliable planning and operation of the Bulk Electric System (BES) are determined based on technically sound principles. A Facility Rating is essential for the determination of System Operating Limits.

4. **Applicability:**

   4.1. Transmission Owner

   4.2. Generator Owner

5. **Effective Date:** See Implementation Plan.

B. Requirements and Measures

R1. Each Generator Owner shall have documentation for determining the Facility Ratings of its solely and jointly owned generator Facility(ies) up to the low side terminals of the main step up transformer if the Generator Owner does not own the main step up transformer and the high side terminals of the main step up transformer if the Generator Owner owns the main step up transformer. *[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*

1.1. The documentation shall contain assumptions used to rate the generator and at least one of the following:

- Design or construction information such as design criteria, ratings provided by equipment manufacturers, equipment drawings and/or specifications, engineering analyses, method(s) consistent with industry standards (e.g. ANSI and IEEE), or an established engineering practice that has been verified by testing or engineering analysis.
- Operational information such as commissioning test results, performance testing or historical performance records, any of which may be supplemented by engineering analyses.

1.2. The documentation shall be consistent with the principle that the Facility Ratings do not exceed the most limiting applicable Equipment Rating of the individual equipment that comprises that Facility.

M1. Each Generator Owner shall have documentation that shows how its Facility Ratings were determined as identified in Requirement 1.

R2. Each Generator Owner shall have a documented methodology for determining Facility Ratings (Facility Ratings methodology) of its solely and jointly owned equipment connected between the location specified in R1 and the point of interconnection with the Transmission Owner that contains all of the following. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

2.1. The methodology used to establish the Ratings of the equipment that comprises the Facility(ies) shall be consistent with at least one of the following:

- Ratings provided by equipment manufacturers or obtained from equipment manufacturer specifications such as nameplate rating.
- One or more industry standards developed through an open process such as Institute of Electrical and Electronic Engineers (IEEE) or International Council on Large Electric Systems (CIGRE).
- A practice that has been verified by testing, performance history or engineering analysis.

2.2. The underlying assumptions, design criteria, and methods used to determine the Equipment Ratings identified in Requirement R2, Part 2.1 including identification of how each of the following were considered:

2.2.1. Equipment Rating standard(s) used in development of this methodology.

2.2.2. Ratings provided by equipment manufacturers or obtained from equipment manufacturer specifications.

2.2.3. Ambient conditions (for particular or average conditions or as they vary in real-time).

2.2.4. Operating limitations.[1]

2.3. A statement that a Facility Rating shall respect the most limiting applicable Equipment Rating of the individual equipment that comprises that Facility.

2.4. The process by which the Rating of equipment that comprises a Facility is determined.

2.4.1. The scope of equipment addressed shall include, but not be limited to, conductors, transformers, relay protective devices, terminal equipment, and series and shunt compensation devices.

2.4.2. The scope of Ratings addressed shall include, as a minimum, both Normal and Emergency Ratings.

M2. Each Generator Owner shall have a documented Facility Ratings methodology that includes all of the items identified in Requirement 2, Parts 2.1 through 2.4.

R3. Each Transmission Owner shall have a documented methodology for determining Facility Ratings (Facility Ratings methodology) of its solely and jointly owned Facilities (except for those generating unit Facilities addressed in R1 and R2) that contains all of the following: *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

3.1. The methodology used to establish the Ratings of the equipment that comprises the Facility shall be consistent with at least one of the following:

- Ratings provided by equipment manufacturers or obtained from equipment manufacturer specifications such as nameplate rating.
- One or more industry standards developed through an open process such as Institute of Electrical and Electronics Engineers (IEEE) or International Council on Large Electric Systems (CIGRE).
- A practice that has been verified by testing, performance history or engineering analysis.

[1] Such as temporary de-ratings of impaired equipment in accordance with good utility practice.

3.2. The underlying assumptions, design criteria, and methods used to determine the Equipment Ratings identified in Requirement R3, Part 3.1 including identification of how each of the following were considered:

3.2.1. Equipment Rating standard(s) used in development of this methodology.

3.2.2. Ratings provided by equipment manufacturers or obtained from equipment manufacturer specifications.

3.2.3. Ambient conditions (for particular or average conditions or as they vary in real-time).

3.2.4. Operating limitations.[2]

3.3. A statement that a Facility Rating shall respect the most limiting applicable Equipment Rating of the individual equipment that comprises that Facility.

3.4. The process by which the Rating of equipment that comprises a Facility is determined.

3.4.1. The scope of equipment addressed shall include, but not be limited to, transmission conductors, transformers, relay protective devices, terminal equipment, and series and shunt compensation devices.

3.4.2. The scope of Ratings addressed shall include, as a minimum, both Normal and Emergency Ratings.

M3. Each Transmission Owner shall have a documented Facility Ratings methodology that includes all of the items identified in Requirement 3, Parts 3.1 through 3.4.

R4. Reserved.

M4. Reserved.

R5. Reserved.

M5. Reserved.

R6. Each Transmission Owner and Generator Owner shall have Facility Ratings for its solely and jointly owned Facilities that are consistent with the associated Facility Ratings methodology or documentation for determining its Facility Ratings. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M6. Each Transmission Owner and Generator Owner shall have evidence to show that its Facility Ratings are consistent with the documentation for determining its Facility Ratings as specified in Requirement R1 or consistent with its Facility Ratings methodology as specified in Requirements R2 and R3 (Requirement R6).

R7. Reserved.

M7. Reserved.

[2] Such as temporary de-ratings of impaired equipment in accordance with good utility practice.

R8. Each Transmission Owner (and each Generator Owner subject to Requirement R2) shall provide requested information as specified below (for its solely and jointly owned Facilities that are existing Facilities, new Facilities, modifications to existing Facilities and re-ratings of existing Facilities) to its associated Reliability Coordinator(s), Planning Coordinator(s), Transmission Planner(s), Transmission Owner(s) and Transmission Operator(s): *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

8.1. As scheduled by the requesting entities:

8.1.1. Facility Ratings

8.1.2. Identity of the most limiting equipment of the Facilities

8.2. Within 30 calendar days (or a later date if specified by the requester), for any requested Facility with a Thermal Rating that limits the use of Facilities under the requester's authority by causing any of the following: 1) An Interconnection Reliability Operating Limit, 2) A limitation of Total Transfer Capability, 3) An impediment to generator deliverability, or 4) An impediment to service to a major load center:

8.2.1. Identity of the existing next most limiting equipment of the Facility

8.2.2. The Thermal Rating for the next most limiting equipment identified in Requirement R8, Part 8.2.1.

M8. Each Transmission Owner (and Generator Owner subject to Requirement R2) shall have evidence, such as a copy of a dated electronic note, or other comparable evidence to show that it provided its Facility Ratings and identity of limiting equipment to its associated Reliability Coordinator(s), Planning Coordinator(s), Transmission Planner(s), Transmission Owner(s) and Transmission Operator(s) in accordance with Requirement R8.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: "Compliance Enforcement Authority" means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Compliance Monitoring and Enforcement Processes:

- Self-Certifications
- Spot Checking
- Compliance Audits
- Self-Reporting

- Compliance Violation Investigations
- Complaints

1.3. Evidence Retention: The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

- The Generator Owner shall keep its current documentation (for R1) and any modifications to the documentation that were in force since last compliance audit period for Measure M1 and Measure M6.
- The Generator Owner shall keep its current, in force Facility Ratings methodology (for R2) and any modifications to the methodology that were in force since last compliance audit period for Measure M2 and Measure M6.
- The Transmission Owner shall keep its current, in force Facility Ratings methodology (for R3) and any modifications to the methodology that were in force since the last compliance audit for Measure M3 and Measure M6.
- The Transmission Owner and Generator Owner shall keep its current, in force Facility Ratings and any changes to those ratings for three calendar years for Measure M6.
- The Transmission Owner (and Generator Owner that is subject to Requirement R2) shall keep evidence for Measure M8 for three calendar years.
- If a Generator Owner or Transmission Owner is found non-compliant, it shall keep information related to the non-compliance until found compliant.
- The Compliance Enforcement Authority shall keep the last audit and all subsequent compliance records.

1.4. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	N/A	The Generator Owner's Facility Rating documentation did not address Requirement R1, Part 1.1.	The Generator Owner's Facility Rating documentation did not address Requirement R1, Part 1.2.	The Generator Owner failed to provide documentation for determining its Facility Ratings.
R2.	The Generator Owner failed to include in its Facility Rating methodology one of the following Parts of Requirement R2: • 2.1. • 2.2.1 • 2.2.2 • 2.2.3 • 2.2.4	The Generator Owner failed to include in its Facility Rating methodology two of the following Parts of Requirement R2: • 2.1 • 2.2.1 • 2.2.2 • 2.2.3 • 2.2.4	The Generator Owner's Facility Rating methodology did not address all the components of Requirement R2, Part 2.4. OR The Generator Owner failed to include in its Facility Rating Methodology, three of the following Parts of Requirement R2: • 2.1. • 2.2.1 • 2.2.2 • 2.2.3 • 2.2.4	The Generator Owner's Facility Rating methodology failed to recognize a facility's rating based on the most limiting component rating as required in Requirement R2, Part 2.3 OR The Generator Owner failed to include in its Facility Rating Methodology four or more of the following Parts of Requirement R2: • 2.1 • 2.2.1 • 2.2.2 • 2.2.3 • 2.2.4

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R3.	The Transmission Owner failed to include in its Facility Rating methodology one of the following Parts of Requirement R3: • 3.1 • 3.2.1 • 3.2.2 • 3.2.3 • 3.2.4	The Transmission Owner failed to include in its Facility Rating methodology two of the following Parts of Requirement R3: • 3.1 • 3.2.1 • 3.2.2 • 3.2.3 • 3.2.4	The Transmission Owner's Facility Rating methodology did not address either of the following Parts of Requirement R3: • 3.4.1 • 3.4.2 OR The Transmission Owner failed to include in its Facility Rating methodology three of the following Parts of Requirement R3: • 3.1 • 3.2.1 • 3.2.2 • 3.2.3 • 3.2.4	The Transmission Owner's Facility Rating methodology failed to recognize a Facility's rating based on the most limiting component rating as required in Requirement R3, Part 3.3 OR The Transmission Owner failed to include in its Facility Rating methodology four or more of the following Parts of Requirement R3: • 3.1 • 3.2.1 • 3.2.2 • 3.2.3 • 3.2.4
R4. Reserved.				
R5. Reserved.				

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R6.	The responsible entity failed to establish Facility Ratings consistent with the associated Facility Ratings methodology or documentation for determining the Facility Ratings for 5% or less of its solely owned and jointly owned Facilities. (R6)	The responsible entity failed to establish Facility Ratings consistent with the associated Facility Ratings methodology or documentation for determining the Facility Ratings for more than 5% or more, but less than up to (and including) 10% of its solely owned and jointly owned Facilities. (R6)	The responsible entity failed to establish Facility Ratings consistent with the associated Facility Ratings methodology or documentation for determining the Facility Ratings for more than 10% up to (and including) 15% of its solely owned and jointly owned Facilities. (R6)	The responsible entity failed to establish Facility Ratings consistent with the associated Facility Ratings methodology or documentation for determining the Facility Ratings for more than15% of its solely owned and jointly owned Facilities. (R6)
R7. Reserved.				
R8.	The responsible entity provided its Facility Ratings to all of the requesting entities but missed meeting the schedules by up to and including 15 calendar days. (R8, Part 8.1) OR The responsible entity provided less than 100%,	The responsible entity provided its Facility Ratings to all of the requesting entities but missed meeting the schedules by more than 15 calendar days but less than or equal to 25 calendar days. (R8, Part 8.1) OR The responsible entity provided less than 95%, but	The responsible entity provided its Facility Ratings to all of the requesting entities but missed meeting the schedules by more than 25 calendar days but less than or equal to 35 calendar days. (R8, Part 8.1) OR The responsible entity provided less than 90%, but	The responsible entity provided its Facility Ratings to all of the requesting entities but missed meeting the schedules by more than 35 calendar days. (R8, Part 8.1) OR The responsible entity provided less than 85% of the required Rating information to all of the

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	but not less than or equal to 95% of the required Rating information to all of the requesting entities. (R8, Part 8.1) OR The responsible entity provided the required Rating information to the requesting entity, but the information was provided up to and including 15 calendar days late. (R8, Part 8.2) OR The responsible entity provided less than 100%, but not less than or equal to 95% of the required Rating information to the requesting entity. (R8, Part 8.2)	not less than or equal to 90% of the required Rating information to all of the requesting entities. (R8, Part 8.1) OR The responsible entity provided the required Rating information to the requesting entity, but did so more 15 calendar days but less than or equal to 25 calendar days late. (R8, Part 8.2) OR The responsible entity provided less than 95%, but not less than or equal to 90% of the required Rating information to the requesting entity. (R8, Part 8.2)	not less than or equal to 85% of the required Rating information to all of the requesting entities. (R8, Part 8.1) OR The responsible entity provided the required Rating information to the requesting entity, but did so more than 25 calendar days but less than or equal to 35 calendar days late. (R8, Part 8.2) OR The responsible entity provided less than 90%, but no less than or equal to 85% of the required Rating information to the requesting entity. (R8, Part 8.2)	requesting entities. (R8, Part 8.1) OR The responsible entity provided the required Rating information to the requesting entity, but did so more than 35 calendar days late. (R8, Part 8.2) OR The responsible entity provided less than 85 % of the required Rating information to the requesting entity. (R8, Part 8.2) OR The responsible entity failed to provide its Rating information to the requesting entity. (R8, Part 8.1)

D. Regional Variances

None.

E. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	Feb 7, 2006	Approved by Board of Trustees	New
1	Mar 16, 2007	Approved by FERC	New
2	May 12, 2010	Approved by Board of Trustees	Complete Revision, merging FAC_008-1 and FAC-009-1 under Project 2009-06 and address directives from Order 693
3	May 24, 2011	Addition of Requirement R8	Project 2009-06 Expansion to address third directive from Order 693
3	May 24, 2011	Adopted by NERC Board of Trustees	
3	November 17, 2011	FERC Order issued approving FAC-008-3	
3	May 17, 2012	FERC Order issued directing the VRF for Requirement R2 be changed from “Lower” to “Medium”	
3	February 7, 2013	R4 and R5 and associated elements approved by NERC Board of Trustees for retirement as part of the Paragraph 81 project (Project 2013-02) pending applicable regulatory approval.	
3	November 21, 2013	R4 and R5 and associated elements approved by FERC for retirement as part of the Paragraph 81 project (Project 2013-02)	
4	May 9, 2020	R7 and R8 and associated elements adopted by NERC Board of Trustees for retirement as part of Project 2018-03 Standards Efficiency Review Retirements.	
4	September 17, 2020	Remanded by FERC (Order No. 873).	Withdrawn
5	February 4, 2021	Adopted by NERC Board of Trustees	Requirement R8 and associated elements restored in response

Version	Date	Action	Change Tracking
			to FERC Order No. 873.

Appendix FAC-008-5-QC-1
Specific provisions applicable in Québec for standard FAC-008-5 — Facility Ratings

This appendix establishes specific provisions for the application of the standard in Québec. Provisions of the standard and of this appendix must be read jointly for comprehension and interpretation purposes. Where the standard and appendix differ, the appendix shall prevail.

A. Introduction

1. Title: No specific provision

2. Number: No specific provision

3. Purpose: No specific provision

4. Applicability:

Functions

No specific provision

Facilities

This standard only applies to the facilities of the Main Transmission System (RTP)

5. Effective Date:

5.1. Adoption of the standard by the Régie de l'énergie: November 10, 2021

5.2. Adoption of the appendix by the Régie de l'énergie: November 10, 2021

5.3. Effective date of the standard and its appendix in Québec: April 1st, 2022

B. Requirements and Measures

No specific provision

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

In Québec, "Compliance Enforcement Authority" means the Régie de l'énergie in its roles of monitoring and enforcing compliance with respect to the Reliability Standard and to this appendix.

1.2. Compliance Monitoring and Enforcement Processes

The Régie de l'énergie establishes the monitoring processes used to evaluate data or information for the purpose of determining compliance or non-compliance with the Reliability Standard and with this appendixNo specific provision

1.3. Data Retention

No specific provision

1.4. Additional Compliance Information

No specific provision

2. Violation Severity Levels

No specific provision

D. Regional Differences

No specific provision

E. Associated Documents

No specific provision

Revision History

Revision	Adoption Date	Action	Change Tracking
1	November 10, 2021	New appendix adoption (D-2021-145)	New

A. Introduction

1. Title: **System Operating Limits Methodology for the Operations Horizon**

2. Number: FAC-011-3

3. Purpose: To ensure that System Operating Limits (SOLs) used in the reliable operation of the Bulk Electric System (BES) are determined based on an established methodology or methodologies.

4. Applicability

4.1. Reliability Coordinator

5. Effective Date: See Implementation Plan for the Revised Definition of "Remedial Action Scheme".

B. Requirements

R1. The Reliability Coordinator shall have a documented methodology for use in developing SOLs (SOL Methodology) within its Reliability Coordinator Area. This SOL Methodology shall:

R1.1. Be applicable for developing SOLs used in the operations horizon.

R1.2. State that SOLs shall not exceed associated Facility Ratings.

R1.3. Include a description of how to identify the subset of SOLs that qualify as IROLs.

R2. The Reliability Coordinator's SOL Methodology shall include a requirement that SOLs provide BES performance consistent with the following:

R2.1. In the pre-contingency state, the BES shall demonstrate transient, dynamic and voltage stability; all Facilities shall be within their Facility Ratings and within their thermal, voltage and stability limits. In the determination of SOLs, the BES condition used shall reflect current or expected system conditions and shall reflect changes to system topology such as Facility outages.

R2.2. Following the single Contingencies[1] identified in Requirement 2.2.1 through Requirement 2.2.3, the system shall demonstrate transient, dynamic and voltage stability; all Facilities shall be operating within their Facility Ratings and within their thermal, voltage and stability limits; and Cascading or uncontrolled separation shall not occur.

R2.2.1. Single line to ground or 3-phase Fault (whichever is more severe), with Normal Clearing, on any Faulted generator, line, transformer, or shunt device.

R2.2.2. Loss of any generator, line, transformer, or shunt device without a Fault.

R2.2.3. Single pole block, with Normal Clearing, in a monopolar or bipolar high voltage direct current system.

R2.3. In determining the system's response to a single Contingency, the following shall be acceptable:

[1] The Contingencies identified in FAC-011 R2.2.1 through R2.2.3 are the minimum contingencies that must be studied but are not necessarily the only Contingencies that should be studied.

R2.3.1. Planned or controlled interruption of electric supply to radial customers or some local network customers connected to or supplied by the Faulted Facility or by the affected area.

R2.3.2. Interruption of other network customers, (a) only if the system has already been adjusted, or is being adjusted, following at least one prior outage, or (b) if the real-time operating conditions are more adverse than anticipated in the corresponding studies

R2.3.3. System reconfiguration through manual or automatic control or protection actions.

R2.4. To prepare for the next Contingency, system adjustments may be made, including changes to generation, uses of the transmission system, and the transmission system topology.

R3. The Reliability Coordinator's methodology for determining SOLs, shall include, as a minimum, a description of the following, along with any reliability margins applied for each:

R3.1. Study model (must include at least the entire Reliability Coordinator Area as well as the critical modeling details from other Reliability Coordinator Areas that would impact the Facility or Facilities under study.)

R3.2. Selection of applicable Contingencies

R3.3. A process for determining which of the stability limits associated with the list of multiple contingencies (provided by the Planning Authority in accordance with FAC-014 Requirement 6) are applicable for use in the operating horizon given the actual or expected system conditions.

R3.3.1. This process shall address the need to modify these limits, to modify the list of limits, and to modify the list of associated multiple contingencies.

R3.4. Level of detail of system models used to determine SOLs.

R3.5. Allowed uses of Remedial Action Schemes.

R3.6. Anticipated transmission system configuration, generation dispatch and Load level

R3.7. Criteria for determining when violating a SOL qualifies as an Interconnection Reliability Operating Limit (IROL) and criteria for developing any associated IROL T_v.

R4. The Reliability Coordinator shall issue its SOL Methodology and any changes to that methodology, prior to the effectiveness of the Methodology or of a change to the Methodology, to all of the following:

R4.1. Each adjacent Reliability Coordinator and each Reliability Coordinator that indicated it has a reliability-related need for the methodology.

R4.2. Each Planning Authority and Transmission Planner that models any portion of the Reliability Coordinator's Reliability Coordinator Area.

R4.3. Each Transmission Operator that operates in the Reliability Coordinator Area.

C. Measures

M1. The Reliability Coordinator's SOL Methodology shall address all of the items listed in Requirement 1 through Requirement 3.

M2. The Reliability Coordinator shall have evidence it issued its SOL Methodology, and any changes to that methodology, including the date they were issued, in accordance with Requirement 4.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

Regional Reliability Organization

1.2. Compliance Monitoring Period and Reset Time Frame

Each Reliability Coordinator shall self-certify its compliance to the Compliance Monitor at least once every three years. New Reliability Authorities shall demonstrate compliance through an on-site audit conducted by the Compliance Monitor within the first year that it commences operation. The Compliance Monitor shall also conduct an on-site audit once every nine years and an investigation upon complaint to assess performance.

The Performance-Reset Period shall be twelve months from the last non-compliance.

1.3. Data Retention

The Reliability Coordinator shall keep all superseded portions to its SOL Methodology for 12 months beyond the date of the change in that methodology. In addition, entities found non-compliant shall keep information related to the non-compliance until found compliant

The Compliance Monitor shall keep the last audit and all subsequent compliance records.

1.4. Additional Compliance Information

The Reliability Coordinator shall make the following available for inspection during an on-site audit by the Compliance Monitor or within 15 business days of a request as part of an investigation upon complaint:

1.4.1 SOL Methodology.

1.4.2 Superseded portions of its SOL Methodology that had been made within the past 12 months.

1.4.3 Evidence that the SOL Methodology and any changes to the methodology that occurred within the past 12 months were issued to all required entities.

2. Levels of Non-Compliance for Western Interconnection: (To be replaced with VSLs once developed and approved by WECC)

2.1. Level 1: There shall be a level one non-compliance if either of the following conditions exists:

2.1.1 The SOL Methodology did not include a statement indicating that Facility Ratings shall not be exceeded.

2.2. Level 2: The SOL Methodology did not include a requirement to address all of the elements in R3.1, R3.2, R3.4 through R3.7 and E1.

2.3. Level 3: There shall be a level three non-compliance if any of the following conditions exists:

2.3.1 The SOL Methodology did not include a statement indicating that Facility Ratings shall not be exceeded and the methodology did not include evaluation of system response to one of the three types of single Contingencies identified in R2.2.

2.3.2 The SOL Methodology did not include a statement indicating that Facility Ratings shall not be exceeded and the methodology did not include evaluation of system response to two of the seven types of multiple Contingencies identified in E1.1.

2.3.3 The System Operating Limits Methodology did not include a statement indicating that Facility Ratings shall not be exceeded and the methodology did not address two of the six required topics in R3.1, R3.2, R3.4 through R3.7.

2.4. Level 4: The SOL Methodology was not issued to all required entities in accordance with R4.

3. Violation Severity Levels:

Requirement	Lower	Moderate	High	Severe
R1	Not applicable.	The Reliability Coordinator has a documented SOL Methodology for use in developing SOLs within its Reliability Coordinator Area, but it does not address R1.2	The Reliability Coordinator has a documented SOL Methodology for use in developing SOLs within its Reliability Coordinator Area, but it does not address R1.3.	The Reliability Coordinator has a documented SOL Methodology for use in developing SOLs within its Reliability Coordinator Area, but it does not address R1.1. OR The Reliability Coordinator has no documented SOL Methodology for use in developing SOLs within its Reliability Coordinator Area.
R2	The Reliability Coordinator's SOL Methodology requires that SOLs are set to meet BES performance following single contingencies, but does not require that SOLs are set to meet BES performance in the pre-contingency state. (R2.1)	Not applicable.	The Reliability Coordinator's SOL Methodology requires that SOLs are set to meet BES performance in the pre-contingency state, but does not require that SOLs are set to meet BES performance following single contingencies. (R2.2 – R2.4)	The Reliability Coordinator's SOL Methodology does not require that SOLs are set to meet BES performance in the pre-contingency state and does not require that SOLs are set to meet BES performance following single contingencies. (R2.1 through R2.4)
R3	The Reliability Coordinator's SOL Methodology includes a description for all but one of the following: R3.1 through R3.7.	The Reliability Coordinator's SOL Methodology includes a description for all but two of the following: R3.1 through R3.7.	The Reliability Coordinator's SOL Methodology includes a description for all but three of the following: R3.1 through R3.7.	The Reliability Coordinator's SOL Methodology is missing a description of four or more of the following: R3.1 through R3.7.
R3.6	N/A	N/A	N/A	N/A
R4	The Reliability Coordinator failed to issue its SOL Methodology and/or one or more changes to that methodology to one of the required entities specified in R4.1, R4.2, and R4.3.	The Reliability Coordinator failed to issue its SOL Methodology and/or one or more changes to that methodology to two of the required entities specified in R4.1, R4.2, and R4.3.	The Reliability Coordinator failed to issue its SOL Methodology and/or one or more changes to that methodology to three of the required entities specified in R4.1, R4.2, and R4.3.	The Reliability Coordinator failed to issue its SOL Methodology and/or one or more changes to that methodology to four or more of the required entities specified in R4.1, R4.2, and R4.3

Requirement	Lower	Moderate	High	Severe
	OR For a change in methodology, the changed methodology was provided to one or more of the required entities before the effectiveness of the change, but was provided to all the required entities no more than 10 calendar days after the effectiveness of the change.	OR For a change in methodology, the changed methodology was provided to one or more of the required entities more than 10 calendar days after the effectiveness of the change, but less than or equal to 20 days after the effectiveness of the change.	OR For a change in methodology, the changed methodology was provided to one or more of required entities more than 20 calendar days after the effectiveness of the change, but less than or equal to30 days after the effectiveness of the change.	OR For a change in methodology, the changed methodology was provided to one or more of the required entities more than30 calendar days after the effectiveness of the change.

Regional Differences

1. The following Interconnection-wide Regional Difference shall be applicable in the Western Interconnection:

1.1. As governed by the requirements of R3.3, starting with all Facilities in service, shall require the evaluation of the following multiple Facility Contingencies when establishing SOLs:

1.1.1 Simultaneous permanent phase to ground Faults on different phases of each of two adjacent transmission circuits on a multiple circuit tower, with Normal Clearing. If multiple circuit towers are used only for station entrance and exit purposes, and if they do not exceed five towers at each station, then this condition is an acceptable risk and therefore can be excluded.

1.1.2 A permanent phase to ground Fault on any generator, transmission circuit, transformer, or bus section with Delayed Fault Clearing except for bus sectionalizing breakers or bus-tie breakers addressed in E1.1.7

1.1.3 Simultaneous permanent loss of both poles of a direct current bipolar Facility without an alternating current Fault.

1.1.4 The failure of a circuit breaker associated with a Remedial Action Scheme to operate when required following: the loss of any element without a Fault; or a permanent phase to ground Fault, with Normal Clearing, on any transmission circuit, transformer or bus section.

1.1.5 A non-three phase Fault with Normal Clearing on common mode Contingency of two adjacent circuits on separate towers unless the event frequency is determined to be less than one in thirty years.

1.1.6 A common mode outage of two generating units connected to the same switchyard, not otherwise addressed by FAC-011.

1.1.7 The loss of multiple bus sections as a result of failure or delayed clearing of a bus tie or bus sectionalizing breaker to clear a permanent Phase to Ground Fault.

1.2. SOLs shall be established such that for multiple Facility Contingencies in E1.1.1 through E1.1.5 operation within the SOL shall provide system performance consistent with the following:

1.2.1 All Facilities are operating within their applicable Post-Contingency thermal, frequency and voltage limits.

1.2.2 Cascading does not occur.

1.2.3 Uncontrolled separation of the system does not occur.

1.2.4 The system demonstrates transient, dynamic and voltage stability.

1.2.5 Depending on system design and expected system impacts, the controlled interruption of electric supply to customers (load shedding), the planned removal from service of certain generators, and/or the curtailment of contracted firm (non-recallable reserved) electric power transfers may be necessary to maintain the overall security of the interconnected transmission systems.

1.2.6 Interruption of firm transfer, Load or system reconfiguration is permitted through manual or automatic control or protection actions.

1.2.7 To prepare for the next Contingency, system adjustments are permitted, including changes to generation, Load and the transmission system topology when determining limits.

1.3. SOLs shall be established such that for multiple Facility Contingencies in E1.1.6 through E1.1.7 operation within the SOL shall provide system performance consistent with the following with respect to impacts on other systems:

1.3.1 Cascading does not occur.

1.4. The Western Interconnection may make changes (performance category adjustments) to the Contingencies required to be studied and/or the required responses to Contingencies for specific facilities based on actual system performance and robust design. Such changes will apply in determining SOLs.

Version History

Version	Date	Action	Change Tracking
1	November 1, 2006	Adopted by Board of Trustees	New
2		Changed the effective date to October 1, 2008 Changed "Cascading Outage" to "Cascading" Replaced Levels of Non-compliance with Violation Severity Levels Corrected footnote 1 to reference FAC-011 rather than FAC-010	Revised
2	June 24, 2008	Adopted by Board of Trustees: FERC Order 705	Revised
2	January 22, 2010	Updated effective date and footer to April 29, 2009 based on the March 20, 2009 FERC Order	Update
2	February 7, 2013	R5 and associated elements approved by NERC Board of Trustees for retirement as part of the Paragraph 81 project (Project 2013-02) pending applicable regulatory approval.	
2	November 21, 2013	R5 and associated elements approved by FERC for retirement as part of the Paragraph 81 project (Project 2013-02)	
2	February 24, 2014	Updated VSLs based on June 24, 2013 approval.	
3	November 13, 2014	Adopted by the NERC Board of Trustees	Replaced references to Special Protection System and SPS with Remedial Action Scheme and RAS
3	November 19, 2015	FERC Order issued approving FAC-011-3. Docket No. RM15-13-000.	

Appendix FAC-011-3-QC-1

Specific provisions applicable in Québec for standard FAC-011-3 – System Operating Limits Methodology for the Operating Horizon

This appendix establishes specific provisions for the application of the standard in Québec. Provisions of the standard and of this appendix must be read jointly for comprehension and interpretation purposes. Where the standard and appendix differ, the appendix shall prevail.

A. Introduction

1. Title: No specific provisions.

2. Number: No specific provisions.

3. Purpose: No specific provisions.

4. Applicability:

4.1. Functional Entities

No specific provisions.

4.2. Facilities

The Facilities subject to this standard are the Facilities of the Main Transmission System (RTP).

5. Effective date:

5.1.	Adoption of the standard by the Régie de l'énergie:	June 16, 2021
5.2.	Adoption of this appendix by the Régie de l'énergie:	June 16, 2021
5.3.	Effective date of the standard and of this appendix in Québec:	October 1st, 2021

B. Requirements

All occurrences of "BES" are replaced with "RTP".

Specific provisions applicable to Requirement R2.2.1:

Requirement R2.2.1 applies as stipulated in the standard, except for RTP Facilities operating at less than 230 kV that were not substantially modified after January 1, 2019 for which Requirement R2.2.1 is replaced by the following:

R2.2.1 Single line to ground with Normal Clearing, on any Faulted generator, line, transformer, or shunt device. This specific provision will be in force for a period of fifteen (15) years following the FAC-011-3 standard adoption date.

With respect to owners of generation Facilities for industrial use (PVI), Requirement R2.2.1 does not apply to RTP Facilities operating at 230 kV and more that were not substantially modified after January 1, 2019 for which Requirement R2.2.1 is replaced by the following:

R2.2.1 Single line to ground with Normal Clearing, on any Faulted generator, line, transformer, or shunt device. This specific provision will be in force for a period of eight (8) years following the FAC-011-3 standard adoption date.

C. Measures

No specific provisions.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

In Québec, "Compliance Enforcement Authority" means the Régie de l'énergie in its roles of monitoring and enforcing compliance with respect to the Reliability Standard and to this appendix.

1.2. Compliance Monitoring Period and Reset Time Frame

No specific provisions.

1.3. Data Retention

No specific provisions.

1.4. Additional Compliance Information

No specific provisions.

2. Levels of Non-Compliance for Western Interconnection: (To be replaced with VSLs once developed and approved by WECC)

No specific provisions.

3. Violation Severity Levels

All occurrences of "BES" are replaced with "RTP".

Regional Differences

No specific provisions.

Version history

Version	Date	Action	Change tracking
1	June 16, 2021	New appendix	New

A. Introduction

1. **Title:** **Establish and Communicate System Operating Limits**

2. **Number:** FAC-014-2

3. **Purpose:** To ensure that System Operating Limits (SOLs) used in the reliable planning and operation of the Bulk Electric System (BES) are determined based on an established methodology or methodologies.

4. **Applicability**

   4.1. Reliability Coordinator

   4.2. Planning Authority

   4.3. Transmission Planner

   4.4. Transmission Operator

5. **Effective Date:** April 29, 2009

B. Requirements

R1. The Reliability Coordinator shall ensure that SOLs, including Interconnection Reliability Operating Limits (IROLs), for its Reliability Coordinator Area are established and that the SOLs (including Interconnection Reliability Operating Limits) are consistent with its SOL Methodology.

R2. The Transmission Operator shall establish SOLs (as directed by its Reliability Coordinator) for its portion of the Reliability Coordinator Area that are consistent with its Reliability Coordinator's SOL Methodology.

R3. The Planning Authority shall establish SOLs, including IROLs, for its Planning Authority Area that are consistent with its SOL Methodology.

R4. The Transmission Planner shall establish SOLs, including IROLs, for its Transmission Planning Area that are consistent with its Planning Authority's SOL Methodology.

R5. The Reliability Coordinator, Planning Authority and Transmission Planner shall each provide its SOLs and IROLs to those entities that have a reliability-related need for those limits and provide a written request that includes a schedule for delivery of those limits as follows:

R5.1. The Reliability Coordinator shall provide its SOLs (including the subset of SOLs that are IROLs) to adjacent Reliability Coordinators and Reliability Coordinators who indicate a reliability-related need for those limits, and to the Transmission Operators, Transmission Planners, Transmission Service Providers and Planning Authorities within its Reliability Coordinator Area. For each IROL, the Reliability Coordinator shall provide the following supporting information:

R5.1.1. Identification and status of the associated Facility (or group of Facilities) that is (are) critical to the derivation of the IROL.

R5.1.2. The value of the IROL and its associated T_v.

R5.1.3. The associated Contingency(ies).

R5.1.4. The type of limitation represented by the IROL (e.g., voltage collapse, angular stability).

R5.2. The Transmission Operator shall provide any SOLs it developed to its Reliability Coordinator and to the Transmission Service Providers that share its portion of the Reliability Coordinator Area.

R5.3. The Planning Authority shall provide its SOLs (including the subset of SOLs that are IROLs) to adjacent Planning Authorities, and to Transmission Planners, Transmission Service Providers, Transmission Operators and Reliability Coordinators that work within its Planning Authority Area.

R5.4. The Transmission Planner shall provide its SOLs (including the subset of SOLs that are IROLs) to its Planning Authority, Reliability Coordinators, Transmission Operators, and Transmission Service Providers that work within its Transmission Planning Area and to adjacent Transmission Planners.

R6. The Planning Authority shall identify the subset of multiple contingencies (if any), from Reliability Standard TPL-003 which result in stability limits.

R6.1. The Planning Authority shall provide this list of multiple contingencies and the associated stability limits to the Reliability Coordinators that monitor the facilities associated with these contingencies and limits.

R6.2. If the Planning Authority does not identify any stability-related multiple contingencies, the Planning Authority shall so notify the Reliability Coordinator.

C. Measures

M1. The Reliability Coordinator, Planning Authority, Transmission Operator, and Transmission Planner shall each be able to demonstrate that it developed its SOLs (including the subset of SOLs that are IROLs) consistent with the applicable SOL Methodology in accordance with Requirements 1 through 4.

M2. The Reliability Coordinator, Planning Authority, Transmission Operator, and Transmission Planner shall each have evidence that its SOLs (including the subset of SOLs that are IROLs) were supplied in accordance with schedules supplied by the requestors of such SOLs as specified in Requirement 5.

M3. The Planning Authority shall have evidence it identified a list of multiple contingencies (if any) and their associated stability limits and provided the list and the limits to its Reliability Coordinators in accordance with Requirement 6.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

Regional Reliability Organization

1.2. Compliance Monitoring Period and Reset Time Frame

The Reliability Coordinator, Planning Authority, Transmission Operator, and Transmission Planner shall each verify compliance through self-certification submitted to its Compliance Monitor annually. The Compliance Monitor may conduct a targeted audit once in each calendar year (January – December) and an investigation upon a complaint to assess performance.

The Performance-Reset Period shall be twelve months from the last finding of non-compliance.

1.3. Data Retention

The Reliability Coordinator, Planning Authority, Transmission Operator, and Transmission Planner shall each keep documentation for 12 months. In addition, entities found non-compliant shall keep information related to non-compliance until found compliant.

The Compliance Monitor shall keep the last audit and all subsequent compliance records.

1.4. Additional Compliance Information

The Reliability Coordinator, Planning Authority, Transmission Operator, and Transmission Planner shall each make the following available for inspection during a targeted audit by the Compliance Monitor or within 15 business days of a request as part of an investigation upon complaint:

1.4.1 SOL Methodology(ies)

1.4.2 SOLs, including the subset of SOLs that are IROLs and the IROLs supporting information

1.4.3 Evidence that SOLs were distributed

1.4.4 Evidence that a list of stability-related multiple contingencies and their associated limits were distributed

1.4.5 Distribution schedules provided by entities that requested SOLs

2. Violation Severity Levels:

Requirement	Lower	Moderate	High	Severe
R1	There are SOLs, for the Reliability Coordinator Area, but from 1% up to but less than 25% of these SOLs are inconsistent with the Reliability Coordinator's SOL Methodology. (R1)	There are SOLs, for the Reliability Coordinator Area, but 25% or more, but less than 50% of these SOLs are inconsistent with the Reliability Coordinator's SOL Methodology. (R1)	There are SOLs, for the Reliability Coordinator Area, but 50% or more, but less than 75% of these SOLs are inconsistent with the Reliability Coordinator's SOL Methodology. (R1)	There are SOLs for the Reliability Coordinator Area, but 75% or more of these SOLs are inconsistent with the Reliability Coordinator's SOL Methodology. (R1)
R2	The Transmission Operator has established SOLs for its portion of the Reliability Coordinator Area, but from 1% up to but less than 25% of these SOLs are inconsistent with the Reliability Coordinator's SOL Methodology. (R2)	The Transmission Operator has established SOLs for its portion of the Reliability Coordinator Area, but 25% or more, but less than 50% of these SOLs are inconsistent with the Reliability Coordinator's SOL Methodology. (R2)	The Transmission Operator has established SOLs for its portion of the Reliability Coordinator Area, but 50% or more, but less than 75% of these SOLs are inconsistent with the Reliability Coordinator's SOL Methodology. (R2)	The Transmission Operator has established SOLs for its portion of the Reliability Coordinator Area, but 75% or more of these SOLs are inconsistent with the Reliability Coordinator's SOL Methodology. (R2)
R3	There are SOLs, for the Planning Coordinator Area, but from 1% up to, but less than, 25% of these SOLs are inconsistent with the Planning Coordinator's SOL Methodology. (R3)	There are SOLs, for the Planning Coordinator Area, but 25% or more, but less than 50% of these SOLs are inconsistent with the Planning Coordinator's SOL Methodology. (R3)	There are SOLs for the Planning Coordinator Area, but 50% or more, but less than 75% of these SOLs are inconsistent with the Planning Coordinator's SOL Methodology. (R3)	There are SOLs, for the Planning Coordinator Area, but 75% or more of these SOLs are inconsistent with the Planning Coordinator's SOL Methodology. (R3)
R4	The Transmission Planner has established SOLs for its portion of the Planning Coordinator Area, but up to 25% of these SOLs are inconsistent with the Planning Coordinator's SOL Methodology. (R4)	The Transmission Planner has established SOLs for its portion of the Planning Coordinator Area, but 25% or more, but less than 50% of these SOLs are inconsistent with the Planning Coordinator's SOL Methodology. (R4)	The Transmission Planner has established SOLs for its portion of the Reliability Coordinator Area, but 50% or more, but less than 75% of these SOLs are inconsistent with the Planning Coordinator's SOL Methodology. (R4)	The Transmission Planner has established SOLs for its portion of the Planning Coordinator Area, but 75% or more of these SOLs are inconsistent with the Planning Coordinator's SOL Methodology. (R4)
R5	The responsible entity provided its SOLs (including the subset of SOLs that are IROLs) to all the requesting entities but missed meeting one or more of the schedules by less than 15	One of the following: The responsible entity provided its SOLs (including the subset of SOLs that are IROLs) to all but one of the requesting entities within the schedules provided.	One of the following: The responsible entity provided its SOLs (including the subset of SOLs that are IROLs) to all but two of the requesting entities within the schedules provided.	One of the following: The responsible entity failed to provide its SOLs (including the subset of SOLs that are IROLs) to more than two of the requesting entities within 45

Requirement	Lower	Moderate	High	Severe
	calendar days. (R5)	(R5) Or The responsible entity provided its SOLs to all the requesting entities but missed meeting one or more of the schedules for 15 or more but less than 30 calendar days. (R5) OR The supporting information provided with the IROLs does not address 5.1.4	(R5) Or The responsible entity provided its SOLs to all the requesting entities but missed meeting one or more of the schedules for 30 or more but less than 45 calendar days. (R5) OR The supporting information provided with the IROLs does not address 5.1.3	calendar days of the associated schedules. (R5) OR The supporting information provided with the IROLs does not address 5.1.1 and 5.1.2.
R6	The Planning Authority failed to notify the Reliability Coordinator in accordance with R6.2	Not applicable.	The Planning Authority identified the subset of multiple contingencies which result in stability limits **but** did not provide the list of multiple contingencies and associated limits to one Reliability Coordinator that monitors the Facilities associated with these limits. (R6.1)	The Planning Authority did not identify the subset of multiple contingencies which result in stability limits. (R6) OR The Planning Authority identified the subset of multiple contingencies which result in stability limits **but** did not provide the list of multiple contingencies and associated limits to more than one Reliability Coordinator that monitors the Facilities associated with these limits. (R6.1)

E. Regional Differences

None identified.

Version History

Version	Date	Action	Change Tracking
1	November 1, 2006	Adopted by Board of Trustees	New
2		Changed the effective date to January 1, 2009 Replaced Levels of Non-compliance with Violation Severity Levels	Revised
2	June 24, 2008	Adopted by Board of Trustees: FERC Order	Revised
2	January 22, 2010	Updated effective date and footer to April 29, 2009 based on the March 20, 2009 FERC Order	Update

Appendix QC-FAC-014-2
Provisions specific to the standard FAC-014-2 applicable in Québec

This appendix establishes specific provisions for the application of the standard in Québec. Provisions of the standard and of its appendix must be read together for the purposes of understanding and interpretation. Where the standard and appendix differ, the appendix shall prevail.

A. Introduction

1. Title: **Establish and Communicate System Operating Limits**

2. Number: FAC-014-2

3. Purpose: No specific provision

4. Applicability:

Functions

No specific provision

Facilities

This standard only applies to the facilities of the Main Transmission System (RTP)

5. Effective Date:

5.1. Adoption of the standard by the Régie de l'énergie: October 30, 2013

5.2. Adoption of the appendix by the Régie de l'énergie: October 30, 2013

5.3. Effective date of the standard and its appendix in Québec: January 1, 2016

B. Requirements

No specific provision

C. Measures

No specific provision

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

The Régie de l'énergie is responsible, in Québec, for compliance monitoring with respect to the reliability standard and its appendix that it adopts.

1.2. Compliance Monitoring Period and Reset Time Frame

No specific provision

1.3. Data Retention

No specific provision

1.4. Additional Compliance Information

No specific provision

2. Violation Severity Levels

No specific provision

E. Regional Differences

No specific provision

Revision History

Revision	Adoption Date	Action	Change Tracking
0	October 30, 2013	New appendix	New

A. Introduction

1. **Title:** Evaluation of Interchange Transactions
2. **Number:** INT-006-5
3. **Purpose:** To ensure that responsible entities conduct a reliability assessment of each Arranged Interchange before it is implemented.
4. **Applicability:**
   - **4.1.** Balancing Authority
   - **4.2.** Transmission Service Provider
5. **Effective Date:** See Implementation Plan.

B. Requirements and Measures

R1. Each Balancing Authority shall approve or deny each on-time Arranged Interchange or emergency Arranged Interchange that it receives and shall do so prior to the expiration of the time period defined in Attachment 1, Column B. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning, Same-day Operations, Real-time Operations]*

1.1. Each Source and Sink Balancing Authority shall deny the Arranged Interchange or curtail Confirmed Interchange if it does not expect to be capable of supporting the magnitude of the Interchange, including ramping, throughout the duration of the Arranged Interchange.

1.2. Each Balancing Authority shall deny the Arranged Interchange or curtail Confirmed Interchange if the Scheduling Path (proper connectivity of Adjacent Balancing Authorities) between it and its Adjacent Balancing Authorities is invalid.

M1. Each Balancing Authority shall have evidence (such as dated and time stamped electronic logs, or other evidence) that it responded to each request for its approval to transition an Arranged Interchange to a Confirmed Interchange within the time defined in Attachment 1, Column B. (R1)

R2. Each Transmission Service Provider shall approve or deny each on-time Arranged Interchange or emergency Arranged Interchange that it receives and shall do so prior to the expiration of the time period defined in Attachment 1, Column B. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning, Same-day Operations, Real-time Operations]*

2.1. Each Transmission Service Provider shall deny the Arranged Interchange or curtail Confirmed Interchange if the transmission path (proper connectivity of adjacent Transmission Service Providers) between it and its adjacent Transmission Service Providers is invalid.

M2. Each Transmission Service Provider shall have evidence (such as dated and time stamped electronic logs, studies, or other evidence) that it responded to each Arranged Interchange or emergency Arranged Interchange within the time defined in Attachment 1, Column B. If the transmission path between the Transmission Service Provider and its adjacent Transmission Service Providers is invalid, each Transmission Service Provider shall have evidence (such as dated and time stamped electronic logs, studies, or other evidence) that it denied the Arranged Interchange or curtailed confirmed Interchange. (R2)

R3. The Source Balancing Authority and the Sink Balancing Authority receiving a Reliability Adjustment Arranged Interchange shall approve or deny it prior to the expiration of the time period defined in Attachment 1, Column B. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning, Same-day Operations, Real-time Operations]*

M3. Each Balancing Authority shall have evidence (such as dated and time stamped electronic logs, studies, or other evidence) that when responding to a Reliability Adjustment Arranged Interchange, it either approved the request or denied the request.

R4. Reserved.

M4. Reserved.

R5. Reserved.

M5. Reserved.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: "Compliance Enforcement Authority" means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

- The Balancing Authority shall maintain evidence to show compliance with R1 and R3 for the most recent three calendar months plus the current month.
- The Transmission Service Provider shall maintain evidence to show compliance with R2 for the most recent three calendar months plus the current month.
- If a Balancing Authority or Transmission Service Provider is found non-compliant, it shall keep information related to the non-compliance until found compliant.

The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or

information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

- Compliance Audits
- Self-Certifications
- Spot Checking
- Compliance Investigations
- Self-Reporting
- Complaint

Violation Severity Levels

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	Operations Planning, Same-day Operations, Real-time Operations	Lower	N/A	N/A	N/A	The Balancing Authority receiving an on-time Arranged Interchange or an emergency Arranged Interchange did not approve or deny it prior to the expiration of the time period defined in Attachment 1, Column B. OR The Source or Sink Balancing Authority did not expect to be capable of supporting the magnitude of the Interchange, including ramping, throughout duration of the Arranged Interchange and did not deny the Arranged Interchange or curtail Confirmed Interchange. OR The Scheduling Path between the Balancing

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						Authority and its Adjacent Balancing Authorities was invalid, and the Balancing Authority did not deny the Arranged Interchange or curtail Confirmed Interchange.
R2.	Operations Planning, Same-day Operations, Real-time Operations	Lower	N/A	N/A	N/A	The Transmission Service Provider receiving an on-time Arranged Interchange or an emergency Arranged Interchange did not approve or deny it prior to the expiration of the time period defined in Attachment 1, Column B. OR The transmission path between the Transmission Service Provider and its adjacent Transmission Service Providers was invalid, and the Transmission

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						Service Provider did not deny the Arranged Interchange or curtail Confirmed Interchange.
R3.	Operations Planning, Same-day Operations, Real-time Operations	Lower	N/A	N/A	The Source Balancing Authority or Sink Balancing Authority receiving a Reliability Adjustment Arranged Interchange denied it prior to the expiration of the time period defined in Attachment 1, Column B.	The Source Balancing Authority or Sink Balancing Authority receiving a Reliability Adjustment Arranged Interchange did not approve or deny it prior to the expiration of the time period defined in Attachment 1, Column B.
R4. Reserved.						
R5. Reserved.						

D. Regional Variances

None.

E. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	May 2, 2006	Adopted by the NERC Board Of Trustees	New
2	May 2, 2007	Adopted by the NERC Board Of Trustees	Revised
3	October 29, 2008	Adopted by the NERC Board Of Trustees	Revised
3	July 1, 2010	Approved by FERC	Revised
4	February 6, 2014	Adopted by the NERC Board Of Trustees	Revised
4	June 30, 2014	FERC letter order issued approving INT-006-4	
5	May 9, 2019	Adopted by the NERC Board of Trustees	Requirements R3.1, R4, and R5 retired under Project 2018-03 Standard Efficiency Review Retirements.
5	September 17, 2020	FERC Order issued approving INT-006-5. Docket No. RM19-16-000, RM19-17-000	

Timing Tables

Timing Requirements for all Interconnections except WECC

		A	B	C	D
If Arranged Interchange [1] is Submitted	**Time Classification**	**Sink BA Makes Initial Distribution of Arranged Interchange [2]**	**BA and TSP Conduct Reliability Assessments**	**Compilation and Distribution Status[2]**	**BA Prepares Confirmed Interchange for Implementation**
>1 hour after the start time	ATF		Entities have up to 2 hours to respond.		NA
<15 minutes prior to ramp start and ≤1 hour after the start time	Late		Entities have up to 10 minutes to respond.		≤ 3 minutes after receipt of Confirmed Interchange
<1 hour and ≥ 15 minutes prior to ramp start	On-time		≤ 10 minutes from Arranged Interchange receipt		≥ 3 minutes prior to ramp start
≥1 hour to < 4 hours prior to ramp start	On-time		≤ 20 minutes from Arranged Interchange receipt		≥ 39 minutes prior to ramp start
≥ 4 hours prior to ramp start	On-time		≤ 2 hours from Arranged Interchange receipt		≥ 1 hour 58 minutes prior to ramp start

[1] Time Classifications and deadlines apply to both initial Arranged Interchange submittal and any subsequent modifications to the Arranged Interchange.

[2] See NAESB WEQ004. The times are being retained in the NAESB tables but are removed here since they are not being referenced in requirements.

Timing Tables

Timing Requirements for WECC

		A	B	C	D
If Arranged Interchange [3] is Submitted	**Time Classification**	**Sink BA Makes Initial Distribution of Arranged Interchange [4]**	**BA and TSP Conduct Reliability Assessments**	**Compilation and Distribution Status[4]**	**BA Prepares Confirmed Interchange for Implementation**
>1 hour after the start time	ATF		Entities have up to 2 hours to respond.		NA
<10 minutes prior to ramp start and ≤1 hour after transaction start time where transaction start time is at the top of the hour	Late		Entities have up to 10 minutes to respond.		≤ 3 minutes after receipt of Confirmed Interchange
<15 minutes prior to ramp start and ≤1 hour after transaction start time where transaction start time is not the top of the hour	Late		Entities have up to 10 minutes to respond.		≤ 3 minutes after receipt of Confirmed Interchange

[3] Time Classifications and deadlines apply to both initial Arranged Interchange submittal and any subsequent modifications to the Arranged Interchange.

[4] See NAESB WEQ004. The times are being retained in the NAESB tables but are removed here since they are not being referenced in requirements.

		A	B	C	D
If Arranged Interchange [3] is Submitted	**Time Classification**	**Sink BA Makes Initial Distribution of Arranged Interchange [4]**	**BA and TSP Conduct Reliability Assessments**	**Compilation and Distribution Status[4]**	**BA Prepares Confirmed Interchange for Implementation**
10 minutes prior to ramp start where transaction start time is at the top of the hour	On-time		≤ 5 minutes from Arranged Interchange receipt		≥ 3 minutes prior to ramp start
11 minutes prior to ramp start where transaction start time is at the top of the hour	On-time		≤ 6 minutes from Arranged Interchange receipt		≥ 3 minutes prior to ramp start
12 minutes prior to ramp start where transaction start time is at the top of the hour	On-time		≤ 7 minutes from Arranged Interchange receipt		≥ 3 minutes prior to ramp start
13 minutes prior to ramp start where transaction start time is at the top of the hour	On-time		≤ 8 minutes from Arranged Interchange receipt		≥ 3 minutes prior to ramp start

		A	B	C	D
If Arranged Interchange [3] is Submitted	**Time Classification**	**Sink BA Makes Initial Distribution of Arranged Interchange [4]**	**BA and TSP Conduct Reliability Assessments**	**Compilation and Distribution Status[4]**	**BA Prepares Confirmed Interchange for Implementation**
14 minutes prior to ramp start where transaction start time is at the top of the hour	On-time		≤ 9 minutes from Arranged Interchange receipt		≥ 3 minutes prior to ramp start
<1 hour and ≥ 15 minutes prior to ramp start	On-time		≤ 10 minutes from Arranged Interchange receipt		≥ 3 minutes prior to ramp start
≥ 1 hour and < 4 hours prior to ramp start	On-time		< 20 minutes from Arranged interchange receipt		≥ 39 minutes prior to ramp start
≥ 4 hours prior to ramp start	On-time		≤ 2 hours from Arranged Interchange receipt		≥ 1 hour 58 minutes prior to ramp start
Submitted before 10:00 PPT with start time ≥ 00:00 PPT of following day	On-time		By 12:00 PPT of day the Arranged Interchange was received		≥ 1 hour 58 minutes prior to ramp start

Guidelines and Technical Basis

Many aspects of managing Interchange are supported by software applications. There are fundamental tasks that each entity should be able to perform in an electronic manner as listed below.

A Load-Serving Entity and Balancing Authority that submits Requests for Interchange should have the capability to electronically:

- Submit a Request for Interchange to a Sink Balancing Authority
- Submit a request to modify Interchange
- Receive distributions of Confirmed Interchange
- Receive distributions of Reliability Adjustment Arranged Interchanges

Each Sink Balancing Authority should have the capability to electronically:

- Receive a Request for Interchange
- Receive a request to modify Interchange
- Validate Requests for Interchange by verifying:
  - Source Balancing Authority megawatts equal Sink Balancing Authority megawatts (adjusted for losses, if appropriate).
  - All reliability entities involved in the Arranged Interchange are valid.
  - Generation source and Load sink are defined.
  - Megawatt profile is defined.
  - Interchange duration is defined.
- Validate request to modify Interchange by verifying:
  - Source Balancing Authority megawatts equal Sink Balancing Authority megawatts (adjusted for losses, if appropriate).
  - Megawatt profile is defined.
  - Interchange duration is defined.
- Distribute the validated Request for Interchange as Arranged Interchange
- Distribute the validated Reliability Adjustment Arranged Interchanges
- Receive communication of approval or denial of Arranged Interchange
  - Distribute notification as each entity approves or denies an Arranged Interchange.
  - Transition Arranged Interchange to Confirmed Interchange if all approvals are received.
  - Distribute notification of whether Arranged Interchange was transitioned to Confirmed Interchange or not.

  - Submit a request to modify Interchange

- Each Load-Serving Entity that approves or denies Arranged Interchange, and each Balancing Authority and Transmission Service Provider should have the capability to electronically:
  - Receive distribution of Arranged Interchange
  - Communicate approval or denial of the Arranged Interchange to the Sink Balancing Authority
  - Receive notification of whether Arranged Interchange was transitioned to Confirmed interchange or not.
  - Submit a request to modify Interchange
- While Interchange is normally facilitated using electronic communication and software tools, there are occasions with those electronic capabilities are reduced or unavailable. It is recommended that all entities involved in aspects of Interchange should have, maintain and implement a plan describing the manner and timing in which all capabilities listed above will be provided when electronic capabilities are reduced or unavailable. Each plan should address the following topics:
  - Alternate methods of communicating Interchange information between Purchasing Selling Entities, Balancing Authorities, and Transmission Service Providers.
  - How to notify others that it is activating the plan
  - How it will process requests for emergency Arranged Interchange and Reliability Adjustment Arranged Interchange.
  - Restrictions and limitations that may apply during the period of reduced or unavailable capability (such as limits on volume, only accepting emergency transactions, etc.).
  - Delegation of approval rights and proxy actions, if such approaches will be used.
  - How known Confirmed Interchange will be scheduled following a reduction in or loss of capability.
  - Personnel plans for short-term and extended periods.
  - Training of personnel in the use of the plan.

Rationale:

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for R1:

Balancing Authorities must take action on a received Arranged Interchange within a certain time frame. Requirement R1, Parts 1.1 and 1.2 provide reliability-related reasons that a Balancing Authority must deny an Arranged Interchange, but Balancing Authorities may deny

for other reasons. If the conditions described in Requirement R1, Parts 1.1 or 1.2 are recognized after approval is granted, the Balancing Authority may curtail the Confirmed Interchange prior to implementation.

Rationale for R2:
TSPs must take action on a received Arranged Interchange within a certain time frame. Requirement R2, Part 2.1 provides reliability-related reasons that a TSP must deny an Arranged Interchange, but TSPs may deny for other reasons. If the conditions described in Requirement R1, Part 2.1 are recognized after approval is granted, the TSP may curtail the Confirmed Interchange prior to implementation.

Appendix INT-006-5-QC-1
Specific provisions applicable in Québec for standard INT-006-5 – Evaluation of Interchange Transaction

This appendix establishes specific provisions for the application of the standard in Québec. Provisions of the standard and of this appendix must be read jointly for comprehension and interpretation purposes. Where the standard and appendix differ, the appendix shall prevail.

A. Introduction

1. **Title:** No specific provisions.
2. **Number:** No specific provisions.
3. **Purpose:** No specific provisions.
4. **Applicability:** No specific provisions.
5. **Effective Date:**

5.1. Adoption of the standard by the Régie de l'énergie: May 4, 2021

5.2. Adoption of the appendix by the Régie de l'énergie: May 4, 2021

5.3. Effective date of the standard and its appendix in Québec: October 1st, 2021

B. Requirements and Measures

No specific provisions.

C. Compliance

1. **Compliance Monitoring Process**

1.1. **Compliance Enforcement Authority**

In Québec, "Compliance Enforcement Authority" means the Régie de l'énergie in its roles of monitoring and enforcing compliance with respect to the Reliability Standard and to this appendix.

1.2. **Evidence Retention**

No specific provisions.

1.3. **Compliance Monitoring and Enforcement Program**

The Régie de l'énergie establishes the monitoring processes used to evaluate data or information for the purpose of determining compliance or non-compliance with the Reliability Standard and with this appendix.

Violation Severity Levels

No specific provisions.

D. Regional Variances

No specific provisions.

E. Associated Documents

No specific provisions.

Attachment 1- Timing Tables

No specific provisions.

Guidelines and technical basis

No specific provisions.

Version History

Version	Date	Action	Change Tracking
1	May 4, 2021	New appendix adoption (D-2021-058)	New

A. Introduction

1. **Title:** Implementation of Interchange
2. **Number:** INT-009-3
3. **Purpose:** To ensure that Balancing Authorities implement the Interchange as agreed upon in the Interchange confirmation process.
4. **Applicability:**
   - **4.1.** Balancing Authority
5. **Effective Date:** See Implementation Plan

B. Requirements and Measures

R1. Each Balancing Authority shall agree with each of its Adjacent Balancing Authorities that its Composite Confirmed Interchange with that Adjacent Balancing Authority, at mutually agreed upon time intervals, excluding Dynamic Schedules and Pseudo-Ties and including any Interchange not yet captured in the Composite Confirmed Interchange, is: [*Violation Risk Factor: Medium*] [*Time Horizon: Real-time Operations*]

1.1. Identical in magnitude to that of the Adjacent Balancing Authority, and

1.2. Opposite in sign or direction to that of the Adjacent Balancing Authority.

M1. The Balancing Authority shall have evidence (such as dated logs, voice recordings, electronic records, or other evidence) that its Composite Confirmed Interchange, excluding Dynamic Schedules and Pseudo-Ties and including any Interchange not yet captured in the Composite Confirmed Interchange, was agreed to by each Adjacent Balancing Authority, identical in magnitude to those of each Adjacent Balancing Authority, and opposite in sign to that of each Adjacent Balancing Authority. (R1)

R2. Reserved.

M2. Reserved.

R3. Each Balancing Authority in whose area the high-voltage direct current tie is controlled shall coordinate the Confirmed Interchange prior to its implementation with the Transmission Operator of the high-voltage direct current tie. [*Violation Risk Factor: Medium*] [*Time Horizon: Real-time Operations, Operations Planning*]

M3. The Balancing Authority shall have evidence (such as dated logs, electronic records, or other evidence) that it coordinated the Confirmed Interchange prior to its implementation with the Transmission Operator of the high-voltage direct current tie. (R3)

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: "Compliance Enforcement Authority" means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

- The Balancing Authority shall maintain evidence to show compliance with R1 and R3 for the most recent 3 months plus the current month.

If a Balancing Authority is found non-compliant, it shall keep information related to the non-compliance until found compliant.

The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

Violation Severity Levels

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	Real-time Operations	Medium	N/A	N/A	N/A	The Balancing Authority did not reach agreement with an Adjacent Balancing Authority on the magnitude or sign of its Composite Confirmed Interchange, at mutually agreed upon time intervals, excluding Dynamic Schedules and Pseudo-Ties and including any Interchange not yet captured in the Composite Confirmed Interchange.
R2. Reserved.						
R3.	Real-time Operations, Operations Planning	Medium	N/A	N/A	N/A	The Balancing Authority failed to coordinate the Confirmed Interchange prior to its implementation with the Transmission Operator of the high-voltage direct current tie.

D. Regional Variances

None.

E. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
0	April 1, 2005	Effective Date	New
1	May 2, 2006	Adopted by the NERC Board of Trustees	Revised
2	February 6, 2014	Adopted by the NERC Board of Trustees	Revised
2	June 30, 2014	FERC letter order issued approving INT-009-2	
2.1	August 22, 2014	Errata submitted for INT-004-3, INT-009-2, INT-010-2 and INT-011-2 to correct inconsistency between the Implementation Plan and the effective date language. The NERC Standards Committee approved errata changes on August 20, 2014.	Errata
2.1	November 26, 2014	FERC letter order approving errata changes.	
3	May 9, 2019	Adopted by NERC Board of Trustees	Requirement R2 retired under Project 2018-03 Standard Efficiency Review Retirements.
3	September 17, 2020	FERC Order issued approving INT-009-3. Docket No. RM19-16-000, RM19-17-000	

Appendix INT-009-3-QC-1
Specific provisions applicable in Québec for standard INT-009-3 – Implementation of Interchange

This appendix establishes specific provisions for the application of the standard in Québec. Provisions of the standard and of this appendix must be read jointly for comprehension and interpretation purposes. Where the standard and appendix differ, the appendix shall prevail.

A. Introduction

1. **Title:** No specific provisions.
2. **Number:** No specific provisions.
3. **Purpose:** No specific provisions.
4. **Applicability:** No specific provisions.
5. **Effective Date:**

   5.1. Adoption of the standard by the Régie de l'énergie: May 4, 2021

   5.2. Adoption of the appendix by the Régie de l'énergie: May 4, 2021

   5.3. Effective date of the standard and its appendix in Québec: October 1st, 2021

B. Requirements and Measures

No specific provisions.

C. Compliance

1. **Compliance Monitoring Process**

   1.1. **Compliance Enforcement Authority**

   In Québec, "Compliance Enforcement Authority" means the Régie de l'énergie in its roles of monitoring and enforcing compliance with respect to the Reliability Standard and to this appendix.

   1.2. **Evidence Retention**

   No specific provisions.

   1.3. **Compliance Monitoring and Enforcement Program**

   The Régie de l'énergie establishes the monitoring processes used to evaluate data or information for the purpose of determining compliance or non-compliance with the Reliability Standard and with this appendix.

Violation Severity Levels

No specific provisions.

D. Regional Variances

No specific provisions.

E. Associated Documents

No specific provisions.

Appendix INT-009-3-QC-1
Specific provisions applicable in Québec for standard INT-009-3 – Implementation of Interchange

Version History

Version	Date	Action	Change Tracking
1	May 4, 2021	New appendix adoption (D-2021-058)	New

A. Introduction

1. **Title**: Reliability Coordination – Responsibilities

2. **Number**: IRO-001-4

3. **Purpose:** To establish the responsibility of Reliability Coordinators to act or direct other entities to act.

4. **Applicability**

   4.1. Reliability Coordinator

   4.2. Transmission Operator

   4.3. Balancing Authority

   4.4. Generator Operator

   4.5. Distribution Provider

5. **Effective Date:**

   See Implementation Plan.

6. **Background:**

   See the Project 2014-03 project page.

B. Requirements and Measures

R1. Each Reliability Coordinator shall act to address the reliability of its Reliability Coordinator Area via direct actions or by issuing Operating Instructions. *[Violation Risk Factor: High][Time Horizon: Same-Day Operations, Real-time Operations]*

M1. Each Reliability Coordinator shall have and provide evidence which may include but is not limited to dated operator logs, dated records, dated and time-stamped voice recordings or dated transcripts of voice recordings, electronic communications, or equivalent documentation, that will be used to determine that it acted to address the reliability of its Reliability Coordinator Area via direct actions or by issuing Operating Instructions.

R2. Each Transmission Operator, Balancing Authority, Generator Operator, and Distribution Provider shall comply with its Reliability Coordinator's Operating Instructions unless compliance with the Operating Instructions cannot be physically implemented or unless such actions would violate safety, equipment, regulatory, or statutory requirements. *[Violation Risk Factor: High] [Time Horizon: Same-Day Operations, Real-time Operations]*

M2. Each Transmission Operator, Balancing Authority, Generator Operator, and Distribution Provider shall have and provide evidence which may include but is not limited to dated operator logs, dated records, dated and time-stamped voice recordings or dated transcripts of voice recordings, electronic communications, or

equivalent documentation, that will be used to determine that it complied with its Reliability Coordinator's Operating Instructions, unless the instruction could not be physically implemented, or such actions would have violated safety, equipment, regulatory or statutory requirements. In such cases, the Transmission Operator, Balancing Authority, Generator Operator, or Distribution Provider shall have and provide copies of the safety, equipment, regulatory, or statutory requirements as evidence for not complying with the Reliability Coordinator's Operating Instructions. If such a situation has not occurred, the Transmission Operator, Balancing Authority, Generator Operator, or Distribution Provider may provide an attestation.

R3. Each Transmission Operator, Balancing Authority, Generator Operator, and Distribution Provider shall inform its Reliability Coordinator of its inability to perform the Operating Instruction issued by its Reliability Coordinator in Requirement R1. *[Violation Risk Factor: High] [Time Horizon: Same-Day Operations, Real-time Operations]*

M3. Each Transmission Operator, Balancing Authority, Generator Operator, and Distribution Provider shall have and provide evidence which may include but is not limited to dated operator logs, dated records, dated and time-stamped voice recordings or dated transcripts of voice recordings, electronic communications, or equivalent documentation, that will be used to determine that it informed its Reliability Coordinator of its inability to perform an Operating Instruction issued by its Reliability Coordinator in Requirement R1.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Compliance Monitoring and Assessment Processes:

As defined in the NERC Rules of Procedure, "Compliance Monitoring and Assessment Processes" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated reliability standard.

1.3. Data Retention

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to

provide other evidence to show that it was compliant for the full time period since the last audit.

The Reliability Coordinator, Transmission Operator, Balancing Authority, Generator Operator, and Distribution Provider shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation:

- The Reliability Coordinator for Requirement R1, Measure M1 shall retain voice recordings for the most recent 90-calendar days and documentation for the most recent 12-calendar months.
- The Transmission Operator, Balancing Authority, Generator Operator, and Distribution Provider for Requirements R2 and R3, Measures M2 and M3 shall retain voice recordings for the most recent 90-calendar days and documentation for the most recent 12-calendar months.

If a Reliability Coordinator, Transmission Operator, Balancing Authority, Generator Operator, or Distribution Provider is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.

The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

1.4. Additional Compliance Information

None.

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	Same-Day Operations, Real-time Operations	High	N/A	N/A	N/A	The Reliability Coordinator failed to act to address the reliability of its Reliability Coordinator Area via direct actions or by issuing Operating Instructions.
R2	Same-Day Operations, Real-time Operations	High	N/A	N/A	N/A	The responsible entity did not comply with the Reliability Coordinator's Operating Instructions, and compliance with the Operating Instructions could have been physically implemented and such actions would not have violated safety, equipment, regulatory, or statutory requirements.
R3	Same-Day Operations, Real-time Operations	High	N/A	N/A	N/A	The responsible entity failed to inform its Reliability Coordinator upon recognition of its inability to perform an Operating Instruction issued by its Reliability Coordinator in Requirement R1 .

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
0	April 1, 2005	Effective Date	New
0	August 8, 2005	Removed "Proposed" from Effective Date	Errata
1	November 1, 2006	Adopted by Board of Trustees	Revised
1	November 19, 2006	Changes "Distribution Provider" to "Transmission Service provider"	Errata
1	April 4, 2007	Approved by FERC – Effective Date	New
1.1	October 29, 2008	Removed "proposed" from effective date BOT adopted errata changes: updated version number to "1.1"	Errata
1.1	May 13, 2009	FERC Approval	Revised
1	May 19, 2011	Replaced Levels of Noncompliance with FERC-approved VSLs	VSL Order
2	July 25, 2011	Revisions under Project 2006-06 to remove Requirement R7 to avoid duplication with IRO-014-2	Revised
2	August 4, 2011	Adopted by Board of Trustees	
3	July 6, 2012	Revised in accordance with SAR for Project 2006-06, Reliability Coordination (RC SDT). Revised the standard and retired six requirements (R1, R2, R4, R5, R6, and R9).	Revised

		Requirement R3 becomes the new R1 and R8 becomes the new R2 and R3.	
3	August 16, 2012	Adopted by Board of Trustees	Revised
4	November 13, 2014	Adopted by Board of Trustees	Revisions under Project 2014-03

Guidelines and Technical Basis

Rationale:

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for Applicability:
Purchasing-Selling Entity and Load-Serving Entity have been deleted from the approved IRO-001-1.1 as they are not listed as entities that the Reliability Coordinator directs in Functional Model v5.

Rationale for Change from Reliability Directive to Operating Instruction:
The change from Reliability Directive to Operating Instruction throughout the standard is in response to NOPR paragraph 64 (…"*We believe that directives from a reliability coordinator or transmission operator should be mandatory at all times, and not just during emergencies (unless contrary to safety, equipment, regulatory or statutory requirements). For example, mandatory compliance with directives in non-emergency situations is important when a decision is made to alter or maintain the state of an element on the interconnected transmission network…*") This change is also consistent with the proposed COM-002-4.

Rationale for Requirements R2 and R3:
The Transmission Service Provider has been removed from Requirements R2 and R3 as the Transmission Service Provider is not listed in the Functional Model as a recipient of corrective actions issued by the Reliability Coordinator. This allows for the retirement of IRO-004-2.

*** FOR INFORMATIONAL PURPOSES ONLY ***

Enforcement Dates: Standard IRO-001-4 — Reliability Coordination - Responsibilities and Authorities

United States

Standard	Requirement	Enforcement Date	Inactive Date
IRO-001-4	All		

This standard has not yet been approved by the applicable regulatory authority.

Printed On: March 24, 2015, 08:20 AM

Appendix QC-IRO-001-4
Provisions specific to the standard IRO-001-4 applicable in Québec

This appendix establishes specific provisions for the application of the standard in Québec. Provisions of the standard and of its appendix must be read together for the purposes of understanding and interpretation. Where the standard and appendix differ, the appendix shall prevail.

A. Introduction

1. Title: **Reliability Coordination — Responsibilities**

2. Number: IRO-001-4

3. Purpose: No specific provision

4. Applicability:

Functions

No specific provision

Facilities

This standard only applies to the facilities of the Main Transmission System (RTP).

5. Effective Date:

5.1. Adoption of the standard by the Régie de l'énergie: June 16, 2017

5.2. Adoption of the appendix by the Régie de l'énergie: June 16, 2017

5.3. Effective date of the standard and its appendix in Québec: July 1st, 2017

6. Background

No specific provision

B. Requirements and Measures

No specific provision

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

The Régie de l'énergie is responsible, in Québec, for compliance monitoring with respect to the reliability standard and its appendix that it adopts.

1.2. Compliance Monitoring and Assessment Processes

Compliance Audit

Self-Certification

Spot Check

Compliance Investigation

Non-Compliance Self-Reporting

Periodic Data Submittal

Exception Reporting

Investigation following a complaint

1.3. Data Retention

No specific provision

1.4. Additional Compliance Information

No specific provision

2. Table of Compliance Elements

No specific provision

D. Regional Variances

No specific provision

E. Interpretations

No specific provision

F. Associated Documents

No specific provision

Guidelines and Technical Basis

No specific provision

Version History

Version	Date	Action	Change Tracking
0	June 16, 2017	New appendix	New

A. Introduction

1. **Title:** Reliability Coordination – Monitoring and Analysis
2. **Number:** IRO-002-7
3. **Purpose:** To provide System Operators with the capabilities necessary to monitor and analyze data needed to perform their reliability functions.
4. **Applicability:**
   - **4.1. Functional Entities:**
     - **4.1.1.** Reliability Coordinators
5. **Effective Date:** See Implementation Plan

B. Requirements and Measures

R1. Reserved.

M1. Reserved.

R2. Each Reliability Coordinator shall have data exchange capabilities, with redundant and diversely routed data exchange infrastructure within the Reliability Coordinator's primary Control Center, for the exchange of Real-time data with its Balancing Authorities and Transmission Operators, and with other entities it deems necessary, for performing its Real-time monitoring and Real-time Assessments. *[Violation Risk Factor: High] [Time Horizon: Same-Day Operations, Real-time Operations]*

M2. Each Reliability Coordinator shall have, and provide upon request, evidence that could include, but is not limited to, system specifications, system diagrams, or other documentation that lists its data exchange capabilities, including redundant and diversely routed data exchange infrastructure within the Reliability Coordinator's primary Control Center, for the exchange of Real-time data with its Balancing Authorities and Transmission Operators, and with other entities it deems necessary, as specified in the requirement.

R3. Each Reliability Coordinator shall test its primary Control Center data exchange capabilities specified in Requirement R2 for redundant functionality at least once every 90 calendar days. If the test is unsuccessful, the Reliability Coordinator shall initiate action within two hours to restore redundant functionality. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. Each Reliability Coordinator shall have, and provide upon request, evidence that it tested its primary Control Center data exchange capabilities specified in Requirement R2 for redundant functionality, or experienced an event that demonstrated the redundant functionality; and if the test was unsuccessful, initiated action within two hours to restore redundant functionality as specified in Requirement R3. Evidence

could include, but is not limited to: dated and time-stamped test records, operator logs, voice recordings, or electronic communications.

R4. Each Reliability Coordinator shall provide its System Operators with the authority to approve planned outages and maintenance of its telecommunication, monitoring and analysis capabilities. *[Violation Risk Factor: High] [Time Horizon: Operations Planning, Same-Day Operations, Real-time Operations]*

M4. Each Reliability Coordinator shall have, and provide upon request evidence that could include, but is not limited to, a documented procedure or equivalent evidence that will be used to confirm that the Reliability Coordinator has provided its System Operators with the authority to approve planned outages and maintenance of its telecommunication, monitoring and analysis capabilities.

R5. Each Reliability Coordinator shall monitor Facilities, the status of Remedial Action Schemes, and non-BES facilities identified as necessary by the Reliability Coordinator, within its Reliability Coordinator Area and neighboring Reliability Coordinator Areas to identify any System Operating Limit exceedances and to determine any Interconnection Reliability Operating Limit exceedances within its Reliability Coordinator Area. *[Violation Risk Factor: High] [Time Horizon: Real-Time Operations]*

M5. Each Reliability Coordinator shall have, and provide upon request, evidence that could include, but is not limited to, Energy Management System description documents, computer printouts, SCADA data collection, or other equivalent evidence that will be used to confirm that it has monitored Facilities, the status of Remedial Action Schemes, and non-BES facilities identified as necessary by the Reliability Coordinator, within its Reliability Coordinator Area and neighboring Reliability Coordinator Areas to identify any System Operating Limit exceedances and to determine any Interconnection Reliability Operating Limit exceedances within its Reliability Coordinator Area.

R6. Each Reliability Coordinator shall have monitoring systems that provide information utilized by the Reliability Coordinator's operating personnel, giving particular emphasis to alarm management and awareness systems, automated data transfers, and synchronized information systems, over a redundant infrastructure. *[Violation Risk Factor: High] [Time Horizon: Real-time Operations]*

M6. The Reliability Coordinator shall have, and provide upon request, evidence that could include, but is not limited to, Energy Management System description documents, computer printouts, SCADA data collection, or other equivalent evidence that will be used to confirm that it has monitoring systems consistent with the requirement.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority:

"Compliance Enforcement Authority" means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention:

The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

- The Reliability Coordinator shall retain its current, in force document and any documents in force for the current year and previous calendar year for Requirements R2 and R4 and Measures M2 and M4.
- The Reliability Coordinator shall retain evidence for Requirement R3 and Measure M3 for the most recent 12 calendar months, with the exception of operator logs and voice recordings which shall be retained for a minimum of 90 calendar days.
- The Reliability Coordinator shall keep data or evidence for Requirements R5 and R6 and Measures M5 and M6 for the current calendar year and one previous calendar year.

1.3. Compliance Monitoring and Enforcement Program

As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1. Reserved.				
R2.	N/A	N/A	The Reliability Coordinator had data exchange capabilities with its Balancing Authorities and Transmission Operators, and with other entities it deems necessary, for performing Real-time monitoring and Real-time Assessments, but did not have redundant and diversely routed data exchange infrastructure within the Reliability Coordinator's primary Control Center, as specified in the requirement.	The Reliability Coordinator did not have data exchange capabilities with its Balancing Authorities and Transmission Operators, and with other entities it deems necessary, for performing Real-time monitoring and Real-time Assessments as specified in the requirement.
R3.	The Reliability Coordinator tested its primary Control Center data exchange capabilities specified in Requirement R2 for	The Reliability Coordinator tested its primary Control Center data exchange capabilities specified in Requirement R2 for	The Reliability Coordinator tested its primary Control Center data exchange capabilities specified in Requirement R2 for	The Reliability Coordinator tested its primary Control Center data exchange capabilities specified in Requirement R2 for

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	redundant functionality, but did so more than 90 calendar days but less than or equal to 120 calendar days since the previous test; OR The Reliability Coordinator tested its primary Control Center data exchange capabilities specified in Requirement R2 for redundant functionality at least once every 90 calendar days but, following an unsuccessful test, initiated action to restore the redundant functionality in more than 2 hours and less than or equal to 4 hours.	redundant functionality, but did so more than 120 calendar days but less than or equal to 150 calendar days since the previous test; OR The Reliability Coordinator tested its primary Control Center data exchange capabilities specified in Requirement R2 for redundant functionality at least once every 90 calendar days but, following an unsuccessful test, initiated action to restore the redundant functionality in more than 4 hours and less than or equal to 6 hours.	redundant functionality, but did so more than 150 calendar days but less than or equal to 180 calendar days since the previous test; OR The Reliability Coordinator tested its primary Control Center data exchange capabilities specified in Requirement R2 for redundant functionality at least once every 90 calendar days but, following an unsuccessful test, initiated action to restore the redundant functionality in more than 6 hours and less than or equal to 8 hours.	redundant functionality, but did so more than 180 calendar days since the previous test; OR The Reliability Coordinator did not test its primary Control Center data exchange capabilities specified in Requirement R2 for redundant functionality; OR The Reliability Coordinator tested its primary Control Center data exchange capabilities specified in Requirement R2 for redundant functionality at least once every 90 calendar days but, following an unsuccessful test, did not initiate action within 8 hours to restore the redundant functionality.

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R4.	N/A	N/A	N/A	The Reliability Coordinator failed to provide its System Operator with the authority to approve planned outages and maintenance of its telecommunication, monitoring and analysis capabilities.
R5.	N/A	N/A	N/A	The Reliability Coordinator did not monitor Facilities, the status of Remedial Action Schemes, and non-BES facilities identified as necessary by the Reliability Coordinator, within its Reliability Coordinator Area and neighboring Reliability Coordinator Areas to identify any System Operating Limit exceedances and to determine any Interconnection Reliability Operating Limit exceedances within its Reliability Coordinator Area.

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R6.	N/A	N/A	N/A	The Reliability Coordinator did not have monitoring systems that provide information utilized by the Reliability Coordinator's operating personnel, giving particular emphasis to alarm management and awareness systems, automated data transfers, and synchronized information systems, over a redundant infrastructure.

D. Regional Variance

A. Regional Variance for the Western Electricity Coordinating Council Region

The following Interconnection-wide variance shall be applicable in the Western Electricity Coordinating Council (WECC) region.

Purpose
To develop a methodology that creates models for performing Operational Planning Analyses and Real-time Assessments.

Applicability
As used in this WECC Regional Variance, Reliability Coordinator is specific to those Reliability Coordinators providing Reliability Coordinator service(s) to entities operating within the Western Interconnection, regardless of where the Reliability Coordinator may be located.

Requirements and Measures

D.A.7. Each Reliability Coordinator shall, in coordination with other Reliability Coordinators, develop a common Interconnection-wide methodology to determine the modeling and monitoring of BES and non-BES Elements that are internal and external to its Reliability Coordinator Area, necessary for providing operational awareness of the impacts on Bulk Electric System Facilities within its Reliability Coordinator Area, including at a minimum: *([Violation Risk Factor: High] [Time Horizon: Operations Planning])*

- **D.A.7.1.** A method for development, maintenance, and periodic review of a Western Interconnection-wide reference model to serve as the baseline from which Reliability Coordinator's operational models are derived;
- **D.A.7.2.** The impacts of Inter-area oscillations;
- **D.A.7.3.** A method to determine Contingencies included in analyses and assessments;
- **D.A.7.4.** A method to determine Remedial Action Schemes included in analyses and assessments;
- **D.A.7.5.** A method to determine forecast data included in analyses and assessments; and
- **D.A.7.6.** A method for the validation and periodic review of the Reliability Coordinator's operational model for steady state and dynamic/oscillatory system response.

M.D.A.7. Each Reliability Coordinator will have evidence that it developed a common Western Interconnection-wide methodology, addressing modeling and

monitoring, in coordination with other Reliability Coordinators, that includes the features required in D.A.7.

D.A.8. Each Reliability Coordinator shall use the methodology developed in D.A.7. ([*Violation Risk Factor: High] [Time Horizon: Operations Planning*])

M.D.A.8. Each Reliability Coordinator will have evidence that it uses the methodology developed in D.A.7., as required in D.A.8. above.

Compliance

Evidence Retention:

- The Reliability Coordinator shall keep data or evidence for Requirements R5, R6, and the WECC Regional Variance, and Measures M5, M6, and the WECC Regional Variance for the current calendar year and one previous calendar year.

R #	Violation Severity Levels for the WECC Regional Variance			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
D.A.7.				The Reliability Coordinator did not develop the methodology as required in D.A.7.
D.A.8.				The Reliability Coordinator did not implement the methodology as required in D.A.8.

E. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
0	April 1, 2005	Effective Date	New
0	August 8, 2005	Removed "Proposed" from Effective Date	Errata
1	November 1, 2006	Adopted by Board of Trustees	Revised
1	April 4, 2007	Replaced Levels of Non-compliance with the Feb 28, BOT approved Violation Severity Levels (VSLs) Corrected typographical errors in BOT approved version of VSLs	Revised to add missing measures and compliance elements
2	October 17, 2008	Adopted by NERC Board of Trustees	Deleted R2, M3 and associated compliance elements as conforming changes associated with approval of IRO-010-1. Revised as part of IROL Project
2	March 17, 2011	Order issued by FERC approving IRO-002-2 (approval effective 5/23/11)	FERC approval
2	February 24, 2014	Updated VSLs based on June 24, 2013 approval.	VSLs revised
3	July 25, 2011	Revised under Project 2006-06	Revised
3	August 4, 2011	Approved by Board of Trustees	Retired R1-R8 under Project 2006-06.
4	November 13, 2014	Approved by Board of Trustees	Revisions under Project 2014-03
4	November 19, 2015	FERC approved IRO-002-4. Docket No. RM15-16-000	FERC approval
5	February 9, 2017	Adopted by Board of Trustees	Revised

5	April 17, 2017	FERC letter Order approved IRO-002-5. Docket No. RD17-4-000	
6	May 9, 2019	Adopted by the NERC Board of Trustees	WECC Regional Variance
7	May 9, 2019	Adopted by the NERC Board of Trustees	Requirement R1 retired as part of Project 2018-03 Standards Efficiency Review Retirements.
7	September 17, 2020	FERC Order issued approving IRO-002-7. Docket No. RM19-16-000, RM19-17-000	

Guidelines and Technical Basis

None.

Rationale

Rationale text from the development of IRO-002-4 in Project 2014-03 and IRO-002-5 in Project 2016-01 follows. Additional information can be found on the Project 2014-03 project page and the Project 2016-01 project page.

Changes made to the proposed definitions were made in order to respond to issues raised in NOPR paragraphs 55, 73, and 74 dealing with analysis of SOLs in all time horizons, questions on Protection Systems and Special Protection Systems in NOPR paragraph 78, and recommendations on phase angles from the SW Outage Report (recommendation 27). The intent of such changes is to ensure that Real-time Assessments contain sufficient details to result in an appropriate level of situational awareness. Some examples include: 1) analyzing phase angles which may result in the implementation of an Operating Plan to adjust generation or curtail transactions so that a Transmission facility may be returned to service, or 2) evaluating the impact of a modified Contingency resulting from the status change of a Special Protection Scheme from enabled/in-service to disabled/out-of-service.

Rationale for Requirements:
The data exchange elements of Requirements R1 and R2 from approved IRO-002-2 have been added back into proposed IRO-002-4 in order to ensure that there is no reliability gap. The Project 2014-03 SDT found no proposed requirements in the current project that covered the issue. Voice communication is covered in proposed COM-001-2 but data communications needs to remain in IRO-002-4 as it is not covered in proposed COM-001-2. Staffing of communications and facilities in corresponding requirements from IRO-002-2 is addressed in approved PER-004-2, Requirement R1 and has been deleted from this draft.

Rationale for R2:
Requirement R2 from IRO-002-3 has been deleted because approved EOP-008-1, Requirement R1, part 1.6.2 addresses redundancy and back-up concerns for outages of analysis tools. New Requirement R4 (R6 in IRO-002-5) has been added to address NOPR paragraphs 96 and 97: *"…As we explain above, the reliability coordinator's obligation to monitor SOLs is important to reliability because a SOL can evolve into an IROL during deteriorating system conditions, and for potential system conditions such as this, the reliability coordinator's monitoring of SOLs provides a necessary backup function to the transmission operator…."*

Rationale for Requirements R1 and R2: (*note*: R1 proposed for retirement in IRO-002-7 as part of Project 2018-03 Standard Efficiency Review Retirements)
The proposed changes address directives for redundancy and diverse routing of data exchange capabilities (FERC Order No. 817 Para 47).

Redundant and diversely routed data exchange capabilities consist of data exchange infrastructure components (e.g., switches, routers, servers, power supplies, and network cabling and communication paths between these components in the primary Control Center for the exchange of system operating data) that will provide continued functionality despite failure or malfunction of an individual component within the Reliability Coordinator's (RC) primary

Control Center. Redundant and diversely routed data exchange capabilities preclude single points of failure in primary Control Center data exchange infrastructure from halting the flow of Real-time data. Requirement R2 does not require automatic or instantaneous fail-over of data exchange capabilities. Redundancy and diverse routing may be achieved in various ways depending on the arrangement of the infrastructure or hardware within the RC's primary Control Center.

The reliability objective of redundancy is to provide for continued data exchange functionality during outages, maintenance, or testing of data exchange infrastructure. For periods of planned or unplanned outages of individual data exchange components, the proposed requirements do not require additional redundant data exchange infrastructure components solely to provide for redundancy.

Infrastructure that is not within the RC's primary Control Center is not addressed by the proposed requirement.

Rationale for Requirement R3:
The revised requirement addresses directives for testing of data exchange capabilities used in primary Control Centers (FERC Order No. 817 Para 51).

A test for redundant functionality demonstrates that data exchange capabilities will continue to operate despite the malfunction or failure of an individual component (e.g., switches, routers, servers, power supplies, and network cabling and communication paths between these components in the primary Control Center for the exchange of system operating data). An entity's testing practices should, over time, examine the various failure modes of its data exchange capabilities. When an actual event successfully exercises the redundant functionality, it can be considered a test for the purposes of the proposed requirement.

Rationale for R4 (R6 in IRO-002-5 and IRO-002-7):
The requirement was added back from approved IRO-002-2 as the Project 2014-03 SDT found no proposed requirements that covered the issues.

Appendix IRO-002-7-QC-1

Specific provisions applicable in Québec for standard IRO-002-7 – Reliability Coordination – Monitoring and Analysis

This appendix establishes specific provisions for the application of the standard in Québec. Provisions of the standard and of this appendix must be read jointly for comprehension and interpretation purposes. Where the standard and appendix differ, the appendix shall prevail.

A. Introduction

1. Title: No specific provisions.

2. Number: No specific provisions.

3. Purpose: No specific provisions.

4. Applicability:

4.1. Functional Entities

No specific provisions.

The applicable facilities for this standard are the facilities of the Main Transmission System (RTP) and, for requirement R5, the facilities designated under this requirement.

5. Effective date:

5.1. Adoption of the standard by the Régie de l'énergie: March 10, 2022

5.2. Adoption of this appendix by the Régie de l'énergie: March 10, 2022

5.3. Effective date of the standard and of this appendix in Québec: April 1st, 2022
All requirements become effective on August 1, 2022

B. Requirements and Measures

Specific provisions applicable to Requirement R5 and Measure M5:

The expression "non BES" is replaced by "non RTP" only for the Facilities in Québec that are within the Reliability Coordinator's Area..

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

In Québec, "Compliance Enforcement Authority" means the Régie de l'énergie in its roles of monitoring and enforcing compliance with respect to the Reliability Standard and to this appendix.

1.2. Evidence Retention

No specific provisions.

1.3. Compliance Monitoring and Enforcement Program

The Régie de l'énergie establishes the monitoring processes used to evaluate data or information for the purpose of determining compliance or non-compliance with the Reliability Standard and with this appendix.

Violation Severity Levels

The expression “non BES” is replaced by “non RTP” only for the Facilities in Québec that are within the Reliability Coordinator’s Area.

D. Regional Variances

No specific provisions.

E. Associated Documents

No specific provisions.

Guidelines and Technical Basis

No specific provisions.

Rationale

No specific provisions.

Version history

Version	Date	Action	Change tracking
1	March 10, 2022	New appendix as per decision D-2022-031.	New

A. Introduction

1. **Title:** **Reliability Coordination — Transmission Loading Relief (TLR)**
2. **Number:** **IRO-006-5**
3. **Purpose:** To ensure coordinated action between Interconnections when implementing Interconnection-wide transmission loading relief procedures to prevent or manage potential or actual SOL and IROL exceedances to maintain reliability of the bulk electric system.
4. **Applicability:**

   4.1. Reliability Coordinator.

   4.2. Balancing Authority.
5. **Proposed Effective Date:** First day of the first calendar quarter following the date this standard is approved by applicable regulatory authorities, or in those jurisdictions where regulatory approval is not required; the standard becomes effective on the first day of the first calendar quarter after the date this standard is approved by the NERC Board of Trustees.

B. Requirements

R1. Each Reliability Coordinator and Balancing Authority that receives a request pursuant to an Interconnection-wide transmission loading relief procedure (such as Eastern Interconnection TLR, WECC Unscheduled Flow Mitigation, or congestion management procedures from the ERCOT Protocols) from any Reliability Coordinator, Balancing Authority, or Transmission Operator in another Interconnection to curtail an Interchange Transaction that crosses an Interconnection boundary shall comply with the request, unless it provides a reliability reason to the requestor why it cannot comply with the request. [*Violation Risk Factor: High*] [*Time Horizon: Real-time Operations*]

C. Measures

M1. Each Reliability Coordinator and Balancing Authority shall provide evidence (such as dated logs, voice recordings, Tag histories, and studies, in electronic or hard copy format) that, when a request to curtail an Interchange Transaction crossing an Interconnection boundary pursuant to an Interconnection-wide transmission loading relief procedure was made from another Reliability Coordinator, Balancing Authority, or Transmission Operator in that other Interconnection, it complied with the request or provided a reliability reason why it could not comply with the request (R1).

D. Compliance

1. **Compliance Monitoring Process**

   1.1. Compliance Enforcement Authority

   Regional Entity.

   1.2. Compliance Monitoring and Enforcement Processes:

The following processes may be used:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.3. Data Retention

The Reliability Coordinator and Balancing Authority shall each keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation:

- The Reliability Coordinator and Balancing Authority shall maintain evidence to show compliance with R1 for the most recent twelve calendar months plus the current month.
- If a Reliability Coordinator or Balancing Authority is found non-compliant, it shall keep information related to the non-compliance until found compliant or for the duration specified above, whichever is longer.

The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

1.4. Additional Compliance Information

None.

Violation Severity Levels

R #	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1				The responsible entity received a request to curtail an Interchange Transaction crossing an Interconnection boundary pursuant to an Interconnection-wide transmission loading relief procedure from a Reliability Coordinator, Balancing Authority, or Transmission Operator, but the entity neither complied with the request, nor provided a reliability reason why it could not comply with the request.

E. Variances

None.

F. Associated Documents

None.

G. Version History

Version	Date	Action	Change Tracking
0	April 1, 2005	Effective Date	New
0	August 8, 2005	Removed "Proposed" from Effective Date	Errata
1	August 8, 2005	Revised Attachment 1	Revision
3	February 26, 2007	Revised Purpose and Attachment 1 related to NERC NAESB split of the TLR procedure	Revision
4	October 23, 2007	Completed NERC/NAESB split	Revision
5	TBD	Removed Attachment 1 and made into a new standard, eliminated unnecessary requirements.	Revision
5	November 4, 2010	Approved by the Board of Trustees	
5	April 21, 2011	FERC Order issued approving IRO-006-5 (approval effective June 27, 2011)	

Appendix QC-IRO-006-5
Provisions specific to the standard IRO-006-5 applicable in Québec

This appendix establishes specific provisions for the application of the standard in Québec. Provisions of the standard and of its appendix must be read together for the purposes of understanding and interpretation. Where the standard and appendix differ, the appendix shall prevail.

A. Introduction

1. Title: **Reliability Coordination — Transmission Loading Relief (TLR)**

2. Number: IRO-006-5

3. Purpose: No specific provision

4. Applicability: No specific provision

5. Effective Date:

5.1. Adoption of the standard by the Régie de l'énergie: May 4, 2015

5.2. Adoption of the appendix by the Régie de l'énergie: May 4, 2015

5.3. Effective date of the standard and its appendix in Québec: January 1, 2016

B. Requirements

No specific provision

C. Measures

No specific provision

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

The Régie de l'énergie is responsible, in Québec, for compliance enforcement with respect to the reliability standard and its appendix that it adopts.

1.2. Compliance Monitoring and Enforcement Processes

No specific provision

1.3. Data Retention

No specific provision

1.4. Additional Compliance Information

No specific provision

2. Violation Severity Levels

No specific provision

E. Variances

No specific provision

F. Associated Documents

No specific provision

Appendix QC-IRO-006-5
Provisions specific to the standard IRO-006-5 applicable in Québec

Revision History

Revision	Adoption Date	Action	Change Tracking
0	May 4, 2015	New appendix	New

A. Introduction

1. Title: Reliability Coordinator Operational Analyses and Real-time Assessments

2. Number: IRO-008-2

3. Purpose: Perform analyses and assessments to prevent instability, uncontrolled separation, or Cascading.

4. Applicability

4.1. Reliability Coordinator.

5. Proposed Effective Date:

See Implementation Plan.

6. Background

See Project 2014-03 project page.

B. Requirements and Measures

R1. Each Reliability Coordinator shall perform an Operational Planning Analysis that will allow it to assess whether the planned operations for the next-day will exceed System Operating Limits (SOLs) and Interconnection Operating Reliability Limits (IROLs) within its Wide Area. [*Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M1. Each Reliability Coordinator shall have evidence of a completed Operational Planning Analysis. Such evidence could include but is not limited to dated power flow study results.

R2. Each Reliability Coordinator shall have a coordinated Operating Plan(s) for next-day operations to address potential System Operating Limit (SOL) and Interconnection Reliability Operating Limit (IROL) exceedances identified as a result of its Operational Planning Analysis as performed in Requirement R1 while considering the Operating Plans for the next-day provided by its Transmission Operators and Balancing Authorities. [*Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M2. Each Reliability Coordinator shall have evidence that it has a coordinated Operating Plan for next-day operations to address potential System Operating Limit (SOL) and Interconnection Reliability Operating Limit (IROL) exceedances identified as a result of the Operational Planning Analysis performed in Requirement R1 while considering the Operating Plans for the next-day provided by its Transmission Operators and Balancing Authorities. Such evidence could include but is not limited to plans for precluding operating in excess of each SOL and IROL that were identified as a result of the Operational Planning Analysis.

R3. Each Reliability Coordinator shall notify impacted entities identified in its Operating Plan(s) cited in Requirement R2 as to their role in such plan(s). *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. Each Reliability Coordinator shall have evidence that it notified impacted entities identified in its Operating Plan(s) cited in Requirement R2 as to their role in such plan(s). Such evidence could include but is not limited to dated operator logs, or e-mail records.

R4. Each Reliability Coordinator shall ensure that a Real-time Assessment is performed at least once every 30 minutes. *[Violation Risk Factor: High] [Time Horizon: Same-day Operations, Real-time Operations]*

M4. Each Reliability Coordinator shall have, and make available upon request, evidence to show it ensured that a Real-time Assessment is performed at least once every 30 minutes. This evidence could include but is not limited to dated computer logs showing times the assessment was conducted, dated checklists, or other evidence.

R5. Each Reliability Coordinator shall notify impacted Transmission Operators and Balancing Authorities within its Reliability Coordinator Area, and other impacted Reliability Coordinators as indicated in its Operating Plan, when the results of a Real-time Assessment indicate an actual or expected condition that results in, or could result in, a System Operating Limit (SOL) or Interconnection Reliability Operating Limit (IROL) exceedance within its Wide Area. *[Violation Risk Factor: High] [Time Horizon: Same-Day Operations, Real-time Operations]*

M5. Each Reliability Coordinator shall make available upon request, evidence that it informed impacted Transmission Operators and Balancing Authorities within its Reliability Coordinator Area, and other impacted Reliability Coordinators as indicated in its Operating Plan, of its actual or expected operations that result in, or could result in, a System Operating Limit (SOL) or Interconnection Reliability Operating Limit (IROL) exceedance within its Wide Area. Such evidence could include but is not limited to dated operator logs, voice recordings or transcripts of voice recordings, electronic communications, or other equivalent evidence. If such a situation has not occurred, the Reliability Coordinator may provide an attestation.

R6. Each Reliability Coordinator shall notify impacted Transmission Operators and Balancing Authorities within its Reliability Coordinator Area, and other impacted Reliability Coordinators as indicated in its Operating Plan, when the System Operating Limit (SOL) or Interconnection Reliability Operating Limit (IROL) exceedance identified in Requirement R5 has been prevented or mitigated. *[Violation Risk Factor: Medium] [Time Horizon: Same-Day Operations, Real-time Operations]*

M6. Each Reliability Coordinator shall make available upon request, evidence that it informed impacted Transmission Operators and Balancing Authorities within its

Reliability Coordinator Area, and other impacted Reliability Coordinators as indicated in its Operating Plan, when the System Operating Limit (SOL) or Interconnection Reliability Operating Limit (IROL) exceedance identified in Requirement R5 has been prevented or mitigated. Such evidence could include but is not limited to dated operator logs, voice recordings or transcripts of voice recordings, electronic communications, or other equivalent evidence. If such a situation has not occurred, the Reliability Coordinator may provide an attestation.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Compliance Monitoring and Assessment Processes

As defined in the NERC Rules of Procedure, "Compliance Monitoring and Assessment Processes" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated reliability standard.

1.3. Data Retention

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

Each Reliability Coordinator shall keep data or evidence to show compliance for Requirements R1 through R3, R5, and R6 and Measures M1 through M3, M5, and M6 for a rolling 90-calendar days period for analyses, the most recent 90-calendar days for voice recordings, and 12 months for operating logs and e-mail records unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

Each Reliability Coordinator shall each keep data or evidence for Requirement R4 and Measure M4 for a rolling 30-calendar day period, unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

If a Reliability Coordinator is found non-compliant, it shall keep information related to the non-compliance until found compliant or the time period specified above, whichever is longer.

The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

1.4. Additional Compliance Information

None

Table of Compliance Elements

R#	Time Horizons	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	Operations Planning	Medium	N/A	N/A	N/A	The Reliability Coordinator did not perform an Operational Planning Analysis allowing it to assess whether its planned operations for the next-day within its Wide Area will exceed any of its System Operating Limits (SOLs) and Interconnection Operating Reliability Limits (IROLs).
R2	Operations Planning	Medium	N/A	N/A	N/A	The Reliability Coordinator did not have a coordinated Operating Plan(s) for next-day operations to address potential System Operating Limit (SOL) and Interconnection Reliability Operating Limit (IROL) exceedances identified as a result of its Operational Planning Analysis as performed in Requirement R1 while considering the Operating Plans for the next-day provided by its Transmission Operators and Balancing Authorities.

R#	Time Horizons	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
For the Requirement R3 and R5 VSLs, the intent of the SDT is to start with the Severe VSL first and then to work your way to the left until you find the situation that fits. In this manner, the VSL will not be discriminatory by size. If a Reliability Coordinator has just one affected reliability entity to inform, the intent is that that situation would be a Severe violation						
R3	Operations Planning	Medium	The Reliability Coordinator did not notify one impacted entity or 5% or less of the impacted entities whichever is greater identified in its Operating Plan(s) as to their role in that plan(s).	The Reliability Coordinator did not notify two impacted entities or more than 5% and less than or equal to 10% of the impacted entities whichever is greater, identified in its Operating Plan(s) as to their role in that plan(s).	The Reliability Coordinator did not notify three impacted entities or more than 10% and less than or equal to 15% of the impacted entities whichever is greater, identified in its Operating Plan(s) as to their role in that plan(s).	The Reliability Coordinator did not notify four or more impacted entities or more than 15% of the impacted entities identified in its Operating Plan(s) as to their role in that plan(s).
R4	Same-day Operations, Real-time Operations	High	For any sample 24-hour period within the 30-day retention period, the Reliability	For any sample 24-hour period within the 30-day retention period, the Reliability Coordinator's	For any sample 24-hour period within the 30-day retention period, the Reliability	For any sample 24-hour period within the 30-day retention period, the Reliability Coordinator's Real-time Assessment was not conducted for three or more 30-minute periods

R#	Time Horizons	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Coordinator's Real-time Assessment was not conducted for one 30-minute period within that 24-hour period.	Real-time Assessment was not conducted for two 30-minute periods within that 24-hour period.	Coordinator's Real-time Assessment was not conducted for three 30-minute periods within that 24-hour period.	within that 24-hour period.
R5	Same-Day Operations, Real-time Operations	High	The Reliability Coordinator did not notify one impacted Transmission Operator or Balancing Authority within its Reliability Coordinator Area or 5% or less of the impacted Transmission Operators and Balancing Authorities within its	The Reliability Coordinator did not notify two impacted Transmission Operators and Balancing Authorities within its Reliability Coordinator Area or more than 5% and less than or equal to 10% of the impacted Transmission Operators and Balancing Authorities within	The Reliability Coordinator did not notify three impacted Transmission Operators and Balancing Authorities within its Reliability Coordinator Area or more than 10% and less than or equal to 15% of the impacted Transmission Operators and	The Reliability Coordinator did not notify four or more impacted Transmission Operators and Balancing Authorities within its Reliability Coordinator Area or more than 15% of the impacted Transmission Operators and Balancing Authorities within its Reliability Coordinator Area identified in the Operating Plan(s) as to their role in the plan(s). OR The Reliability Coordinator did not notify the other impacted Reliability Coordinators, as indicated in its Operating Plan, when the results of its Real-time

R#	Time Horizons	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Reliability Coordinator Area whichever is greater, when the results of its Real-time Assessment indicate an actual or expected condition that results in, or could result in, a System Operating Limit (SOL) or Interconnection Reliability Operating Limit (IROL) exceedance within its Wide Area.	its Reliability Coordinator Area whichever is greater, when the results of its Real-time Assessment indicate an actual or expected condition that results in, or could result in, a System Operating Limit (SOL) or Interconnection Reliability Operating Limit (IROL) exceedance within its Wide Area.	Balancing Authorities within its Reliability Coordinator Area whichever is greater, when the results of its Real-time Assessment indicate an actual or expected condition that results in, or could result in, a System Operating Limit (SOL) or Interconnection Reliability Operating Limit (IROL) exceedance within its Wide Area.	Assessment indicate an actual or expected condition that results in, or could result in, a System Operating Limit (SOL) or Interconnection Reliability Operating Limit (IROL) exceedance within its Wide Area.

R#	Time Horizons	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R6	Same-Day Operations, Real-time Operations	Medium	The Reliability Coordinator did not notify one impacted Transmission Operator or Balancing Authority within its Reliability Coordinator Area or 5% or less of the impacted Transmission Operators and Balancing Authorities within its Reliability Coordinator Area whichever is greater, when the System Operating Limit (SOL) or Interconnection Reliability	The Reliability Coordinator did not notify two impacted Transmission Operators or Balancing Authorities within its Reliability Coordinator Area or more than 5% and less than or equal to 10% of the impacted Transmission Operators and Balancing Authorities within its Reliability Coordinator Area whichever is greater, when the System Operating Limit (SOL) or Interconnection Reliability Operating Limit	The Reliability Coordinator did not notify three impacted Transmission Operators or Balancing Authorities within its Reliability Coordinator Area or more than 10% and less than or equal to 15% of the impacted Transmission Operators and Balancing Authorities within its Reliability Coordinator Area whichever is greater, when the System Operating Limit	The Reliability Coordinator did not notify four or more impacted Transmission Operators or Balancing Authorities within its Reliability Coordinator Area or more than 15% of the impacted Transmission Operators and Balancing Authorities within its Reliability Coordinator Area when the System Operating Limit (SOL) or Interconnection Reliability Operating Limit (IROL) exceedance identified in Requirement R5 was prevented or mitigated. OR The Reliability Coordinator did not notify four or more other impacted Reliability Coordinators as indicated in its Operating Plan when the System Operating Limit (SOL) or Interconnection Reliability Operating Limit (IROL) exceedance identified in Requirement R5 was prevented or mitigated.

R#	Time Horizons	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Operating Limit (IROL) exceedance identified in Requirement R5 was prevented or mitigated. OR The Reliability Coordinator did not notify one other impacted Reliability Coordinator as indicated in its Operating Plan when the when the System Operating Limit (SOL) or Interconnection Reliability Operating Limit (IROL) exceedance identified in	(IROL) exceedance identified in Requirement R6 was prevented or mitigated. OR The Reliability Coordinator did not notify two other impacted Reliability Coordinators as indicated in its Operating Plan when the System Operating Limit (SOL) or Interconnection Reliability Operating Limit (IROL) exceedance identified in Requirement R5 was prevented or	(SOL) or Interconnection Reliability Operating Limit (IROL) exceedance identified in Requirement R5 was prevented or mitigated. OR The Reliability Coordinator did not notify three other impacted Reliability Coordinators as indicated in its Operating Plan when the System Operating Limit (SOL) or Interconnection Reliability Operating Limit	

R#	Time Horizons	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Requirement R5 was prevented or mitigated.	mitigated.	(IROL) exceedance identified in Requirement R5 was prevented or mitigated.	

D. Regional Variances

None

E. Interpretations

None

F. Associated Documents

Operating Plan - An Operating Plan includes general Operating Processes and specific Operating Procedures. It may be an overview document which provides a prescription for an Operating Plan for the next-day, or it may be a specific plan to address a specific SOL or IROL exceedance identified in the Operational Planning Analysis (OPA). Consistent with the NERC definition, Operating Plans can be general in nature, or they can be specific plans to address specific reliability issues. The use of the term Operating Plan in the revised TOP/IRO standards allows room for both. An Operating Plan references processes and procedures, including electronic data exchange, which are available to the System Operator on a daily basis to allow the operator to reliably address conditions which may arise throughout the day. It is valid for tomorrow, the day after, and the day after that. Operating Plans should be augmented by temporary operating guides which outline prevention/mitigation plans for specific situations which are identified day-to-day in an OPA or a Real-time Assessment (RTA). As the definition in the Glossary of Terms states, a restoration plan is an example of an Operating Plan. It contains all the overarching principles that the System Operator needs to work his/her way through the restoration process. It is not a specific document written for a specific blackout scenario but rather a collection of tools consisting of processes, procedures, and automated software systems that are available to the operator to use in restoring the system. An Operating Plan can in turn be looked upon in a similar manner. It does not contain a prescription for the specific set-up for tomorrow but contains a treatment of all the processes, procedures, and automated software systems that are at the operator's disposal. The existence of an Operating Plan, however, does not preclude the need for creating specific action plans for specific SOL or IROL exceedances identified in the OPA. When a Reliability Coordinator performs an OPA, the analysis may reveal instances of possible SOL or IROL exceedances for pre- or post-Contingency conditions. In these instances, Reliability Coordinators are expected to ensure that there are plans in place to prevent or mitigate those SOLs or IROLs, should those operating conditions be encountered the next day. The Operating Plan may contain a description of the process by which specific prevention or mitigation plans for day-to-day SOL or IROL exceedances identified in the OPA are handled and communicated. This approach could alleviate any potential administrative burden associated with perceived requirements for continual day-to-day updating of "the Operating Plan document" for compliance purposes.

Version History

Version	Date	Action	Change Tracking
1	October 17, 2008	Adopted by NERC Board of Trustees	
1	March 17, 2011	Order issued by FERC approving IRO-008-1 (approval effective 5/23/11)	
1	February 28, 2014	Updated VSLs and VRF's based on June 24, 2013 approval.	
2	November 13, 2014	Adopted by NERC Board of Trustees	Revisions under Project 2014-03

Guidelines and Technical Basis

Rationale:

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Changes made to the proposed definitions were made in order to respond to issues raised in NOPR paragraphs 55, 73, and 74 dealing with analysis of SOLs in all time horizons, questions on Protection Systems and Special Protection Systems in NOPR paragraph 78, and recommendations on phase angles from the SW Outage Report (recommendation 27). The intent of such changes is to ensure that Real-time Assessments contain sufficient details to result in an appropriate level of situational awareness. Some examples include: 1) analyzing phase angles which may result in the implementation of an Operating Plan to adjust generation or curtail transactions so that a Transmission facility may be returned to service, or 2) evaluating the impact of a modified Contingency resulting from the status change of a Special Protection Scheme from enabled/in-service to disabled/out-of-service.

Rationale for R1:
Revised in response to NOPR paragraph 96 on the obligation of Reliability Coordinators to monitor SOLs. Measure M1 revised for consistency with TOP-003-3, Measure M1.

Rationale for R2 and R3:
Requirements added in response to IERP and SW Outage Report recommendations concerning the coordination and review of plans.

Rationale for R5 and R6:
In Requirements R5 and R6 the use of the term ‘impacted’ and the tie to the Operating Plan where notification protocols will be set out should minimize the volume of notifications.

*** FOR INFORMATIONAL PURPOSES ONLY ***

Enforcement Dates: Standard IRO-008-2 — Reliability Coordinator Operational Analyses and Real-time Assessments

United States

Standard	Requirement	Enforcement Date	Inactive Date
IRO-008-2	All		

This standard has not yet been approved by the applicable regulatory authority.

Printed On: March 24, 2015, 08:21 AM

Appendix QC-IRO-008-2
Provisions specific to the standard IRO-008-2 applicable in Québec

This appendix establishes specific provisions for the application of the standard in Québec. Provisions of the standard and of its appendix must be read together for the purposes of understanding and interpretation. Where the standard and appendix differ, the appendix shall prevail.

A. Introduction

1. Title: **Reliability Coordinator Operational Analyses and Real-time Assessments**

2. Number: IRO-008-2

3. Purpose: No specific provision

4. Applicability :

Functions

No specific provision

Facilities

This standard only applies to the facilities of the Main Transmission System (RTP).

5. Effective Date :

5.1. Adoption of the standard by the Régie de l'énergie: June 16, 2017

5.2. Adoption of the appendix by the Régie de l'énergie: June 16, 2017

5.3. Effective date of the standard and its appendix in Québec: July 1st, 2017

6. Background :

No specific provision

B. Requirements and Measures

No specific provision

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

The Régie de l'énergie is responsible, in Québec, for compliance enforcement with respect to the reliability standard and its appendix that it adopts.

1.2. Compliance Monitoring and Assessment Processes

Compliance Audit

Self-Certification

Spot Check

Compliance Investigation

Non-Compliance Self-Reporting

Periodic Data Submittal

Exception Reporting

Investigation following a complaint

1.3. Data Retention

No specific provision

1.4. Additional Compliance Information

No specific provision

2. Table of Compliance Elements

No specific provision

D. Regional Variances

No specific provision

E. Interpretations

No specific provision

F. Associated Documents

The Quebec glossary reference is the "Quebec Reliability Standards Glossary of Terms".

Guidelines and Technical Basis

No specific provision

Version History

Version	Date	Action	Change Tracking
0	June 16, 2017	New appendix	New

A. Introduction

1. **Title:** **Reliability Coordinator Actions to Operate Within IROLs**
2. **Number:** IRO-009-2
3. **Purpose:** To prevent instability, uncontrolled separation, or cascading outages that adversely impact the reliability of the interconnection by ensuring prompt action to prevent or mitigate instances of exceeding Interconnection Reliability Operating Limits (IROLs).
4. **Applicability:**

   4.1. Functional Entities:

   4.1.1. Reliability Coordinator.

5. **Effective Date:** See the Implementation Plan for IRO-009-2.

B. Requirements and Measures

R1. For each IROL (in its Reliability Coordinator Area) that the Reliability Coordinator identifies one or more days prior to the current day, the Reliability Coordinator shall have one or more Operating Processes, Procedures, or Plans that identify actions the Reliability Coordinator shall take or actions the Reliability Coordinator shall direct others to take (up to and including load shedding): *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning or Same Day Operations]*

1.1. That can be implemented in time to prevent the identified IROL exceedance.

1.2. To mitigate the magnitude and duration of an IROL exceedance such that the IROL exceedance is relieved within the IROL's T_v.

M1. Each Reliability Coordinator shall have, and make available upon request, evidence to confirm that it has Operating Processes, Procedures, or Plans to address both preventing and mitigating the magnitude and duration of IROL exceedances in accordance with Requirement R1. This evidence shall include a list of any IROLs (and each associated T_v) identified in advance, along with one or more dated Operating Processes, Procedures, or Plans that will be used.

R2. Each Reliability Coordinator shall initiate one or more Operating Processes, Procedures, or Plans (not limited to the Operating Processes, Procedures, or Plans developed for Requirement R1) that are intended to prevent an IROL exceedance, as identified in the Reliability Coordinator's Real-time monitoring or Real-time Assessment. *[Violation Risk Factor: High] [Time Horizon: Real-time Operations]*

M2. Each Reliability Coordinator shall have, and make available upon request, evidence to confirm that it initiated one or more Operating Processes, Procedures or Plans (not limited to the Operating Processes, Procedures, or Plans developed for Requirements R1) in accordance with Requirement R2. This evidence could include, but is not

limited to, Operating Processes, Procedures, or Plans from Requirement R1, dated operating logs, dated voice recordings, dated transcripts of voice recordings, or other evidence.

R3. Each Reliability Coordinator shall act or direct others to act so that the magnitude and duration of an IROL exceedance is mitigated within the IROL's T_v, as identified in the Reliability Coordinator's Real-time monitoring or Real-time Assessment. *[Violation Risk Factor: High] [Time Horizon: Real-time Operations]*

M3. Each Reliability Coordinator shall have, and make available upon request, evidence to confirm that it acted or directed others to act in accordance with Requirement R3. This evidence could include, but is not limited to, Operating Processes, Procedures, or Plans, dated operating logs, dated voice recordings, dated transcripts of voice recordings, or other evidence.

R4. Each Reliability Coordinator shall operate to the most limiting IROL and T_v in instances where there is a difference in an IROL or its T_v between Reliability Coordinators that are responsible for that Facility (or group of Facilities). *[Violation Risk Factor: High] [Time Horizon: Real-time Operations]*

M4. Each Reliability Coordinator shall have, and make available upon request, evidence to confirm that it operated to the most limiting IROL and T_v in instances where there was a difference in an IROL or its T_v. Such evidence could include, but is not limited to, dated computer printouts, dated operator logs, dated voice recordings, dated transcripts of voice recordings, or other equivalent evidence in accordance with Requirement R4.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority:
"Compliance Enforcement Authority" means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention:
The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

The Reliability Coordinator shall retain evidence of Requirement R1; Requirement R2; Requirement R3; and Requirement R4 for a rolling 12 months.

The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records, and any reported IROL violations submitted since the last audit.

1.3. Compliance Monitoring and Enforcement Program
As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

1.4. Additional Compliance Information

None.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.				An IROL in its Reliability Coordinator Area was identified one or more days in advance and the Reliability Coordinator does not have an Operating Process, Procedure, or Plan that identifies actions to prevent that IROL exceedance (Part 1.1). OR An IROL in its Reliability Coordinator Area was identified one or more days in advance and the Reliability Coordinator does not have an Operating Process, Procedure, or Plan that identifies actions to mitigate that IROL exceedance within the IROL's T_v. (Part 1.2).
R2.				No Operating Processes, Procedures, or Plans were

				initiated that were intended to prevent a predicted IROL exceedance as identified in the Reliability Coordinator's Real-time monitoring or Real-time Assessment.
R3.				Actual system conditions showed that there was an IROL exceedance in its Reliability Coordinator Area, and that the IROL exceedance was not mitigated within the IROL's T_v.
R4.				The most limiting IROL or its T_v was not operated to between Reliability Coordinators that are responsible for the Facility (or group of Facilities) associated with the IROL.

D. Regional Variances

None.

E. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	October 17, 2008	Adopted by NERC Board of Trustees	
1	March 17, 2011	FERC approved IRO-009-1	
2	August 13, 2015	Adopted by NERC Board of Trustees	Revised to address the recommendations of the Project 2012-09 Interconnected Reliability Operations Five-Year Review Team.

Standard Attachments

None.

Rationale

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT adoption, the text from the rationale text boxes was moved to this section.

Rationale for revisions to Requirement R1: The standard drafting team (IRO SDT) revised this requirement by combining IRO-009-1 Requirements R1 and R2 to form one requirement with two subparts to make the requirements more concise, as both requirements contained similar language.

Rationale for revisions to new Requirement R2 (previously Requirement R3): The IRO SDT revised the language of this requirement to improve clarity as well as consistency with similar NERC Board of Trustees (Board) approved standards, such as, TOP standard revisions (TOP-001-3 R14); "IROL exceedance," "Real-time monitoring," and "Real-time Assessments."

Rationale for Revisions to Requirement R3 (previously Requirement R4): The IRO SDT removed the term "without delay" from the requirement upon determining that the point of time at which the requirement is triggered is inherent in the requirement itself. The IRO SDT also revised the language of this requirement to improve clarity as well as consistency with similar Board approved standards, such as, TOP standard revisions (TOP-001-3 R14); "IROL exceedance," "Real-time monitoring," and "Real-time Assessments."

Rationale for revisions to Requirement R4 (previously Requirement R5): The IRO SDT revised the language of this requirement for clarity as well as consistency with similar Board approved standards, such as TOP standard revisions (TOP-001-3 R18). The IRO SDT retained clarifying language to limit applicability to appropriate affected RCs.

Appendix QC-IRO-009-2
Provisions specific to the standard IRO-009-2 applicable in Québec

This appendix establishes specific provisions for the application of the standard in Québec. Provisions of the standard and of its appendix must be read together for the purposes of understanding and interpretation. Where the standard and appendix differ, the appendix shall prevail.

A. Introduction

1. Title: **Reliability Coordinator Actions to Operate Within IROLs**

2. Number: IRO-009-2

3. Purpose: No specific provision

4. Applicability: No specific provision

5. Effective Date:

5.1. Adoption of the standard by the Régie de l'énergie: June 16, 2017

5.2. Adoption of the appendix by the Régie de l'énergie: June 16, 2017

5.3. Effective date of the standard and its appendix in Québec: July 1st, 2017

B. Requirements and Measures

No specific provision

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

The Régie de l'énergie is responsible, in Québec, for compliance enforcement with respect to the reliability standard and its appendix that it adopts.

1.2. Evidence Retention

No specific provision

1.3. Compliance Monitoring and Enforcement Program

Compliance Audit

Self-Certification

Spot Check

Compliance Investigation

Non-Compliance Self-Reporting

Periodic Data Submittal

Exception Reporting

Investigation following a complaint

1.4. Additional Compliance Information

No specific provision

2. Violation Severity Levels

No specific provision

Appendix QC-IRO-009-2
Provisions specific to the standard IRO-009-2 applicable in Québec

D. Regional Variances

No specific provision

E. Associated Documents

No specific provision

Standard Attachments

No specific provision

Rationale

No specific provision

Version History

Revision	Date	Action	Change Tracking
0	June 16, 2017	New appendix	New

A. Introduction

1. **Title:** Reliability Coordinator Data and information Specification and Collection
2. **Number:** IRO-010-5
3. **Purpose:** To prevent instability, uncontrolled separation, or Cascading outages that adversely impact reliability, by ensuring each Reliability Coordinator has the data and information it needs to plan, monitor and assess the operation of its Reliability Coordinator Area.
4. **Applicability:**
   - **4.1.** Reliability Coordinator
   - **4.2.** Balancing Authority
   - **4.3.** Generator Owner
   - **4.4.** Generator Operator
   - **4.5.** Transmission Operator
   - **4.6.** Transmission Owner
   - **4.7.** Distribution Provider
5. **Effective Date:** See Implementation Plan for Project 2021-06.

B. Requirements

R1. The Reliability Coordinator shall maintain documented specification(s) for the data and information necessary for it to perform its Operational Planning Analyses, Real-time monitoring, and Real-time Assessments. The specification shall include but not be limited to: *(Violation Risk Factor: Low) (Time Horizon: Operations Planning)*

1.1. A list of data and information needed by the Reliability Coordinator to support its Operational Planning Analyses, Real-time monitoring, and Real- time Assessments including non-BES data and information, external network data and information, and identification of the entities responsible for responding to the specification as deemed necessary by the Reliability Coordinator.

1.2. Provisions for notification of current Protection System and Remedial Action Scheme (RAS) status or degradation that impacts System reliability.

1.3. Provisions for notification of BES generating unit(s) during local forecasted cold weather to include:

1.3.1 Operating limitations based on:

1.3.1.1. capability and availability;

1.3.1.2. fuel supply and inventory concerns;

1.3.1.3. fuel switching capabilities; and

1.3.1.4. environmental constraints

1.3.2. Generating unit(s) minimum:

1.3.2.1. design temperature; or

1.3.2.2. historical operating temperature; or

1.3.2.3. current cold weather performance temperature determined by an engineering analysis.

1.4. Identification of a mutually agreeable process for resolving conflicts.

1.5. Method(s) for the entity identified in Part 1.1 to provide data and information that includes, but is not limited to.

1.5.1 Specific deadlines or periodicity in which data and information is to be provided;

1.5.2 Performance criteria for the availability and accuracy of data and information, as applicable;

1.5.3 Provisions to update or correct data and information, as applicable or necessary.

1.5.4 A mutually agreeable format.

1.5.5 A mutually agreeable method(s) for securely transferring data and information.

M1. The Reliability Coordinator shall make available its dated, current, in force documented specification(s) for data and information.

R2. The Reliability Coordinator shall distribute its data and information specification(s) to entities that have data required by the Reliability Coordinator's Operational Planning Analyses, Real- time monitoring, and Real-time Assessments. *(Violation Risk Factor: Low) (Time Horizon: Operations Planning)*

M2. The Reliability Coordinator shall make available evidence that it has distributed its specification(s) to entities that have data and information required by the Reliability Coordinator's Operational Planning Analyses, Real-time monitoring, and Real-time Assessments. This evidence could include but is not limited to web postings with an electronic notice of the posting, dated operator logs, voice recordings, postal receipts showing the recipient, date and contents, or e-mail records.

R3. Each Reliability Coordinator, Balancing Authority, Generator Owner, Generator Operator, Transmission Operator, Transmission Owner, and Distribution Provider receiving a specification(s) in Requirement R2 shall satisfy the obligations of the documented specifications . *(Violation Risk Factor: Medium) (Time Horizon: Operations Planning, Same-Day Operations, Real-time Operations)*

M3. The Reliability Coordinator, Balancing Authority, Generator Owner, Generator Operator, Reliability Coordinator, Transmission Operator, Transmission Owner, and Distribution Provider receiving a specification(s) in Requirement R2 shall make available evidence that it satisfied the obligations of the documented specification using the specified criteria. Such evidence could include but is not limited to electronic or hard copies of data transmittals or attestations of receiving entities.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with the mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The Reliability Coordinator, Balancing Authority, Generator Owner, Generator Operator, Transmission Operator, Transmission Owner, and Distribution Provider shall each keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

The Reliability Coordinator shall retain its dated, current, in force documented specification(s) for the data and information necessary for it to perform its Operational Planning Analyses, Real-time monitoring, and Real-time Assessments for Requirement R1, Measure M1 as well as any documents in force since the last compliance audit.

The Reliability Coordinator shall keep evidence for three calendar years that it has distributed its specification(s) to entities that have data required by the Reliability Coordinator's Operational Planning Analyses, Real-time monitoring, and Real-time Assessments for Requirement R2, Measure M2.

Each Reliability Coordinator, Balancing Authority, Generator Owner, Generator Operator, Transmission Operator, Transmission Owner, and Distribution Provider receiving a specification(s) shall retain evidence for the most recent 90-calendar days that it has satisfied the obligations of the documented specifications in accordance with Requirement R3 and Measurement M3.

1.3. Compliance Monitoring and Enforcement Program:
As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated reliability standard.

Violation Severity Levels

R#	Time Horizon	VRF	Violation Severity Levels			
			Lower	Moderate	High	Severe
R1	Operations Planning	Low	The Reliability Coordinator did not include one or two of the parts (Part 1.1 through Part 1.5) of the documented specification(s) for the data and information necessary for it to perform its Operational Planning Analyses, Real-time monitoring, and Real- time Assessments.	The Reliability Coordinator did not include three of the parts (Part 1.1 through Part 1.5) of the documented specification(s) for the data and information necessary for it to perform its Operational Planning Analyses, Real-time monitoring, and Real-time Assessments.	The Reliability Coordinator did not include four of the parts (Part 1.1 through Part 1.5) of the documented specification(s) for the data and information necessary for it to perform its Operational Planning Analyses, Real-time monitoring, and Real-time Assessments.	The Reliability Coordinator did not include any of the parts (Part 1.1 through Part 1.5) of the documented specification(s) for the data and information necessary for it to perform its Operational Planning Analyses, Real-time monitoring, and Real-time Assessments. OR, The Reliability Coordinator did not have a documented specification(s) for the data and information necessary for it to perform its Operational Planning Analyses, Real-time monitoring, and Real-time Assessments.
For the Requirement R2 VSLs only, the intent of the SDT is to start with the Severe VSL first and then to work your way to the left until you find the situation that fits. In this manner, the VSL will not be discriminatory by size of entity. If a small entity has just one affected reliability entity to inform, the intent is that that situation would be a Severe violation.						

R#	Time Horizon	VRF	Violation Severity Levels			
			Lower	Moderate	High	Severe
R2	Operations Planning	Low	The Reliability Coordinator did not distribute its specification(s) as developed in Requirement R1 to one entity, or 5% or less of the entities, whichever is greater, that have data and information required by the Reliability Coordinator's Operational Planning Analyses, Real-time monitoring, and Real-time Assessments.	The Reliability Coordinator did not distribute its specification(s) as developed in Requirement R1 to two entities, or more than 5% and less than or equal to 10% of the reliability entities, whichever is greater, that have data and information required by the Reliability Coordinator's Operational Planning Analyses, and Real-time monitoring, and Real-time Assessments.	The Reliability Coordinator did not distribute its specification(s) as developed in Requirement R1 to three entities, or more than 10% and less than or equal to 15% of the reliability entities, whichever is greater, that have data and information required by the Reliability Coordinator's Operational Planning Analyses, Real-time monitoring, and Real-time Assessments.	The Reliability Coordinator did not distribute its specification(s) as developed in Requirement R1 to four or more entities, or more than 15% of the entities, whichever is greater, that have data and information required by the Reliability Coordinator's Operational Planning Analyses, Real-time monitoring, and Real-time Assessments.
R3	Operations Planning, Same-Day Operations, Real-time Operations	Medium	The responsible entity receiving a specification(s) in Requirement R2 satisfied the obligations of the documented specifications but failed to meet one of the parts in Requirement Part 1.5.	The responsible entity receiving a specification(s) in Requirement R2 satisfied the obligations of the documented specifications but failed to meet two of the parts in Requirement R1Part 1.5.	The responsible entity receiving a specification(s) in Requirement R2 satisfied the obligations of the documented specifications but failed to meet any of the parts in Requirement R1 Part 1.5.	The responsible entity receiving a specification(s) in Requirement R2 did not satisfy the obligations of the documented specifications .

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	October 17, 2008	Adopted by Board of Trustees	New
1a	August 5, 2009	Added Appendix 1: Interpretation of R1.2 and R3 as approved by Board of Trustees	Addition
1a	March 17, 2011	Order issued by FERC approving IRO- 010-1a (approval effective 5/23/11)	
1a	November 19, 2013	Updated VRFs based on June 24, 2013 approval	
2	April 2014	Revisions pursuant to Project 2014-03	
2	November 13, 2014	Adopted by NERC Board of Trustees	Revisions under Project 2014-03
2	November 19, 2015	FERC approved IRO-010-2. Docket No. RM15-16-000	
3	February 6, 2020	Adopted by NERC Board of Trustees	Revisions under Project 2017-07
3	October 30, 2020	FERC approved IRO-010-3. Docket No. RD20-4-000	
4	March 22, 2021	Adopted by NERC Board of Trustees	Revisions under Project 2019-06 Cold Weather
4	June 11, 2021	Adopted by NERC Board of Trustees	Revisions under Project 2019-06
4	August 24,2021	FERC approved IRO-010-4. Docket No. RD21-5-000	
4	August 27, 2021	Effective Date	April 1, 2023
5	August 17, 2023	Adopted by NERC Board of Trustees	Revision under project 2021-06

5	November 2, 2023	FERC Approved IRO-010-5. Docket No. RD23-6-000	
5	November 3, 2023	Effective Date	July 1, 2025

Appendix IRO-010-5-QC-1
Specific provisions applicable in Québec for standard IRO-010-4
IRO-010-5 – Reliability Coordinator Data and Information Specification and Collection

This appendix establishes specific provisions for the application of the standard in Québec. Provisions of the standard and of this appendix must be read jointly for the comprehension and interpretation purposes. Where the standard and appendix differ, the appendix shall prevail.

A. Introduction

1. Title: No specific provision.

2. Number: No specific provision.

3. Purpose: No specific provision.

4. Applicability :

This standard applies to the facilities of the Main Transmission System (RTP) and, for requirement R1, to the facilities designated under this requirement.

5. Effective Date :

5.1.	Adoption of the standard by the Régie de l'énergie:	September 13, 2024
5.2.	Adoption of the appendix by the Régie de l'énergie:	September 13, 2024
5.3.	Effective date of the standard and of its appendix in Québec:	April 1, 2026

B. Requirements

Specific provision applicable to requirement R1 (1.1):
The expression "non BES" is replaced by "non RTP".

Specific provisions applicable to requirement R1 (1.3):
The expression "BES" is replaced by "RTP".

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

In Québec, "Compliance Enforcement Authority" means the Régie de l'énergie in its roles of monitoring and enforcing compliance with respect to the Reliability Standard and to this appendix.

1.2. Evidence Retention

No specific provision

1.3. Compliance Monitoring and Enforcement Program:

The Régie de l'énergie establishes the monitoring processes used to evaluate data or information for the purpose of determining compliance or non-compliance with the Reliability Standard and with this appendix.

Violation Severity Levels

No specific provision.

D. Regional Variances

No specific provision.

E. Interpretations

No specific provision.

F. Associated Documents

No specific provision.

Version History

Revision	Date	Action	Change Tracking
1	September 13, 2024	New appendix as per decision D-2024-096.	New

A. Introduction

1. **Title:** Coordination Among Reliability Coordinators

2. **Number:** IRO-014-3

3. **Purpose:** To ensure that each Reliability Coordinator's operations are coordinated such that they will not adversely impact other Reliability Coordinator Areas and to preserve the reliability benefits of interconnected operations.

4. **Applicability:**

   4.1. Reliability Coordinator

5. **Effective Date**

   See Implementation Plan.

6. **Background:**

   See Project 2014-03 project page.

B. Requirements and Measures

R1. Each Reliability Coordinator shall have and implement Operating Procedures, Operating Processes, or Operating Plans, for activities that require notification or coordination of actions that may impact adjacent Reliability Coordinator Areas, to support Interconnection reliability. These Operating Procedures, Operating Processes, or Operating Plans shall include, but are not limited to, the following: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning, Same-Day Operations]*

1.1. Criteria and processes for notifications.

1.2. Energy and capacity shortages.

1.3. Control of voltage, including the coordination of reactive resources.

1.4. Exchange of information including planned and unplanned outage information to support its Operational Planning Analyses and Real-time Assessments.

1.5. Provisions for periodic communications to support reliable operations.

M1. Each Reliability Coordinator shall have available the latest approved documented version of its Operating Procedures, Operating Processes, and Operating Plans that require notifications, or the coordination of actions among impacted Reliability Coordinators for conditions or activities that may impact adjacent Reliability Coordinator Areas. This documentation shall include dated, current in force documentation with the specified elements, and notes from periodic communications.

R2. Each Reliability Coordinator shall maintain its Operating Procedures, Operating Processes, or Operating Plans identified in Requirement R1 as follows: *[Violation Risk Factor: Low] [Time Horizon: Operations Planning, Same-Day Operations]*

2.1. Review and update annually with no more than 15 months between reviews.

2.2. Obtain written agreement from all of the Reliability Coordinators required to take the indicated action(s) for each update.

2.3. Distribute to all Reliability Coordinators that are required to take the indicated action(s) within 30 days of an update.

M2. Each Reliability Coordinator shall have dated evidence that its Operating Procedures, Operating Processes, and Operating Plans that require one or more other Reliability Coordinators to take action were maintained as specified. This evidence may include but is not limited to dated documentation with confirmation of receipt, dated notice of acceptance or agreement to take specified actions, or dated electronic communications with confirmation of receipt and acceptance or agreement to take specified actions.

R3. Each Reliability Coordinator, upon identification of an expected or actual Emergency in its Reliability Coordinator Area, shall notify other impacted Reliability Coordinators. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning, Same Day Operations, Real-time Operations]*

M3. Each Reliability Coordinator shall have and provide evidence which may include but is not limited to operator logs, voice recordings, or transcripts of voice recordings, electronic communications, or equivalent dated documentation, that will be used to determine that it, upon identification of an expected or actual Emergency in its Reliability Coordinator Area, notified other impacted Reliability Coordinators.

R4. Each impacted Reliability Coordinator shall operate as though the Emergency exists during each instance where Reliability Coordinators disagree on the existence of an Emergency. *[Violation Risk Factor: High] [Time Horizon: Operations Planning, Same-Day Operations, Real-time Operations]*

M4. Each Reliability Coordinator shall have and provide evidence which may include but is not limited to operator logs, voice recordings or transcripts of voice recordings, electronic communications, or equivalent documentation, that will be used to determine that it operated as though an Emergency existed during each instance where Reliability Coordinators disagreed on the existence of an Emergency.

R5. Each Reliability Coordinator that Identifies an Emergency in its Reliability Coordinator Area shall develop an action plan to resolve the Emergency during those instances where impacted Reliability Coordinators disagree on the existence of an Emergency. *[Violation Risk Factor: High][Time Horizon: Operations Planning, Same-Day Operations, Real-time Operations]*

M5. Each Reliability Coordinator that identifies an Emergency in its Reliability Coordinator Area shall have evidence that it developed an action plan during those instances where impacted Reliability Coordinators disagreed on the existence of an Emergency. This evidence may include but is not limited to operator logs, voice recordings or

transcripts of voice recordings, electronic communications, or equivalent dated documentation.

R6. Each impacted Reliability Coordinator shall implement the action plan developed by the Reliability Coordinator that identifies the Emergency during those instances where Reliability Coordinators disagree on the existence of an Emergency, unless such actions would violate safety, equipment, regulatory, or statutory requirements. *[Violation Risk Factor: High][Time Horizon: Operations Planning, Same-Day Operations, Real-time Operations]*

M6. Each impacted Reliability Coordinator shall have and provide evidence which may include but is not limited to operator logs, voice recordings or transcripts of voice recordings, electronic communications, or equivalent dated documentation, that will be used to determine that it implemented the action plan developed by the Reliability Coordinator who identifies the Emergency when Reliability Coordinators disagree on the existence of an Emergency unless such actions would have violated safety, equipment, regulatory, or statutory requirements.

R7. Each Reliability Coordinator shall assist Reliability Coordinators, if requested and able, provided that the requesting Reliability Coordinator has implemented its emergency procedures, unless such actions cannot be physically implemented or would violate safety, equipment, regulatory, or statutory requirements. *[Violation Risk Factor: High] [Time Horizon: Real-time Operations]*

M7. Each Reliability Coordinator shall make available upon request, evidence that requested assistance was provided, if able, to requesting Reliability Coordinators unless such actions could not be physically implemented or would violate safety, equipment, regulatory, or statutory requirements. Such evidence could include but is not limited to dated operator logs, voice recordings or transcripts of voice recordings, electronic communications, or other equivalent evidence in electronic or hard copy format. If such a situation has not occurred, the Reliability Coordinator may provide an attestation.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Compliance Monitoring and Assessment Processes:

As defined in the NERC Rules of Procedure, "Compliance Monitoring and Assessment Processes" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated reliability standard.

1.3. Data Retention

The Reliability Coordinator shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation:

- Each Reliability Coordinator shall retain its current, in force document and any documents in force since the last compliance audit for Requirements R1 and R2 and Measures M1 and M2.
- Each Reliability Coordinator shall retain its most recent 12 months of evidence for Requirement R5 and Measure M5.
- Each Reliability Coordinator shall retain 3-calendar years plus current calendar year of evidence for Requirement R6 and Measure M6.
- Each Reliability Coordinator shall retain evidence for 90-calendar days for operator logs and voice recordings and for the period since the last compliance audit for other evidence for Requirements R3, R4, and R7 and Measures M3, M4, and M7.

If a Reliability Coordinator is found non-compliant, it shall keep information related to the non-compliance until found compliant, or for the time period specified above, whichever is longer.

The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

1.4 Additional Compliance Information

None

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	Operations Planning, Same-Day Operations	Medium	The Reliability Coordinator has Operating Procedures, Operating Processes, or Operating Plans in place for activities that require notification or coordination of actions with impacted adjacent Reliability Coordinators to support Interconnection reliability but failed to address one of the topical areas identified in Parts 1.1 through 1.5.	The Reliability Coordinator has Operating Procedures, Operating Processes, or Operating Plans in place for activities that require notification, or coordination of actions with impacted adjacent Reliability Coordinators to support Interconnection reliability but failed to address two of the topical areas identified in Parts 1.1 through 1.5.	The Reliability Coordinator has Operating Procedures, Operating Processes, or Operating Plans in place for activities that require notification, or coordination of actions with impacted adjacent Reliability Coordinators to support Interconnection reliability but failed to address three of the topical areas identified in Parts 1.1 through 1.5.	The Reliability Coordinator failed to have Operating Procedures, Operating Processes, or Operating Plans in place for activities that require notification, or coordination of actions with impacted adjacent Reliability Coordinators to support Interconnection reliability. OR, The Reliability Coordinator failed to implement its Operating Procedures, Operating processes, or Operating Plans when activities required notification, or coordination of actions with impacted adjacent Reliability Coordinators to support

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						Interconnection reliability.
R2	Operations Planning, Same-Day Operations	Lower	N/A	The Reliability Coordinator has Operating Procedures, Operating Processes, or Operating Plans identified in Requirement R1 but failed to address one of the parts specified in Requirement R2.	The Reliability Coordinator has Operating Procedures, Operating Processes, or Operating Plans identified in Requirement R1 but failed to address two of the parts specified in Requirement R2.	The Reliability Coordinator has Operating Procedures, Operating Processes, or Operating Plans identified in Requirement R1 but failed to address all three of the parts specified in Requirement R2.
For the Requirement R3 VSLs only, the intent of the SDT is to start with the Severe VSL first and then to work your way to the left until you find the situation that fits. In this manner, the VSL will not be discriminatory by size. If a Reliability Coordinator has just one affected reliability entity to inform, the intent is that that situation would be a Severe violation.						
R3	Operations Planning, Same-Day Operations, Real-time Operations	Medium	The Reliability Coordinator did not notify one other impacted Reliability Coordinator upon identification of an expected or actual Emergency in its Reliability Coordinator Area.	The Reliability Coordinator did not notify two other impacted Reliability Coordinators upon identification of an expected or actual Emergency in its Reliability Coordinator Area.	The Reliability Coordinator did not notify three other impacted Reliability Coordinators upon identification of an expected or actual Emergency in its Reliability Coordinator Area.	The Reliability Coordinator did not notify four or more other impacted Reliability Coordinators upon identification of an expected or actual Emergency in its Reliability Coordinator Area.

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R4	Operations Planning, Same-Day Operations, Real-time Operations	High	N/A	N/A	N/A	The Reliability Coordinator failed to operate as though the Emergency existed during an instance where Reliability Coordinators disagreed on the existence of an Emergency.
R5	Operations Planning, Same-Day Operations, Real-time Operations	High	N/A	N/A	N/A	The Reliability Coordinator that identifies the Emergency in its Reliability Coordinator Area failed to develop an action plan to resolve the Emergency during an instance where impacted Reliability Coordinators disagreed on the existence of Emergency.
R6	Real-time Operations, Same-Day Operations	High	N/A	N/A	N/A	The impacted Reliability Coordinator failed to implement the action plan developed by the Reliability Coordinator that identifies the

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						Emergency during an instance where Reliability Coordinators disagreed on the existence of the Emergency.
R7	Real-time Operations	High	N/A	N/A	N/A	The Reliability Coordinator did not provide assistance to Reliability Coordinators, if requested and able, provided that the requesting Reliability Coordinator had implemented its emergency procedures, unless such actions could not physically be implemented or would have violated safety, equipment, regulatory, or statutory requirements.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

Operating Plan - An Operating Plan includes general Operating Processes and specific Operating Procedures. It may be an overview document which provides a prescription for an Operating Plan for the next-day, or it may be a specific plan to address a specific SOL or IROL exceedance identified in the Operational Planning Analysis (OPA). Consistent with the NERC definition, Operating Plans can be general in nature, or they can be specific plans to address specific reliability issues. The use of the term Operating Plan in the revised TOP/IRO standards allows room for both. An Operating Plan references processes and procedures, including electronic data exchange, which are available to the System Operator on a daily basis to allow the operator to reliably address conditions which may arise throughout the day. It is valid for tomorrow, the day after, and the day after that. Operating Plans should be augmented by temporary operating guides which outline prevention/mitigation plans for specific situations which are identified day-to-day in an OPA or a Real-time Assessment (RTA). As the definition in the Glossary of Terms states, a restoration plan is an example of an Operating Plan. It contains all the overarching principles that the System Operator needs to work his/her way through the restoration process. It is not a specific document written for a specific blackout scenario but rather a collection of tools consisting of processes, procedures, and automated software systems that are available to the operator to use in restoring the system. An Operating Plan can in turn be looked upon in a similar manner. It does not contain a prescription for the specific set-up for tomorrow but contains a treatment of all the processes, procedures, and automated software systems that are at the operator's disposal. The existence of an Operating Plan, however, does not preclude the need for creating specific action plans for specific SOL or IROL exceedances identified in the OPA. When a Reliability Coordinator performs an OPA, the analysis may reveal instances of possible SOL or IROL exceedances for pre- or post-Contingency conditions. In these instances, Reliability Coordinators are expected to ensure that there are plans in place to prevent or mitigate those SOLs or IROLs, should those operating conditions be encountered the next day. The Operating Plan may contain a description of the process by which specific prevention or mitigation plans for day-to-day SOL or IROL exceedances identified in the OPA are handled and communicated. This approach could alleviate any potential administrative burden associated with perceived requirements for continual day-to-day updating of "the Operating Plan document" for compliance purposes.

Version History

Version	Date	Action	Change Tracking
1	August 10, 2005	1. Changed incorrect use of certain hyphens (-) to "en dash (–)." 2. Hyphenated "30-day" when used as adjective. 3. Changed standard header to be consistent with standard "Title." 4. Initial capped heading "Definitions of Terms Used in Standard." 5. Added "periods" to items where appropriate. 6. Changed "Timeframe" to "Time Frame" in item D, 1.2. 7. Lower cased all words that are not "defined" terms — drafting team, self-certification. 8. Changed apostrophes to "smart" symbols. 9. Added comma in all word strings "Procedures, Processes, or Plans," etc. 10. Added hyphens to "Reliability Coordinator-to-Reliability Coordinator" where used as adjective. 11. Removed comma in item 2.1.2. 12. Removed extra spaces between words where appropriate.	January 20, 2006
1	February 7, 2006	Adopted by Board of Trustees	Revised
1	March 16, 2007	Approved by FERC	
2	August 4, 2011	Revised per Project 2006-6; Revised existing requirements for clarity, retired R3 and R4 and incorporated requirements from IRO-015-1 and IRO-016-1 into this standard. Adopted by Board of Trustees	Revised

3	November 13, 2014	Adopted by Board of Trustees	Revisions under Project 2014-03

Guidelines and Technical Basis

Rationale:

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for Terminology:
Terminology changed from Adverse Reliability Impact to Emergency for consistency amongst standards. Emergency is a more inclusive term.

Rationale for Requirement R7:
Language added for consistency with proposed TOP-001-3, Requirement R7.

*** FOR INFORMATIONAL PURPOSES ONLY ***

Enforcement Dates: Standard IRO-014-3 — Coordination Among Reliability Coordinators

United States

Standard	Requirement	Enforcement Date	Inactive Date
IRO-014-3	All		

This standard has not yet been approved by the applicable regulatory authority.

Printed On: March 24, 2015, 08:22 AM

Appendix QC-IRO-014-3
Provisions specific to the standard IRO-014-3 applicable in Québec

This appendix establishes specific provisions for the application of the standard in Québec. Provisions of the standard and of its appendix must be read together for the purposes of understanding and interpretation. Where the standard and appendix differ, the appendix shall prevail.

A. Introduction

1. Title: **Coordination Among Reliability Coordinators**

2. Number: IRO-014-3

3. Purpose: No specific provision

4. Applicability: No specific provision

5. Effective Date :

5.1. Adoption of the standard by the Régie de l'énergie: June 16, 2017

5.2. Adoption of the appendix by the Régie de l'énergie: June 16, 2017

5.3. Effective date of the standard and its appendix in Québec: July 1st, 2017

6. Background :

No specific provision

B. Requirements and Measures

No specific provision

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

The Régie de l'énergie is responsible, in Québec, for compliance monitoring with respect to the reliability standard and its appendix that it adopts.

1.2. Compliance Monitoring and Assessment Processes

Compliance Audit

Self-Certification

Spot Check

Compliance Investigation

Non-Compliance Self-Reporting

Periodic Data Submittal

Exception Reporting

Investigation following a complaint

1.3. Data Retention

No specific provision

1.4. Additional Compliance Information

No specific provision

2. Table of Compliance Elements

No specific provision

D. Regional Variances

No specific provision

E. Interpretations

No specific provision

F. Associated Documents

The Quebec glossary reference is the "Quebec Reliability Standards Glossary of Terms".

Guidelines and Technical Basis

No specific provision

Version History

Revision	Date	Action	Change Tracking
0	June 16, 2017	New appendix	New

A. Introduction

1. **Title: Outage Coordination**

2. **Number: IRO-017-1**

3. **Purpose:** To ensure that outages are properly coordinated in the Operations Planning time horizon and Near-Term Transmission Planning Horizon.

4. **Applicability:**

   4.1. Reliability Coordinator

   4.2. Transmission Operator

   4.3. Balancing Authority

   4.4. Planning Coordinator

   4.5. Transmission Planner

5. **Effective Date:**

   See Implementation Plan.

6. **Background:**

   See Project 2014-03 project page.

B. Requirements and Measures

R1. Each Reliability Coordinator shall develop, implement, and maintain an outage coordination process for generation and Transmission outages within its Reliability Coordinator Area. The outage coordination process shall: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1. Identify applicable roles and reporting responsibilities including:

1.1.1. Development and communication of outage schedules.

1.1.2. Assignment of coordination responsibilities for outage schedules between Transmission Operator(s) and Balancing Authority(s).

1.2. Specify outage submission timing requirements.

1.3. Define the process to evaluate the impact of Transmission and generation outages within its Wide Area.

1.4. Define the process to coordinate the resolution of identified outage conflicts with its Transmission Operators and Balancing Authorities, and other Reliability Coordinators.

M1. Each Reliability Coordinator shall make available its dated, current, in force outage coordination process for generation and Transmission outages within its Reliability Coordinator Area.

R2. Each Transmission Operator and Balancing Authority shall perform the functions specified in its Reliability Coordinator's outage coordination process. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M2. Each Transmission Operator and Balancing Authority shall provide evidence upon request that it performed the functions specified in its Reliability Coordinator's outage coordination process. Such evidence could include but is not limited to web postings with an electronic notice of the posting, dated operator logs, voice recordings, postal receipts showing the recipient, date and contents, or e-mail records.

R3. Each Planning Coordinator and Transmission Planner shall provide its Planning Assessment to impacted Reliability Coordinators. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

M3. Each Planning Coordinator and Transmission Planner shall provide evidence upon request showing that it provided its Planning Assessment to impacted Reliability Coordinators. Such evidence could include but is not limited to web postings with an electronic notice of the posting, dated operator logs, voice recordings, postal receipts showing the recipient, date and contents, or e-mail records.

R4. Each Planning Coordinator and Transmission Planner shall jointly develop solutions with its respective Reliability Coordinator(s) for identified issues or conflicts with planned outages in its Planning Assessment for the Near-Term Transmission Planning Horizon. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

M4. Each Planning Coordinator, and Transmission Planner shall provide evidence upon request showing that it jointly developed solutions with its respective Reliability Coordinator(s) for identified issues or conflicts with planned outages in its Planning Assessment for the Near-term Transmission Planning Horizon. Such evidence could include but is not limited to web postings with an electronic notice of the posting, dated operator logs, voice recordings, postal receipts showing the recipient, date and contents, or e-mail records.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Process

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Compliance Monitoring and Assessment Processes

As defined in the NERC Rules of Procedure, "Compliance Monitoring and Assessment Processes" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated reliability standard.

1.3. Data Retention

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

Each responsible entity shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation:

Each Reliability Coordinator shall retain its dated, current, in force, outage coordination process in accordance with Requirement R1 and Measurement M1 as well as any documents in force since the last compliance audit.

Each Transmission Operator and Balancing Authority shall retain evidence for three calendar years that it followed its Reliability Coordinator outage coordination process in accordance with Requirement R2 and Measurement M2.

Each Planning Coordinator and Transmission Planner shall retain evidence for three calendar years that it has its Planning Assessment to impacted Reliability Coordinators in accordance with Requirement R3 and Measurement M3.

Each Reliability Coordinator, Planning Coordinator, and Transmission Planner shall retain evidence for three calendar years that it has coordinated solutions within the Reliability Coordinator Area for identified issues or conflicts with planned outages in the Planning Assessment in accordance with Requirement R4 and Measurement M4.

If a responsible entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or the time period specified above, whichever is longer.

The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

1.4. Additional Compliance Information

None.

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	Operations Planning	Medium	The Reliability Coordinator did develop, implement, and maintain an outage coordination process for generation and Transmission outages within its Reliability Coordinator Area but it was missing one of the parts specified in Requirement R1 (Parts 1.1 – 1.4).	The Reliability Coordinator did develop, implement, and maintain an outage coordination process for generation and Transmission outages within its Reliability Coordinator Area but it was missing two of the parts specified in Requirement R1 (Parts 1.1 – 1.4).	The Reliability Coordinator did develop, implement, and maintain an outage coordination process for generation and Transmission outages within its Reliability Coordinator Area but it was missing three of the parts specified in Requirement R1 (Parts 1.1 – 1.4).	The Reliability Coordinator did develop, implement, and maintain an outage coordination process for generation and Transmission outages within its Reliability Coordinator Area but it was missing all four of the parts specified in Requirement R1 (Parts 1.1 – 1.4). OR, The Reliability Coordinator did not develop, implement, and maintain an outage coordination process for generation and Transmission outages within its Reliability Coordinator Area.
R2	Operations Planning	Medium	N/A	N/A	N/A	The Transmission Operator or Balancing Authority did not perform the functions specified in its Reliability Coordinator's outage coordination process.
R3	Operations Planning	Medium	N/A	N/A	N/A	The Planning Coordinator or Transmission Planner did not provide its Planning Assessment to impacted Reliability Coordinators.

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R4	Operations Planning	Medium	N/A	N/A	N/A	The Planning Coordinator or Transmission Planner did not jointly develop solutions with its respective Reliability Coordinator(s) for identified issues or conflicts with planned outages in its Planning Assessment for the Near-term Transmission Planning Horizon.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

Time Horizon: The official definition of the Operations Planning Time Horizon is: "operating and resource plans from day-ahead up to and including seasonal." The SDT equates 'seasonal' as being up to one year out and that these requirements covers the period from day-ahead to one year out.

Version History

Version	Date	Action	Change Tracking
1	April 2014	New standard developed by Project 2014-03	New
1	November 13, 2014	Adopted by NERC Board of Trustees	Revisions under Project 2014-03

Guidelines and Technical Basis

Rationale:

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

This standard is in response to issues raised in NOPR paragraph 90 and recommendations made by the Independent Expert Review Panel and SW Outage Report on the need for an outage coordination standard. It allows for one cohesive standard to address all outage coordination concerns as opposed to having multiple requirements spread throughout the various standards.

Rationale for Time Horizon:
The official definition of the Operations Planning Time Horizon is: "operating and resource plans from day-ahead up to and including seasonal." The SDT equates 'seasonal' as being up to one year out and that these requirements covers the period from day-ahead to one year out.

Rationale for R3:

Planning Assessment is a defined term and a document that Planning Coordinators and Transmission Planners already have to produce for approved TPL-001-4. It is not a compilation of load flow studies but a textual summary of what was found in those studies including rationales and assumptions.

Rationale for R4:
The SDT has re-written Requirement R4 to show that the process starts with the Planning Assessments created by the Planning Coordinator and Transmission Planner and then those Planning Assessments are reviewed and reconciled as needed with the Reliability Coordinator. This is in response to comments in paragraph 90 of the FERC NOPR about directly involving the Reliability Coordinator in the planning process for periods beyond the present one year outreach as well as recommendations in the IERP. The re-write should not be construed as relieving the Reliability Coordinator of responsibilities in this area but simply as a reflection of how the process actually starts.

In the future, the SDT believes that such coordination should take place in the TPL standards and to support that position, the SDT has created an item in a draft SAR for TPL-001-4 that would revise Requirement R8 to make the Reliability Coordinator an explicit party in the review process described there.

In addition, the SDT will submit a request to the Functional Model Working Team to adjust the roles and responsibilities of the Reliability Coordinator to this new paradigm.

*** FOR INFORMATIONAL PURPOSES ONLY ***

Enforcement Dates: Standard IRO-017-1 — Outage Coordination

United States

Standard	Requirement	Enforcement Date	Inactive Date
IRO-017-1	All		

This standard has not yet been approved by the applicable regulatory authority.

Printed On: March 24, 2015, 08:22 AM

Appendix QC-IRO-017-1
Provisions specific to the standard IRO-017-1 applicable in Québec

This appendix establishes specific provisions for the application of the standard in Québec. Provisions of the standard and of its appendix must be read together for the purposes of understanding and interpretation. Where the standard and appendix differ, the appendix shall prevail.

A. Introduction

1. Title: **Outage Coordination**

2. Number: IRO-017-1

3. Purpose: No specific provision

4. Applicability :

Functions

No specific provision

Facilities

This standard only applies to the facilities of the Main Transmission System (RTP).

5. Effective Date :

5.1. Adoption of the standard by the Régie de l'énergie: June 16, 2017

5.2. Adoption of the appendix by the Régie de l'énergie: June 16, 2017

5.3. Effective date of the standard and its appendix in Québec: July 1st, 2017

6. Background :

No specific provision

B. Requirements and Measures

No specific provision

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Process

The Régie de l'énergie is responsible, in Québec, for compliance monitoring with respect to the reliability standard and its appendix that it adopts.

1.2. Compliance Monitoring and Assessment Processes

Compliance Audit

Self-Certification

Spot Check

Compliance Investigation

Non-Compliance Self-Reporting

Periodic Data Submittal

Exception Reporting

Investigation following a complaint

1.3. Data Retention

No specific provision

1.4. Additional Compliance Information

No specific provision

2. Table of Compliance Elements

No specific provision

D. Regional Variances

No specific provision

E. Interpretations

No specific provision

F. Associated Documents

No specific provision

Guidelines and Technical Basis

No specific provision

Version History

Revision	Date	Action	Change Tracking
0	June 16, 2017	New appendix	New

A. Introduction

1. **Title:** **Reliability Coordinator Real-time Reliability Monitoring and Analysis Capabilities**

2. **Number:** **IRO-018-1(i)**

3. **Purpose:** Establish requirements for Real-time monitoring and analysis capabilities to support reliable System operations.

4. **Applicability:**

   4.1. Functional Entities:

   4.1.1. Reliability Coordinators

5. **Effective Date:** See Implementation Plan

B. Requirements and Measures

R1. Each Reliability Coordinator shall implement an Operating Process or Operating Procedure to address the quality of the Real-time data necessary to perform its Real-time monitoring and Real-time Assessments. The Operating Process or Operating Procedure shall include: *[Violation Risk Factor: High] [Time Horizon: Real-time Operations]*

1.1. Criteria for evaluating the quality of Real-time data;

1.2. Provisions to indicate the quality of Real-time data to the System Operator; and

1.3. Actions to address Real-time data quality issues with the entity(ies) responsible for providing the data when data quality affects Real-time Assessments.

M1. Each Reliability Coordinator shall have evidence it implemented its Operating Process or Operating Procedure to address the quality of the Real-time data necessary to perform its Real-time monitoring and Real-time Assessments. This evidence could include, but is not limited to: 1) an Operating Process or Operating Procedure in electronic or hard copy format meeting all provisions of Requirement R1; and 2) evidence the Reliability Coordinator implemented the Operating Process or Operating Procedure as called for in the Operating Process or Operating Procedure, such as dated operator or supporting logs, dated checklists, voice recordings, voice transcripts, or other evidence.

R2. Each Reliability Coordinator shall implement an Operating Process or Operating Procedure to address the quality of analysis used in its Real-time Assessments. The Operating Process or Operating Procedure shall include: *[Violation Risk Factor: Medium] [Time Horizon: Real-time Operations]*

2.1. Criteria for evaluating the quality of analysis used in its Real-time Assessments;

2.2. Provisions to indicate the quality of analysis used in its Real-time Assessments; and

2.3. Actions to address analysis quality issues affecting its Real-time Assessments.

M2. Each Reliability Coordinator shall have evidence it implemented its Operating Process or Operating Procedure to address the quality of analysis used in its Real-time Assessments as specified in Requirement R2. This evidence could include, but is not limited to: 1) an Operating Process or Operating Procedure in electronic or hard copy format meeting all provisions of Requirement R2; and 2) evidence the Reliability Coordinator implemented the Operating Process or Operating Procedure as called for in the Operating Process or Operating Procedure, such as dated operator logs, dated checklists, voice recordings, voice transcripts, or other evidence.

R3. Each Reliability Coordinator shall have an alarm process monitor that provides notification(s) to its System Operators when a failure of its Real-time monitoring alarm processor has occurred. *[Violation Risk Factor: Medium] [Time Horizon: Real-time Operations]*

M3. Each Reliability Coordinator shall have evidence of an alarm process monitor that provides notification(s) to its System Operators when a failure of its Real-time monitoring alarm processor has occurred. This evidence could include, but is not limited to, operator logs, computer printouts, system specifications, or other evidence.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority:
"Compliance Enforcement Authority" means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention:
The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show it was compliant for the full-time period since the last audit.

The Reliability Coordinator shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

The Reliability Coordinator shall retain evidence of compliance for Requirements R1 and R3 and Measures M1 and M3 for the current calendar year and one previous calendar year, with the exception of operator logs and

voice recordings which shall be retained for a minimum of 90 calendar days, unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

The Reliability Coordinator shall retain evidence of compliance for Requirement R2 and Measure M2 for a rolling 30-day period, unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

If a Reliability Coordinator is found non-compliant it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.

The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program

As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	N/A	The Reliability Coordinator's Operating Process or Operating Procedure to address the quality of the Real-time data necessary to perform its Real-time monitoring and Real-time Assessments did not include one of the elements listed in Part 1.1 through Part 1.3.	The Reliability Coordinator's Operating Process or Operating Procedure to address the quality of the Real-time data necessary to perform its Real-time monitoring and Real-time Assessments did not include two of the elements listed in Part 1.1 through Part 1.3.	The Reliability Coordinator's Operating Process or Operating Procedure to address the quality of the Real-time data necessary to perform its Real-time monitoring and Real-time Assessments did not include any of the elements listed in Part 1.1 through Part 1.3; OR The Reliability Coordinator did not implement an Operating Process or Operating Procedure to address the quality of the Real-time data necessary to perform its Real-time monitoring and Real-time Assessments.
R2.	N/A	The Reliability Coordinator's Operating Process or Operating Procedure to address the quality of	The Reliability Coordinator's Operating Process or Operating Procedure to address the quality of	The Reliability Coordinator's Operating Process or Operating Procedure to address the quality of

		analysis used in its Real-time Assessments did not include one of the elements listed in Part 2.1 through Part 2.3.	analysis used in its Real-time Assessments did not include two of the elements listed in Part 2.1 through Part 2.3.	analysis used in its Real-time Assessments did not include any of the elements listed in Part 2.1 through Part 2.3; OR The Reliability Coordinator did not implement an Operating Process or Operating Procedure to address the quality of analysis used in its Real-time Assessments.
R3.	N/A	N/A	The Reliability Coordinator has an alarm process monitor but the alarm process monitor did not provide a notification(s) to its System Operators when a failure of its Real-time monitoring alarm processor occurred.	The Reliability Coordinator does not have an alarm process monitor that provides notification(s) to its System Operators when a failure of its Real-time monitoring alarm processor has occurred.

D. Regional Variances

None.

E. Associated Documents

- Implementation Plan

Version History

Version	Date	Action	Change Tracking
1	October 30, 3015	New standard developed in Project 2009-02 to respond to recommendations in Real-time Best Practices Task Force Report and FERC directives.	N/A
1	May 5, 2016	Adopted by the Board of Trustees.	New
1	September 22, 2016	FERC Order issued approving IRO-018-1. Docket No. RD16-6-000	
1(i)	September 22, 2016	FERC directive to change Requirement 1 from 'medium' to 'high'. Docket No. RD16-6-000	Revised
1(i)	November 2, 2016	Adopted by the Board of Trustees	New
1(i)	December 14, 2016	FERC letter Order approving revisions to the VRFs for R1 from 'medium' to 'high'. Docket No. RD16-6-001.	

Guidelines and Technical Basis

Real-time monitoring, or *monitoring* the Bulk Electric System (BES) in Real-time, is a primary function of Reliability Coordinators (RCs), Transmission Operators (TOPs), and Balancing Authorities (BAs) as required by TOP and IRO Reliability Standards. As used in TOP and IRO Reliability Standards, monitoring involves observing operating status and operating values in Real-time for awareness of system conditions. Real-time monitoring may include the following activities performed in Real-time:

- Acquisition of operating data;
- Display of operating data as needed for visualization of system conditions;
- Audible or visual alerting when warranted by system conditions; and
- Audible or visual alerting when monitoring and analysis capabilities degrade or become unavailable.

Requirement R1

The RC uses a set of Real-time data identified in IRO-010-1a Requirement R1 and IRO-010-2 Requirement R1 to perform its Real-time monitoring and Real-time Assessments. Requirements to perform monitoring and Real-time Assessments appear in other Reliability Standards.

The RC's Operating Process or Operating Procedure must contain criteria for evaluating the quality of Real-time data as specified in proposed IRO-018-1 Requirement R1 Part 1.1. The criteria support identification of applicable data quality issues, which may include:

- Data outside of a prescribed data range;
- Analog data not updated within a predetermined time period;
- Data entered manually to override telemetered information; or
- Data otherwise identified as invalid or suspect.

The Operating Process or Operating Procedure must include provisions for indicating the quality of Real-time data to operating personnel. Descriptions of quality indicators such as display color codes, data quality flags, or other such indicators as found in Real-time monitoring specifications could be used.

Requirement R1 Part 1.3 specifies the RC shall include actions to address Real-time data quality issues with the entity(ies) responsible for providing the data when data quality affects Real-time Assessments. Requirement R1 Part 1.3 is focused on addressing data point quality issues affecting Real-time Assessments. Other data quality issues of a lower priority are addressed according to an entity's operating practices and are not covered under Requirement R1 Part 1.3.

The RC's actions to address data quality issues are steps within existing authorities and capabilities that provide awareness and enable the RC to meet its obligations for performing the Real-time Assessment. Examples of actions to address data quality issues include, but are not limited to, the following:

- Notifying entities that provide Real-time data to the RC;

- Following processes established for resolving data conflicts as specified in IRO-010-1a, IRO-010-2, or other applicable Reliability Standards;
- Taking corrective actions on the RC's own data;
- Changing data sources or other inputs so that the data quality issue no longer affects the RC's Real-time Assessment; and
- Inputting data manually and updating as necessary.

The Operating Process or Operating Procedure must clearly identify to operating personnel how to determine the data that affects the quality of the Real-time Assessment so that effective actions can be taken to address data quality issues in an appropriate timeframe.

Requirement R2

Requirement R2 ensures RCs have procedures to address issues related to the quality of the analysis results used for Real-time Assessments. Requirements to perform Real-time Assessments appear in other Reliability Standards. Examples of the types of analysis used in Real-time Assessments include, as applicable, state estimation, Real-time Contingency analysis, Stability analysis or other studies used for Real-time Assessments.

Examples of the types of criteria used to evaluate the quality of analysis used in Real-time Assessments may include solution tolerances, mismatches with Real-time data, convergences, etc.

The Operating Process or Operating Procedure must describe how the quality of analysis results used in Real-time Assessment will be shown to operating personnel.

Requirement R3

Requirement R3 addresses recommendation S7 of the Real-time Best Practices Task Force report concerning operator awareness of alarm availability.

An alarm process monitor could be an application within a Real-time monitoring system or it could be a separate system. 'Heartbeat' or 'watchdog' monitors are examples of an alarm process monitor. An alarm process monitor should be designed and implemented such that a stall of the Real-time monitoring alarm processor does not cause a failure of the alarm process monitor.

Rationale

Rationale for Requirement R1: The Reliability Coordinator (RC) uses a set of Real-time data identified in IRO-010-1a Requirement R1 and IRO-010-2 Requirement R1 to perform its Real-time monitoring and Real-time Assessments. Requirements to perform Real-time monitoring and Real-time Assessments appear in other Reliability Standards.

The Operating Process or Operating Procedure must include provisions for indicating the quality of Real-time data to operating personnel. Descriptions of quality indicators such as display color codes, data quality flags, or other such indicators as found in Real-time monitoring specifications could be used.

Requirement R1 Part 1.3 of this standard specifies the RC shall include actions to address Real-time data quality issues affecting its Real-time Assessments in its Operating Process or Operating Procedure. Examples of actions to address Real-time data quality issues are provided in the Guidelines and Technical Basis section. These actions could be the same as the process used to resolve data conflicts required by IRO-010-2 Requirement R3 Part 3.2 provided that this process addresses Real-time data quality issues.

The revision in Part 1.3 to address Real-time data quality issues *when data quality affects Real-time Assessments* clarifies the scope of data points that must be covered by the Operating Process or Operating Procedure.

Rationale for Requirement R2: Requirement R2 ensures RCs have procedures to address issues related to the quality of the analysis results used for Real-time Assessments. Requirements to perform Real-time Assessments appear in other Reliability Standards. Examples of the types of analysis used in Real-time Assessments include, as applicable, state estimation, Real-time Contingency analysis, Stability analysis or other studies used for Real-time Assessments.

The Operating Process or Operating Procedure must include provisions for how the quality of analysis results used in Real-time Assessment will be shown to operating personnel. Operating personnel includes System Operators and staff responsible for supporting Real-time operations.

Rationale for Requirement R3: The requirement addresses recommendation S7 of the Real-time Best Practices Task Force report concerning operator awareness of alarm availability.

The requirement in Draft Two of the proposed standard has been revised for clarity by removing the term *independent*. The alarm process monitor must be able to provide notification of failure of the Real-time monitoring alarm processor. This capability could be provided by an application within a Real-time monitoring system or by a separate component used by the System Operator. The alarm process monitor must not fail with a simultaneous failure of the Real-time monitoring alarm processor.

Appendix IRO-018-1(i)-QC-1

Specific provisions applicable in Québec for standard IRO-018-1(i) – Reliability Coordinator Real-time Reliability Monitoring and Analysis Capabilities

This appendix establishes specific provisions for the application of the standard in Québec. Provisions of the standard and of this appendix must be read jointly for comprehension and interpretation purposes. Where the standard and appendix differ, the appendix shall prevail.

A. Introduction

1. Title: No specific provisions.

2. Number: No specific provisions.

3. Purpose: No specific provisions.

4. Applicability:

4.1. Functional Entities

No specific provisions.

5. Effective date:

5.1.	Adoption of the standard by the Régie de l'énergie:	June 9, 2020
5.2.	Adoption of this appendix by the Régie de l'énergie:	June 9, 2020
5.3.	Effective date of the standard and of this appendix in Québec:	January 1, 2022

B. Requirements and Measures

No specific provisions.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

In Québec, "Compliance Enforcement Authority" means the Régie de l'énergie in its roles of monitoring and enforcing compliance with respect to the Reliability Standard and to this appendix.

1.2. Evidence Retention

No specific provisions.

1.3. Compliance Monitoring and Enforcement Program

The Régie de l'énergie establishes the monitoring processes used to evaluate data or information for the purpose of determining compliance or non-compliance with the Reliability Standard and with this appendix.

Violation Severity Levels

No specific provisions.

D. Regional Variances

No specific provisions.

E. Associated Documents

No specific provisions.

Appendix IRO-018-1(i)-QC-1

Specific provisions applicable in Québec for standard IRO-018-1(i) – Reliability Coordinator Real-time Reliability Monitoring and Analysis Capabilities

Guidelines and Technical Basis

No specific provisions.

Rationale

No specific provisions.

Version history

Version	Date	Action	Change tracking
1	June 9, 2020	New appendix	New

A. Introduction

1. Title: Verification and Data Reporting of Generator Real and Reactive Power Capability and Synchronous Condenser Reactive Power Capability

2. Number: MOD-025-2

3. Purpose: To ensure that accurate information on generator gross and net Real and Reactive Power capability and synchronous condenser Reactive Power capability is available for planning models used to assess Bulk Electric System (BES) reliability.

4. Applicability:

4.1. Functional entities

4.1.1 Generator Owner

4.1.2 Transmission Owner that owns synchronous condenser(s)

4.2. Facilities:

For the purpose of this standard, the term, "applicable Facility" shall mean any one of the following:

4.2.1 Individual generating unit greater than 20 MVA (gross nameplate rating) directly connected to the Bulk Electric System.

4.2.2 Synchronous condenser greater than 20 MVA (gross nameplate rating) directly connected to the Bulk Electric System.

4.2.3 Generating plant/Facility greater than 75 MVA (gross aggregate nameplate rating) directly connected to the Bulk Electric System.

5. Effective Date:

5.1. In those jurisdictions where regulatory approval is required[1]:

5.1.1 By the first day of the first calendar quarter, two calendar years following applicable regulatory approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities, each Generator Owner and Transmission Owner shall have verified at least 40 percent of its applicable Facilities.

5.1.2 By the first day of the first calendar quarter, three calendar years following applicable regulatory approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities, each Generator Owner and Transmission Owner shall have verified at least 60 percent of its applicable Facilities.

5.1.3 By the first day of the first calendar quarter, four calendar years following applicable regulatory approval, or as otherwise made effective pursuant to

[1] Wind Farm Verification - If an entity has two wind sites, and verification of one site is complete, the entity is 50% complete regardless of the number of turbines at each site. A wind site is a group of wind turbines connected at a common point of interconnection or utilizing a common aggregate control system.

the laws applicable to such ERO governmental authorities, each Generator Owner and Transmission Owner shall have verified at least 80 percent of its applicable Facilities.

5.1.4 By the first day of the first calendar quarter, five calendar years following applicable regulatory approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities, each Generator Owner and Transmission Owner shall have verified 100 percent of its applicable Facilities.

5.2. In those jurisdictions where regulatory approval is not required[2]:

5.2.1 By the first day of the first calendar quarter, two calendar years following Board of Trustees approval, each Generator Owner and Transmission Owner shall have verified at least 40 percent of its applicable Facilities.

5.2.2 By the first day of the first calendar quarter, three calendar years following Board of Trustees approval, each Generator Owner and Transmission Owner shall have verified at least 60 percent of its applicable Facilities.

5.2.3 By the first day of the first calendar quarter, four calendar years following Board of Trustees approval, each Generator Owner and Transmission Owner shall have verified at least 80 percent of its applicable Facilities.

5.2.4 By the first day of the first calendar quarter, five calendar years following Board of Trustees approval, each Generator Owner and Transmission Owner shall have verified 100 percent of its applicable Facilities.

Note: The verification percentage above is based on the number of applicable units owned.

[2] Wind farm verification - If an entity has two wind sites, and verification of one site is complete, the entity is 50% complete regardless of the number of turbines at each site. A wind site is a group of wind turbines connected at a common point of interconnection or utilizing a common aggregate control system.

Requirements

R1. Each Generator Owner shall provide its Transmission Planner with verification of the Real Power capability of its applicable Facilities as follows: *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

1.1. Verify the Real Power capability of its generating units in accordance with Attachment 1.

1.2. Submit a completed Attachment 2 (or a form containing the same information as identified in Attachment 2) to its Transmission Planner within 90 calendar days of either (i) the date the data is recorded for a staged test; or (ii) the date the data is selected for verification using historical operational data.

R2. Each Generator Owner shall provide its Transmission Planner with verification of the Reactive Power capability of its applicable Facilities as follows: *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

2.1. Verify, in accordance with Attachment 1, (i) the Reactive Power capability of its generating units and (ii) the Reactive Power capability of its synchronous condenser units.

2.2. Submit a completed Attachment 2 (or a form containing the same information as identified in Attachment 2) to its Transmission Planner within 90 calendar days of either (i) the date the data is recorded for a staged test; or (ii) the date the data is selected for verification using historical operational data.

R3. Each Transmission Owner shall provide its Transmission Planner with verification of the Reactive Power capability of its applicable Facilities as follows: *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

3.1. Verify, in accordance with Attachment 1, the Reactive Power capability of its synchronous condenser units.

3.2. Submit a completed Attachment 2 (or a form containing the same information as identified in Attachment 2) to its Transmission Planner within 90 calendar days of either (i) the date the data is recorded for a staged test; or (ii) the date the data is selected for verification using historical operational data.

B. Measures

M1. Each Generator Owner will have evidence that it performed the verification, such as a completed Attachment 2 or the Generator Owner form with the same information or dated information collected and used to complete attachments, and will have evidence that it submitted the information within 90 days to its Transmission Planner; such as dated electronic mail messages or mail receipts in accordance with Requirement R1.

M2. Each Generator Owner will have evidence that it performed the verification, such as a completed Attachment 2 or the Generator Owner form with the same information, or dated information collected and used to complete attachments and will have evidence that it submitted the information within 90 days to its Transmission Planner; such as dated electronic mail messages or mail receipts in accordance with Requirement R2.

M3. Each Transmission Owner will have evidence that it performed the verification, such as a completed Attachment 2 or the Transmission Owner form with equivalent information or dated information collected and used to complete attachments, and will have evidence that it submitted the information within 90 days to its Transmission Planner; such as dated electronic mail messages or mail receipts in accordance with Requirement R3.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

The Regional Entity shall serve as the Compliance enforcement authority unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention

The following evidence retention periods identify a period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention specified below is shorter than the time since the last compliance audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Generator Owner and Transmission Owner shall each keep the data or evidence to show compliance as identified below, unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation:

- The Generator Owner shall retain the latest MOD-025 Attachment 2 and the data behind Attachment 2 or Generator Owner form with equivalent information and submittal evidence for Requirements R1 and R2, Measures M1 and M2 for the time period since the last compliance audit.
- The Transmission Owner shall retain the latest MOD-025 Attachment 2 and the data behind Attachment 2 or Transmission Owner form with equivalent information and submittal evidence for Requirement R3, Measure M3 for the time period since the last compliance audit.

If a Generator Owner or Transmission Owner is found noncompliant, it shall keep information related to the noncompliance until mitigation is complete or for the time specified above, whichever is longer.

The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes

Compliance Audit

Self-Certification

Spot Checking

Compliance Investigation

Self-Reporting

Complaint

1.4. Additional Compliance Information

None

2. Violation Severity Levels

R #	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	The Generator Owner verified and recorded the Real Power capability of its applicable generating unit, but submitted the data to its Transmission Planner more than 90 calendar days, but within 120 calendar days, of the date the data is recorded for a staged test or the date the data is selected for verification using historical operational data. OR The Generator Owner verified the Real Power capability, per Attachment 1 and submitted the data but was missing 1 to less than or equal to 33 percent of the data.	The Generator Owner verified and recorded the Real Power capability of its applicable generating unit, but submitted the data to its Transmission Planner more than 120 calendar days, but within 150 calendar days, of the date the data is recorded for a staged test or the date the data is selected for verification using historical operational data. OR The Generator Owner verified the Real Power capability, per Attachment 1 and submitted the data but was missing more than 33 to 66 percent of the data.	The Generator Owner verified and recorded the Real Power capability of its applicable generating unit, but submitted the data to its Transmission Planner more than 150 calendar days, but within 180 calendar days, of the date the data is recorded for a staged test or the date the data is selected for verification using historical operational data. OR The Generator Owner verified the Real Power capability, per Attachment 1 and submitted the data but was missing from 67 to 99 percent of the data. OR	The Generator Owner verified and recorded the Real Power capability of its applicable generating unit, but submitted the data to its Transmission Planner more than 180 calendar days of the date the data is recorded for a staged test or the date the data is selected for verification using historical operational data. OR The Generator Owner failed to verify the Real Power capability, per Attachment 1 of an applicable generating unit. OR The Generator Owner performed the Real Power verification per Attachment 1, “Periodicity for conducting a new verification” item

	OR The Generator Owner performed the Real Power verification per Attachment 1, "Periodicity for conducting a new verification" item 1 or item 2 (5 year requirement) but did so in more than 66 calendar months but less than or equal to 69 months. OR The Generator Owner performed the Real Power verification per Attachment 1, "Periodicity for conducting a new verification" item 1, 2 or 3 (12 calendar month requirement) but did so in more than 12 calendar months but less than or equal to 13 calendar months.	OR The Generator Owner performed the Real Power verification per Attachment 1, "Periodicity for conducting a new verification" item 1 or item 2 (5 year requirement) but did so in more than 69 calendar months but less than or equal to 72 months. OR The Generator Owner performed the Real Power verification per Attachment 1, "Periodicity for conducting a new verification" item 1, 2 or 3 (12 calendar month requirement) but did so in more than 13 calendar months but less than or equal to 14 calendar months.	The Generator Owner performed the Real Power verification per Attachment 1, "Periodicity for conducting a new verification" item 1 or item 2 (5 year requirement) but did so in more than 72 calendar months but less than or equal to 75 months. OR The Generator Owner performed the Real Power verification per Attachment 1, "Periodicity for conducting a new verification" item 1, 2 or 3 (12 calendar month requirement) but did so in more than 14 calendar months but less than or equal to 15 calendar months.	1 or item 2 (5 year requirement) but did so in more than 75 calendar months. OR The Generator Owner performed the Real Power verification per Attachment 1, "Periodicity for conducting a new verification" item 1, 2 or 3 (12 calendar month requirement) but did so in more than 15 calendar months.
R2	The Generator Owner verified and recorded the	The Generator Owner verified and recorded the	The Generator Owner verified and recorded the Reactive	The Generator Owner verified and recorded the Reactive Power

	Reactive Power capability of its applicable generating unit or applicable synchronous condenser, but submitted the data to its Transmission Planner more than 90 calendar days, but within 120 calendar days, of the date the data is recorded for a staged test or the date the data is selected for verification using historical operational data. OR The Generator Owner verified the Reactive Power capability, per Attachment 1 and submitted the data but was missing 1 to up to and including 33 percent of the data. OR The Generator Owner performed the Reactive Power verification per	Reactive Power capability of its applicable generating unit or applicable synchronous condenser, but submitted the data to its Transmission Planner more than 120 calendar days, but within 150 calendar days, of the date the data is recorded for a staged test or the date the data is selected for verification using historical operational data. OR The Generator Owner verified the Reactive Power capability, per Attachment 1 and submitted the data but was missing 34 to 66 percent of the data. OR The Generator Owner performed the Reactive Power verification per Attachment 1, "Periodicity for conducting a new verification" item 1 or item 2	Power capability of its applicable generating unit or applicable synchronous condenser, but submitted the data to its Transmission Planner more than 150 calendar days, but within 180 calendar days, of the date the data is recorded for a staged test or the date the data is selected for verification using historical operational data. OR The Generator Owner verified the Reactive Power capability, per Attachment 1 and submitted the data but was missing 67 to 99 percent of the data. OR The Generator Owner performed the Reactive Power verification per Attachment 1, "Periodicity for conducting a new verification" item 1 or item 2 (5 year requirement) but did so in more than 72	capability of its applicable generating unit or applicable synchronous condenser, but submitted the data to its Transmission Planner more than 180 calendar days of the date the data is recorded for a staged test or the date the data is selected for verification using historical operational data. OR The Generator Owner failed to verify the Reactive Power capability, per Attachment 1 of an applicable generating unit or synchronous condenser unit. OR The Generator Owner performed the Reactive Power verification per Attachment 1, "Periodicity for conducting a new verification" item 1 or item 2 (5 year requirement) but did so in more than 75 calendar months. OR

	Attachment 1, "Periodicity for conducting a new verification" item 1 or item 2 (5 year requirement) but did so in more than 66 calendar months but less than or equal to 69 months. OR The Generator Owner performed the Reactive Power verification per Attachment 1, "Periodicity for conducting a new verification" item 1, 2 or 3 (12 calendar month requirement) but did so in more than 12 calendar months but less than or equal to 13 calendar months.	(5 year requirement) but did so in more than 69 calendar months but less than or equal to 72 months. OR The Generator Owner performed the Reactive Power verification per Attachment 1, "Periodicity for conducting a new verification" item 1, 2 or 3 (12 calendar month requirement) but did so in more than 13 calendar months but less than or equal to 14 calendar months.	calendar months but less than or equal to 75 months. OR The Generator Owner performed the Reactive Power verification per Attachment 1, "Periodicity for conducting a new verification" item 1, 2 or 3 (12 calendar month requirement) but did so in more than 14 calendar months but less than or equal to 15 calendar months.	The Generator Owner performed the Reactive Power verification per Attachment 1, "Periodicity for conducting a new verification" item 1, 2 or 3 (12 calendar month requirement) but did so in more than 15 calendar months.
R3	The Transmission Owner verified and recorded the Reactive Power capability of its applicable synchronous condenser, but submitted the data to its Transmission Planner more	The Transmission Owner verified and recorded the Reactive Power capability of its applicable synchronous condenser, but submitted the data to its Transmission Planner more than 120	The Transmission Owner verified and recorded the Reactive Power capability of an applicable synchronous condenser unit, but submitted the data to its Transmission Planner more than 150	The Transmission Owner verified and recorded the Reactive Power capability of its applicable synchronous condenser, but submitted the data to its Transmission Planner more than 180 calendar days of the date the data is

	than 90 calendar days, but within 120 calendar days, of the date the data is recorded for a staged test or the date the data is selected for verification using historical operational data. OR The Transmission Owner verified the Reactive Power capability, per Attachment 1 and submitted the data but was missing 1 to up to and including 33 percent of the data. OR The Transmission Owner performed the Reactive Power verification per Attachment 1, "Periodicity for conducting a new verification" item 1 or item 2 (5 year requirement) but did so in more than 66 calendar months but less	calendar days, but within 150 calendar days, of the date the data is recorded for a staged test or the date the data is selected for verification using historical operational data. OR The Transmission Owner verified the Reactive Power capability, per Attachment 1 and submitted the data but was missing 34 to 66 percent of the data. OR The Transmission Owner performed the Reactive Power verification per Attachment 1, "Periodicity for conducting a new verification" item 1 or item 2 (5 year requirement) but did so in more than 69 calendar months but less than or equal to 72 months.	calendar days, but within 180 calendar days, of the date the data is recorded for a staged test or the date the data is selected for verification using historical operational data. OR The Transmission Owner verified the Reactive Power capability, per Attachment 1 and submitted the data but was missing 67 to 99 percent of the data. OR The Transmission Owner performed the Reactive Power verification per Attachment 1, "Periodicity for conducting a new verification" item 1 or item 2 (5 year requirement) but did so in more than 72 calendar months but less than or equal to 75 months.	recorded for a staged test or the date the data is selected for verification using historical operational data. OR The Transmission Owner failed to verify the Reactive Power capability, per Attachment 1 of an applicable synchronous condenser unit. OR The Transmission Owner performed the verification per Attachment 1, "Periodicity for conducting a new verification" item 1 or item 2 (5 year requirement) but did so in more than 75 calendar months. OR The Transmission Owner performed the Reactive Power verification per Attachment 1, "Periodicity for conducting a new verification" item 1, 2 or 3 (12 calendar month requirement) but did so in more than 15calendar months.

	than or equal to 69 months. OR The Transmission Owner performed the Reactive Power verification per Attachment 1, "Periodicity for conducting a new verification" item 1, 2 or 3 (12 calendar month requirement) but did so in more than 12 calendar months but less than or equal to 13 calendar months.	OR The Transmission Owner performed the Reactive Power verification per Attachment 1, "Periodicity for conducting a new verification" item 1, 2 or 3 (12 calendar month requirement) but did so in more than 13 calendar months but less than or equal to 14 calendar months.	OR The Transmission Owner performed the Reactive Power verification per Attachment 1, "Periodicity for conducting a new verification" item 1, 2 or 3 (12 calendar month requirement) but did so in more than 14 calendar months but less than or equal to 15 calendar months.	

D. Regional Variances

None

E. Associated Documents

Version History

Version	Date	Action	Change Tracking
1	12/1/2005	1. Changed tabs in footer. 2. Removed comma after 2004 in "Development Steps Completed," #1. 3. Changed incorrect use of certain hyphens (-) to "en dash" (–) and "em dash (—)." 4. Added "periods" to items where appropriate. 5. Changed apostrophes to "smart" symbols. 6. Changed "Timeframe" to "Time Frame" in item D, 1.2. 7. Lower cased all instances of "regional" in section D.3. 8. Removed the word "less" after 94% in section 3.4. Level 4.	01/20/06
2	February 7, 2013	Adopted by NERC Board of Trustees	Revised per SAR for Project 2007-09 and combined with MOD-024-1
2	March 20, 2014	FERC Order issued approving MOD-025-2. (Order becomes effective on 7/1/16.)	

MOD-025 Attachment 1 – Verification of Generator Real and Reactive Power Capability and Synchronous Condenser Reactive Power Capability

Periodicity for conducting a new verification:

The periodicity for performing Real and Reactive Power capability verification is as follows:

1. For staged verification; verify each applicable Facility at least every five years (with no more than 66 calendar months between verifications), or within 12 calendar months of the discovery of a change that affects its Real Power or Reactive Power capability by more than 10 percent of the last reported verified capability and is expected to last more than six months. The first verification for each applicable Facility under this standard must be a staged test.
2. For verification using operational data; verify each applicable Facility at least every five years (with no more than 66 calendar months between verifications), or within 12 calendar months following the discovery that its Real Power or Reactive Power capability has changed by more than 10 percent of the last reported verified capability and is expected to last more than six months. If data for different points is recorded on different days, designate the earliest of those dates as the verification date, and report that date as the verification date on MOD-025, Attachment 2 for periodicity purposes.
3. For either verification method, verify each new applicable Facility within 12 calendar months of its commercial operation date. Existing units that have been in long term shut down and have not been tested for more than five years shall be verified within 12 calendar months.

It is intended that Real Power testing be performed at the same time as full load Reactive Power testing, however separate testing is allowed for this standard. For synchronous condensers, perform only the Reactive Power capability verifications as specified below.

If the Reactive Power capability is verified through test, it is to be scheduled at a time advantageous for the unit being verified to demonstrate its Reactive Power capabilities while the Transmission Operator takes measures to maintain the plant's system bus voltage at the scheduled value or within acceptable tolerance of the scheduled value.

Verification specifications for applicable Facilities:

1. For generating units of 20 MVA or less that are part of a plant greater than 75 MVA in aggregate, record data either on an individual unit basis or as a group. Perform verification individually for every generating unit or synchronous condenser greater than 20 MVA (gross nameplate rating).

2. Verify with all auxiliary equipment needed for expected normal operation in service for both the Real Power and Reactive Power capability verification. Perform verification with the automatic voltage regulator in service for the Reactive Power capability

verification. Operational data from within the two years prior to the verification date is acceptable for the verification of either the Real Power or the Reactive Power capability, as long as a) that operational data meets the criteria in 2.1 through 2.4 below and b) the operational data demonstrates at least 90 percent of a previously staged test that demonstrated at least 50 percent of the Reactive capability shown on the associated thermal capability curve (D-curve). If the previously staged test was unduly restricted (so that it did not demonstrate at least 50 percent of the associated thermal capability curve) by unusual generation or equipment limitations (e.g., capacitor or reactor banks out of service), then the next verification will be by another staged test, not operational data:

2.1. Verify Real Power capability and Reactive Power capability over-excited (lagging) of all applicable Facilities at the applicable Facilities' normal (not emergency) expected maximum Real Power output at the time of the verifications.

2.1.1 Verify synchronous generating unit's maximum real power and lagging reactive power for a minimum of one hour.

2.1.2 Verify variable generating units, such as wind, solar, and run of river hydro, at the maximum Real Power output the variable resource can provide at the time of the verification. Perform verification of Reactive Power capability of wind turbines and photovoltaic inverters with at least 90 percent of the wind turbines or photovoltaic inverters at a site on-line. If verification of wind turbines or photovoltaic inverter Facility cannot be accomplished meeting the 90 percent threshold, document the reasons the threshold was not met and test to the full capability at the time of the test. Reschedule the test of the facility within six months of being able to reach the 90 percent threshold. Maintain, as steady as practical, Real and Reactive Power output during verifications.

2.2. Verify Reactive Power capability of all applicable Facilities, other than wind and photovoltaic, for maximum overexcited (lagging) and under-excited (leading) reactive capability for the following conditions:

2.2.1 At the minimum Real Power output at which they are normally expected to operate collect maximum leading and lagging reactive values as soon as a limit is reached.

2.2.2 At maximum Real Power output collect maximum leading reactive values as soon as a limit is reached.

2.2.3 Nuclear Units are not required to perform Reactive Power verification at minimum Real Power output.

2.3. For hydrogen-cooled generators, perform the verification at normal operating hydrogen pressure.

2.4. Calculate the Generator Step-Up (GSU) transformer losses if the verification measurements are taken from the high side of the GSU transformer. GSU

transformer real and reactive losses may be estimated, based on the GSU impedance, if necessary.

3. Record the following data for the verifications specified above:

3.1. The value of the gross Real and Reactive Power generating capabilities at the end of the verification period.

3.2. The voltage schedule provided by the Transmission Operator, if applicable.

3.3. The voltage at the high and low side of the GSU and/or system interconnection transformer(s) at the end of the verification period. If only one of these values is metered, the other may be calculated.

3.4. The ambient conditions, if applicable, at the end of the verification period that the Generator Owner requires to perform corrections to Real Power for different ambient conditions such as:

- Ambient air temperature
- Relative humidity
- Cooling water temperature
- Other data as determined to be applicable by the Generator Owner to perform corrections for ambient conditions.

3.5. The date and time of the verification period, including start and end time in hours and minutes.

3.6. The existing GSU and/or system interconnection transformer(s) voltage ratio and tap setting.

3.7. The GSU transformer losses (real or reactive) if the verification measurements were taken from the high side of the GSU transformer.

3.8. Whether the test data is a result of a staged test or if it is operational data.

4. Develop a simplified key one-line diagram (refer to MOD-025, Attachment 2) showing sources of auxiliary Real and Reactive Power and associated system connections for each unit verified. Include GSU and/or system Interconnection and auxiliary transformers. Show Reactive Power flows, with directional arrows.

4.1. If metering does not exist to measure specific Reactive auxiliary load(s), provide an engineering estimate and associated calculations. Transformer Real and Reactive Power losses will also be estimates or calculations. Only output data are required when using a computer program to calculate losses or loads.

5. If an adjustment is requested by the Transmission Planner, then develop the relationships between test conditions and generator output so that the amount of Real Power that can be expected to be delivered from a generator can be determined at different conditions, such as peak summer conditions. Adjust MW values tested to the ambient conditions specified by the Transmission Planner upon request and submit them to the Transmission Planner within 90 days of the request or the date the data was recorded/selected whichever is later.

Note 1: Under some transmission system conditions, the data points obtained by the Mvar verification required by the standard will not duplicate the manufacturer supplied thermal capability curve (D-curve). However, the verification required by the standard, even when conducted under these transmission system conditions, may uncover applicable Facility limitations; such as rotor thermal instability, improper tap settings or voltage ratios, inaccurate AVR operation, etc., which could be further analyzed for resolution. The Mvar limit level(s) achieved during a staged test or from operational data may not be representative of the unit's reactive capability for extreme system conditions. See Note 2.

Note 2: While not required by the standard, it is desirable to perform engineering analyses to determine expected applicable Facility capabilities under less restrictive system voltages than those encountered during the verification. Even though this analysis will not verify the complete thermal capability curve (D-curve), it provides a reasonable estimate of applicable Facility capability that the Transmission Planner can use for modeling.

Note 3: The Reactive Power verification is intended to define the limits of the unit's Reactive Power capabilities. If a unit has no leading capability, then it should be reported with no leading capability; or the minimum lagging capability at which it can operate.

Note 4: Synchronous Condensers only need to be tested at two points (one over-excited point and one under-excited point) since they have no Real Power output.

MOD-025 Attachment 2

One-line Diagram, Table, and Summary for Verification Information Reporting

Note: If the configuration of the applicable Facility does not lend itself to the use of the diagram, tables, or summaries for reporting the required information, changes may be made to this form, provided that all required information (identified in MOD-025, Attachment 1) is reported.

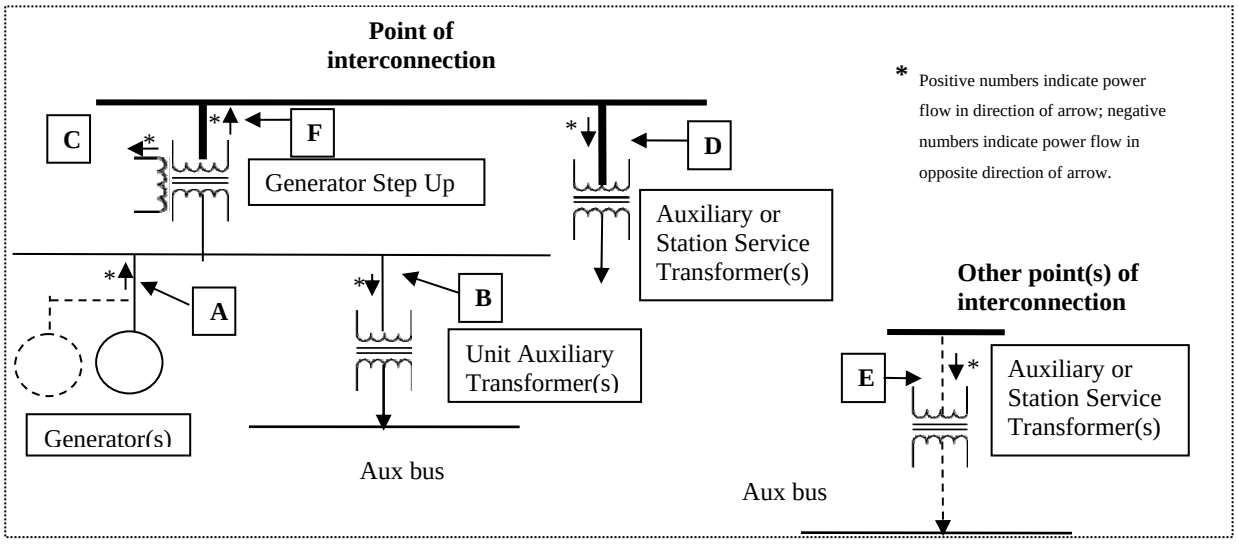
Company: **Reported By (name):**

Plant: **Unit No.:** **Date of Report:**

Check all that apply:

- ☐ Over-excited Full Load Reactive Power Verification
- ☐ Under-excited Full Load Reactive Power Verification
- ☐ Over-excited Minimum Load Reactive Power Verification
- ☐ Under-excited Minimum Load Reactive Power Verification
- ☐ Real Power Verification
- ☐ Staged Test Data
- ☐ Operational Data

Simplified one-line diagram showing plant auxiliary Load connections and verification data:



Point	Voltage	Real Power	Reactive Power	Comment
A	**kV**	**MW**	**Mvar**	Sum multiple generators that are verified together or are part of the same unit. Report individual unit values separately whenever the verification measurements were taken at the individual unit. Individual values are required for units or synchronous condensers > 20 MVA.
Identify calculated values, if any:				
B	**kV**	**MW**	**Mvar**	Sum multiple unit auxiliary transformers.
Identify calculated values, if any:				
C	**kV**	**MW**	**Mvar**	Sum multiple tertiary Loads, if any.
Identify calculated values, if any:				
D	**kV**	**MW**	**Mvar**	Sum multiple auxiliary and station service transformers.
Identify calculated values, if any:				
E	**kV**	**MW**	**Mvar**	If multiple points of Interconnection, describe these for accurate modeling; report points individually (sum multiple auxiliary transformers).
F	**kV**	**MW**	**Mvar**	Net unit capability
Identify calculated values, if any:				

MOD-025 -Attachment 2 (continued)

Verification Data

Provide data by unit or Facility, as appropriate

Data Type	Data Recorded	Last Verification (Previous Data; will be blank for the initial verification)
Gross Reactive Power Capability (*Mvar)		
Aux Reactive Power (*Mvar)		
Net Reactive Power Capability (*Mvar) equals Gross Reactive Power Capability (*Mvar) minus Aux Reactive Power connected at the same bus (*Mvar) minus tertiary Reactive Power connected at the same bus(*Mvar)		
Gross Real Power Capability (*MW)		
Aux Real Power (*MW)		
Net Real Power Capability (*MW) equals Gross Real Power Capability (*MW) minus Aux Real Power connected at the same bus (*MW) minus tertiary Real Power connected at the same bus(*MW)		
* Note: Enter values at the end of the verification period.		
GSU losses (only required if verification measurements are taken on the high side of the GSU - Mvar)		

Summary of Verification

- Date of Verification _____,Verification Start Time _____, Verification End Time _____
- Scheduled Voltage _____
- Transformer Voltage Ratio: GSU _____, Unit Aux _____, Station Aux _____, Other Aux _____
- Transformer Tap Setting: GSU _____, Unit Aux _____, Station Aux _____, Other Aux _____
- Ambient conditions at the end of the verification period:

  Air temperature: _____

  Humidity: _____

  Cooling water temperature: _____

  Other data as applicable: _____

- Generator hydrogen pressure at time of test (if applicable) _____

Date that data shown in last verification column in table above was taken _____

Remarks :

Note: If the verification value did not reach the thermal capability curve (D-curve), describe the reason.

Appendix QC-MOD-025-2
Provisions specific to the standard MOD-025-2 applicable in Québec

This appendix establishes specific provisions for the application of the standard in Québec. Provisions of the standard and of its appendix must be read together for the purposes of understanding and interpretation. Where the standard and appendix differ, the appendix shall prevail.

A. Introduction

1. Title: **Verification and Data Reporting of Generator Real and Reactive Power Capability and Synchronous Condenser Reactive Power Capability**

2. Number: MOD-025-2

3. Purpose: No specific provision

4. Applicability:

4.1. Functional entities

No specific provision

4.2. Facilities

For the purpose of this standard, the term, "applicable Facility" shall mean any one of the following:

4.2.1 Generating unit that is part of the Main Transmission System (RTP).

4.2.2 Synchronous condenser that is part of the Main Transmission System (RTP).

4.2.3 Generating plant/Facility that is part of the Main Transmission System (RTP).

5. Effective Date:

5.1. Adoption of the standard by the Régie de l'énergie: September 27, 2017

5.2. Adoption of the appendix by the Régie de l'énergie: September 27, 2017

5.3. Effective date of the standard and its appendix in Québec: October 1st, 2017

Enforcement dates for generating stations connected to the RTP

Applicable Facility (all requirements) (%)	**Date of enforcement in Québec**
At least 40% of applicable facilities	January 1st, 2018
At least 60% of applicable facilities	October 1st, 2018
At least 80% of applicable facilities	October 1st, 2019
100% of applicable facilities	October 1st, 2020

Applicable enforcement dates for generating stations not connected to the RTP

Applicable Facility (all requirements) (%)	Date of enforcement in Québec
At least 15% of applicable facilities	January 1st, 2018
At least 50% of applicable facilities	October 1st, 2018
At least 75% of applicable facilities	October 1st, 2019
100% of applicable facilities	October 1st, 2020

B. Requirements

No specific provision

C. Measures

No specific provision

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

The Régie de l'énergie is responsible, in Québec, for compliance monitoring with respect to the reliability standard and its appendix that it adopts.

1.2. Evidence Retention

No specific provision

1.3. Compliance Monitoring and Assessment Processes

No specific provision

1.4. Additional Compliance Information

No specific provision

2. Violation Severity Levels

No specific provision

E. Regional Variances

No specific provision

F. Associated Documents

No specific provision

MOD-025-2 – Attachment 1

No specific provision

Appendix QC-MOD-025-2
Provisions specific to the standard MOD-025-2 applicable in Québec

MOD-025-2 – Attachment 2

No specific provision

Revision History

Version	Date	Action	Change Tracking
0	September 27, 2017	New appendix	New

A. Introduction

1. Title: Verification of Models and Data for Generator Excitation Control System or Plant Volt/Var Control Functions

2. Number: MOD-026-1

3. Purpose: To verify that the generator excitation control system or plant volt/var control function[1] model (including the power system stabilizer model and the impedance compensator model) and the model parameters used in dynamic simulations accurately represent the generator excitation control system or plant volt/var control function behavior when assessing Bulk Electric System (BES) reliability.

4. Applicability:

4.1. Functional Entities:

4.1.1 Generator Owner

4.1.2 Transmission Planner

4.2. Facilities:

For the purpose of the requirements contained herein, Facilities that are directly connected to the Bulk Electric System (BES) will be collectively referred as an "applicable unit" that meet the following:

4.2.1 Generation in the Eastern or Quebec Interconnections with the following characteristics:

4.2.1.1 Individual generating unit greater than 100 MVA (gross nameplate rating).

4.2.1.2 Individual generating plant consisting of multiple generating units that are directly connected at a common BES bus with total generation greater than 100 MVA (gross aggregate nameplate rating).

4.2.2 Generation in the Western Interconnection with the following characteristics:

4.2.2.1 Individual generating unit greater than 75 MVA (gross nameplate rating).

4.2.2.2 Individual generating plant consisting of multiple generating units that are directly connected at a common BES bus with total generation greater than 75 MVA (gross aggregate nameplate rating).

[1] Excitation control system or plant volt/var control function:

a. For individual synchronous machines, the generator excitation control system includes the generator, exciter, voltage regulator, impedance compensation and power system stabilizer.

b. For an aggregate generating plant, the volt/var control system includes the voltage regulator & reactive power control system controlling and coordinating plant voltage and associated reactive capable resources.

4.2.3 Generation in the ERCOT Interconnection with the following characteristics:

4.2.3.1 Individual generating unit greater than 50 MVA (gross nameplate rating).

4.2.3.2 Individual generating plant consisting of multiple generating units that are directly connected at a common BES bus with total generation greater than 75 MVA (gross aggregate nameplate rating).

4.2.4 For all Interconnections:

- A technically justified[2] unit that meets NERC registry criteria but is not otherwise included in the above Applicability sections 4.2.1, 4.2.2, or 4.2.3 and is requested by the Transmission Planner.

5. Effective Date:

5.1. For Requirements R1, and R3 through R6, the first day of the first calendar quarter beyond the date that this standard is approved by applicable regulatory authorities or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities. In those jurisdictions where regulatory approval is not required, the standard shall become effective on the first day of the first calendar quarter beyond the date this standard is approved by the NERC Board of Trustees, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

5.2. For Requirement R2, 30 percent of the entity's applicable unit gross MVA for each Interconnection on the first day of the first calendar quarter that is four years following applicable regulatory approval or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities, or in those jurisdictions where no regulatory approval is required, on the first day of the first calendar quarter that is four years following NERC Board of Trustees adoption or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

5.3. For Requirement R2, 50 percent of the entity's applicable unit gross MVA for each Interconnection on first day of the first calendar quarter that is six years following applicable regulatory approval or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities, or in those jurisdictions where no regulatory approval is required, on the first day of the first calendar quarter that is six years following NERC Board of Trustees adoption or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

5.4. For Requirement R2, 100 percent of the entity's applicable unit gross MVA for each Interconnection on the first day of the first calendar quarter that is 10 years

[2] Technical justification is achieved by the Transmission Planner demonstrating that the simulated unit or plant response does not match the measured unit or plant response.

following applicable regulatory approval or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities, or in those jurisdictions where no regulatory approval is required, on the first day of the first calendar quarter that is 10 years following NERC Board of Trustees adoption or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

B. Requirements

R1. Each Transmission Planner shall provide the following requested information to the Generator Owner within 90 calendar days of receiving a written request : *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

- Instructions on how to obtain the list of excitation control system or plant volt/var control function models that are acceptable to the Transmission Planner for use in dynamic simulation,
- Instructions on how to obtain the dynamic excitation control system or plant volt/var control function model library block diagrams and/or data sheets for models that are acceptable to the Transmission Planner, or
- Model data for any of the Generator Owner's existing applicable unit specific excitation control system or plant volt/var control function contained in the Transmission Planner's dynamic database from the current (in-use) models, including generator MVA base.

R2. Each Generator Owner shall provide for each applicable unit, a verified generator excitation control system or plant volt/var control function model, including documentation and data (as specified in Part 2.1) to its Transmission Planner in accordance with the periodicity specified in MOD-026 Attachment 1. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

2.1. Each applicable unit's model shall be verified by the Generator Owner using one or more models acceptable to the Transmission Planner. Verification for individual units less than 20 MVA (gross nameplate rating) in a generating plant (per Section 4.2.1.2, 4.2.2.2, or 4.2.3.2) may be performed using either individual unit or aggregate unit model(s), or both. Each verification shall include the following:

2.1.1. Documentation demonstrating the applicable unit's model response matches the recorded response for a voltage excursion from either a staged test or a measured system disturbance,

2.1.2. Manufacturer, model number (if available), and type of the excitation control system including, but not limited to static, AC brushless, DC rotating, and/or the plant volt/var control function (if installed),

2.1.3. Model structure and data including, but not limited to reactance, time constants, saturation factors, total rotational inertia, or equivalent data for the generator,

2.1.4. Model structure and data for the excitation control system, including the closed loop voltage regulator if a closed loop voltage regulator is installed or the model structure and data for the plant volt/var control function system,

2.1.5. Compensation settings (such as droop, line drop, differential compensation), if used, and

2.1.6. Model structure and data for power system stabilizer, if so equipped.

R3. Each Generator Owner shall provide a written response to its Transmission Planner within 90 calendar days of receiving one of the following items for an applicable unit:

- Written notification from its Transmission Planner (in accordance with Requirement R6) that the excitation control system or plant volt/var control function model is not usable,
- Written comments from its Transmission Planner identifying technical concerns with the verification documentation related to the excitation control system or plant volt/var control function model, or
- Written comments and supporting evidence from its Transmission Planner indicating that the simulated excitation control system or plant volt/var control function model response did not match the recorded response to a transmission system event.

The written response shall contain either the technical basis for maintaining the current model, the model changes, or a plan to perform model verification[3] (in accordance with Requirement R2). *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

R4. Each Generator Owner shall provide revised model data or plans to perform model verification[4] (in accordance with Requirement R2) for an applicable unit to its Transmission Planner within 180 calendar days of making changes to the excitation control system or plant volt/var control function that alter the equipment response characteristic.[5] *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

[3] If verification is performed, the 10-year period as outlined in MOD-026 Attachment 1 is reset.

[4] Ibid

[5] Exciter, voltage regulator, plant volt/var or power system stabilizer control replacement including software alterations that alter excitation control system equipment response, plant digital control system addition or replacement, plant digital control system software alterations that alter excitation control system equipment response, plant volt/var function equipment addition or replacement (such as static var systems, capacitor banks, individual unit excitation systems, etc), a change in the voltage control mode (such as going from power factor control to automatic voltage control, etc), exciter, voltage regulator, impedance compensator, or power system stabilizer settings change. Automatic changes in settings that occur due to changes in operating mode do not apply to Requirement R4.

R5. Each Generator Owner shall provide a written response to its Transmission Planner, within 90 calendar days following receipt of a technically justified[6] unit request from the Transmission Planner to perform a model review of a unit or plant that includes one of the following: *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

- Details of plans to verify the model (in accordance with Requirement R2), or
- Corrected model data including the source of revised model data such as discovery of manufacturer test values to replace generic model data or updating of data parameters based on an on-site review of the equipment.

R6. Each Transmission Planner shall provide a written response to the Generator Owner within 90 calendar days of receiving the verified excitation control system or plant volt/var control function model information in accordance with Requirement R2 that the model is usable (meets the criteria specified in Parts 6.1 through 6.3) or is not usable.

6.1. The excitation control system or plant volt/var control function model initializes to compute modeling data without error,

6.2. A no-disturbance simulation results in negligible transients, and

6.3. For an otherwise stable simulation, a disturbance simulation results in the excitation control and plant volt/var control function model exhibiting positive damping.

If the model is not usable, the Transmission Planner shall provide a technical description of why the model is not usable. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

C. Measures

M1. The Transmission Planner must have and provide the dated request for instructions or data, the transmitted instructions or data, and dated evidence of a written transmittal (e.g., electronic mail message, postal receipt, or confirmation of facsimile) as evidence that it provided the request within 90 calendar days in accordance with Requirement R1.

M2. The Generator Owner must have and provide dated evidence it verified each generator excitation control system or plant volt/var control function model according to Part 2.1 for each applicable unit and a dated transmittal (e.g., electronic mail message, postal receipt, or confirmation of facsimile) as evidence it provided the model, documentation, and data to its Transmission Planner, in accordance with Requirement R2.

M3. Evidence for Requirement R3 must include the Generator Owner's dated written response containing the information identified in Requirement R3 and dated evidence

[6] Technical justification is achieved by the Transmission Planner demonstrating that the simulated unit or plant response does not match the measured unit or plant response.

of transmittal (e.g., electronic mail message, postal receipt, or confirmation of facsimile) of the response.

M4. Evidence for Requirement R4 must include, for each of the Generator Owner's applicable units for which system changes specified in Requirement R4 were made, a dated revised model data or plans to perform a model verification and dated evidence (e.g., electronic mail message, postal receipt, or confirmation of facsimile) it provided the revised model and data or plans within 180 calendar days of making changes.

M5. Evidence for Requirement R5 must include the Generator Owner's dated written response containing the information identified in Requirement R5 and dated evidence (e.g., electronic mail message, postal receipt, or confirmation of facsimile) it provided a written response within 90 calendar days following receipt of a technically justified request.

M6. Evidence of Requirement R6 must include, for each model received, the dated response indicating the model was usable or not usable according to the criteria specified in Parts 6.1 through 6.3 and for a model that is not usable, a technical description; and dated evidence of transmittal (e.g., electronic mail message, postal receipt, or confirmation of facsimile) that the Generator Owner was notified within 90 calendar days of receipt of model information.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

The Regional Entity shall serve as the Compliance Enforcement Authority unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Data Retention

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Generator Owner and Transmission Planner shall each keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation:

- The Transmission Planner shall retain the information/data request and provided response evidence of Requirements R1 and R6, Measures M1 and M6 for three calendar years from the date the document was provided.

- The Generator Owner shall retain the latest excitation control system or plant volt/var control function model verification evidence of Requirement R2, Measure M2.
- The Generator Owner shall retain the information/data request and provided response evidence of Requirements R3 through R5, and Measures M3 through M5 for three calendar years from the date the document was provided.

If a Generator Owner or Transmission Planner is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete or approved or for the time specified above, whichever is longer.

The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes

Compliance Audit

Self-Certification

Spot Checking

Compliance Investigation

Self-Reporting

Complaints

1.4. Additional Compliance Information

None

2. Violation Severity Levels

R #	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	The Transmission Planner provided the instructions and data to the Generator Owner more than 90 calendar days but less than or equal to 120 calendar days of receiving a written request.	The Transmission Planner provided the instructions and data to the Generator Owner more than 120 calendar days but less than or equal to 150 calendar days of receiving a written request.	The Transmission Planner provided the instructions and data to the Generator Owner more than 150 calendar days but less than or equal to 180 calendar days of receiving a written request.	The Transmission Planner failed to provide the instructions and data to the Generator Owner within 180 calendar days of receiving a written request.
R2	The Generator Owner provided its verified model(s), including documentation and data to its Transmission Planner after the timeframe specified in MOD-026 Attachment 1 but less than or equal to 90 calendar days late; OR The Generator Owner provided the Transmission Planner verified models that omitted one of the six Parts identified in Requirement R2, Parts 2.1.1 through 2.1.6.	The Generator Owner provided its verified model(s), including documentation and data to its Transmission Planner more than 90 calendar days but less than or equal to 180 calendar days late as specified by the periodicity timeframe in MOD-026 Attachment 1. OR The Generator Owner provided the Transmission Planner verified models that omitted two of the six Parts identified in Requirement R2, Parts 2.1.1 through 2.1.6.	The Generator Owner provided its verified model(s), including documentation and data to its Transmission Planner more than 180 calendar days but less than or equal to 270 calendar days late as specified by the periodicity timeframe in MOD-026 Attachment 1. OR The Generator Owner provided the Transmission Planner verified models that omitted three of the six Parts identified in Requirement R2, Parts 2.1.1 through 2.1.6.	The Generator Owner provided its verified model(s), including documentation and data more than 270 calendar days late to its Transmission Planner in accordance with the periodicity specified in MOD-026 Attachment 1. OR The Generator Owner failed to use model(s) acceptable to the Transmission Planner as specified in Requirement R2, Part 2.1. OR The Generator Owner provided the Transmission Planner verified model(s) but omitted four or more of the six parts identified in Requirement R2, Subparts 2.1.1 through 2.1.6.

R #	Lower VSL	Moderate VSL	High VSL	Severe VSL
R3	The Generator Owner provided a written response more than 90 calendar days but less than or equal to 120 calendar days of receiving written notice.	The Generator Owner provided a written response more than 120 calendar days but less than or equal to 150 calendar days of receiving written notice.	The Generator Owner provided a written response more than 150 calendar days but less than or equal to 180 calendar days of receiving written notice.	The Generator Owner failed to provide a written response within 180 calendar days of receiving written notice. OR The Generator Owner's written response failed to contain either the technical basis for maintaining the current model, or a list of future model changes, or a plan to perform another model verification.
R4	The Generator Owner provided revised model data or plans to perform model verification more than 180 calendar days but less than or equal to 210 calendar days of making changes to the excitation control system or plant volt/var control function that altered the equipment response characteristic.	The Generator Owner provided revised model data or plans to perform model verification more than 210 calendar days but less than or equal to 240 calendar days of making changes to the excitation control system or plant volt/var control function that altered the equipment response characteristic.	The Generator Owner provided revised model data or plans to perform model verification more than 240 calendar days but less than or equal to 270 calendar days of making changes to the excitation control system or plant volt/var control function that altered the equipment response characteristic.	The Generator Owner failed to provide revised model data or failed to provide plans to perform model verification within 270 calendar days of making changes to the excitation control system or plant volt/var control function that altered the equipment response characteristic.
R5	The Generator Owner provided a written response more than 90 calendar days but less than or equal to 120 calendar days to the Transmission Planner following receipt of a technically justified request to perform a model review of an applicable unit.	The Generator Owner provided a written response more than 120 calendar days but less than or equal to 150 calendar days to the Transmission Planner following receipt of a technically justified request to perform a model review of an applicable unit.	The Generator Owner provided a written response more than 150 calendar days but less than or equal to 180 calendar days to the Transmission Planner following receipt of a technically justified request to perform a model review of an applicable unit.	The Generator Owner failed to provide a written response to the Transmission Planner within 180 calendar days following receipt of a technically justified request to perform a model review of an applicable unit. OR The Generator Owner’s written response failed to include one of the sub bullets of Requirement R5.

R #	Lower VSL	Moderate VSL	High VSL	Severe VSL
R6	The Transmission Planner provided a written response to the Generator Owner indicating whether the model is usable or not usable; including a technical description if the model is not usable, more than 90 calendar days but less than or equal to 120 calendar days of receiving verified model information.	The Transmission Planner provided a written response to the Generator Owner indicating whether the model is usable or not usable; including a technical description if the model is not usable, more than 120 calendar days but less than or equal to 150 calendar days of receiving the verified model information. OR The Transmission Planner's written response omitted confirmation for one of the specified model criteria listed in Requirement R6, Parts 6.1 through 6.3.	The Transmission Planner provided a written response to the Generator Owner indicating whether the model is usable or not usable; including a technical description if the model is not usable, more than 150 calendar days but less than or equal to 180 calendar days of receiving the verified model information. OR The Transmission Planner's written response omitted confirmation for two of the specified model criteria listed in Requirement R6, Parts 6.1 through 6.3.	The Transmission Planner failed to provide a written response to the Generator Owner within 180 calendar days of receiving the verified model information. OR The Transmission Planner's written response omitted confirmation for all specified model criteria listed in Requirement R6, Parts 6.1 through 6.3.

E. Regional Variances

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	February 7, 2013	Adopted by NERC Board of Trustees	New
1	March 20, 2014	FERC Order issued approving MOD-026-1. (Order becomes effective for R1, R3, R4, R5, and R6 on 7/1/14. R2 becomes effective on 7/1/18.)	

G. References

The following documents contain technical information beyond the scope of this Standard on excitation control system functionality, modeling, and testing.

1. IEEE 421.1 Definitions for Excitation Systems for Synchronous Machines
2. IEEE 421.2 Guide for Identification, Testing, and Evaluation of the Dynamic Performance of Excitation Control Systems
3. IEEE 421.5 IEEE Recommended Practice for Excitation System Models for Power System Stability Studies
4. K. Clark, R.A. Walling, N.W. Miller, "Solar Photovoltaic (PV) Plant Models in PSLF," IEEE/PES General Meeting, Detroit, MI, July 2011
5. M. Asmine, J. Brochu, J. Fortmann, R. Gagnon, Y. Kazachkov, C.-E. Langlois, C. Larose, E. Muljadi, J. MacDowell, P. Pourbeik, S. A. Seman, and K. Wiens, "Model Validation for Wind Turbine Generator Models", IEEE Transactions on Power System, Volume 26, Issue 3, August 2011
6. A. Ellis, E. Muljadi, J. Sanchez-Gasca, Y. Kazachkov, "Generic Models for Simulation of Wind Power Plants in Bulk System Planning Studies," IEEE PES General Meeting 2011, Detroit, MI, July 24-28
7. N.W. Miller, J. J. Sanchez-Gasca, K. Clark, J.M. MacDowell, "Dynamic Modeling of GE Wind Plants for Stability Simulations," IEEE PES General Meeting 2011, Detroit, MI, July 24-28
8. A. Ellis, Y. Kazachkov, E. Muljadi, P. Pourbeik, J.J. Sanchez-Gasca, Working Group Joint Report – WECC Working Group on Dynamic Performance of Wind Power Generation & IEEE Working Group on Dynamic Performance of Wind Power Generation, "Description and Technical Specifications for Generic WTG Models – A Status Report," Proc. IEEE PES 2011 Power Systems Conference and Exposition (PSCE), March 2011, Phoenix, AZ
9. K. Clark, N.W. Miller, R.A. Walling, "Modeling of GE Solar Photovoltaic (PV) Plants for Grid Studies," version 1.1, April 2010
10. K. Clark, N.W. Miller, J. J. Sanchez-Gasca, "Modeling of GE Wind Turbine-Generators for Grid Studies," version 4.5, April 16, 2010, Available from GE Energy
11. R.J. Piwko, N.W. Miller, J.M. MacDowell, "Field Testing & Model Validation of Wind Plants," in Proc. IEEE PES General Meeting, Pittsburg, PA, July 2008
12. N. Miller, K. Clark, J. MacDowell and W. Barton, "Experience with Field and Factory Testing for Model Validation of GE Wind Plants," in Proc. Eur. Wind Energy Conf. Exhib., Brussels, Belgium, March/April 2008

13. IEEE Task Force on Generator Model Validation Testing of the Power System Stability Subcommittee, "Guidelines for Generator Stability Model Validation Testing," IEEE PES General Meeting 2007, paper 07GM1307

14. W.W. Price and J. J. Sanchez-Gasca, "Simplified Wind Turbine Generator Aerodynamic Models for Transient Stability Studies," in PROC IEEE PES 2006 Power Systems Conf. Expo. (PSCE), Atlanta, GA, October 1, 2006, p. 986-992

15. J.J. Sanchez-Gasca, R.J. Piwko, N. W. Miller, W. W. Price, "On the Integration of Wind Power Plants in Large Power Systems," Proc. X Symposium of Specialists in Electric and Expansion Planning (SEPOPE), Florianopolis, Brazil, May 2006

16. N. W. Miller, J. J. Sanchez-Gasca, W. W. Price, R. W. Delmerico, "Dynamic Modeling of GE 1.5 and 3.6 MW Wind Turbine-Generators for Stability Simulations," Proc. IEEE Power Engineering Society General Meeting, Toronto, Ontario, July 2003

17. P. Pourbeik, C. Pink and R. Bisbee, "Power Plant Model Validation for Achieving Reliability Standard Requirements Based on Recorded On-Line Disturbance Data", Proceedings of the IEEE PSCE, March, 2011

MOD-026 Attachment 1 Excitation Control System or Plant Volt/Var Function Model Verification Periodicity		
Row Number	**Verification Condition**	**Required Action**
1	Establishing the initial verification date for an applicable unit. (Requirement R2)	Transmit the verified model, documentation and data to the Transmission Planner on or before the Effective Date. Row 4 applies when calculating generation fleet compliance during the 10-year implementation period. See Section A5 for Effective Dates.
2	Subsequent verification for an applicable unit. (Requirement R2)	Transmit the verified model, documentation and data to the Transmission Planner on or before the 10-year anniversary of the last transmittal (per Note 1).
3	Initial verification for a new applicable unit or for an existing applicable unit with new excitation control system or plant volt/var control function equipment installed. (Requirement R2)	Transmit the verified model, documentation and data to the Transmission Planner within 365 calendar days after the commissioning date.

MOD-026 Attachment 1 Excitation Control System or Plant Volt/Var Function Model Verification Periodicity		
Row Number	**Verification Condition**	**Required Action**
4	Existing applicable unit that is equivalent to another unit(s) at the same physical location. AND Each applicable unit has the same MVA nameplate rating. AND The nameplate rating is ≤ 350 MVA. AND Each applicable unit has the same components and settings. AND The model for one of these equivalent applicable units has been verified. (Requirement R2)	Document circumstance with a written statement and include with the verified model, documentation and data provided to the Transmission Planner for the verified equivalent unit. Verify a different equivalent unit during each 10-year verification period. Applies to Row 1 when calculating generation fleet compliance during the 10-year implementation period.
5	The Generator Owner has submitted a verification plan. (Requirement R3, R4 or R5)	Transmit the verified model, documentation and data to the Transmission Planner within 365 calendar days after the submittal of the verification plan.

MOD-026 Attachment 1 Excitation Control System or Plant Volt/Var Function Model Verification Periodicity		
Row Number	**Verification Condition**	**Required Action**
6	New or existing applicable unit does not include an active closed loop voltage or reactive power control function. (Requirement R2)	Requirement 2 is met with a written statement to that effect transmitted to the Transmission Planner. Perform verification per the periodicity specified in Row 3 for a "New Generating Unit" (or new equipment) only if active closed loop function is established. See Footnote 1 (see Section A.3) for clarification of what constitutes an active closed loop function for both conventional synchronous machines (reference Footnote 1a) and aggregate generating plants (reference Footnote 1b).
7	Existing applicable unit has a current average net capacity factor over the most recent three calendar years, beginning on January 1 and ending on December 31 of 5% or less. (Requirement R2)	Requirement 2 is met with a written statement to that effect transmitted to the Transmission Planner. At the end of this 10-year timeframe, the current average three year net capacity factor (for years 8, 9, and 10) can be examined to determine if the capacity factor exemption can be declared for the next 10-year period. If not eligible for the capacity factor exemption, then model verification must be completed within 365 calendar days of the date the capacity factor exemption expired. For the definition of net capacity factor, refer to Appendix F of the GADS Data Reporting Instructions on the NERC website.

MOD-026 Attachment 1

Excitation Control System or Plant Volt/Var Function Model Verification Periodicity

Row Number	Verification Condition	Required Action

NOTES:

NOTE 1: Establishing the recurring 10-year unit verification period start date:

The start date is the actual date of submittal of a verified model to the Transmission Planner for the most recently performed unit verification.

NOTE 2: Consideration for early compliance:

Existing generator excitation control system or plant volt/var control function model verification is sufficient for demonstrating compliance for a 10-year period from the actual transmittal date if either of the following applies:

- The Generator Owner has a verified model that is compliant with the applicable regional policies, guidelines or criteria existing at the time of model verification.
- The Generator Owner has an existing verified model that is compliant with the requirements of this standard.

Appendix QC-MOD-026-1
Provisions specific to the standard MOD-026-1 applicable in Québec

This appendix establishes specific provisions for the application of the standard in Québec. Provisions of the standard and of its appendix must be read together for the purposes of understanding and interpretation. Where the standard and appendix differ, the appendix shall prevail.

A. Introduction

1. Title: **Verification of Models and Data for Generator Excitation Control System or Plant Volt/Var Control Functions**

2. Number: MOD-026-1

3. Purpose: No specific provision

4. Applicability:

4.1. Functional entities

No specific provision

4.2. Facilities

For the purpose of the requirements contained herein, Facilities that form part of the Main Transmission System (RTP) will be collectively referred as an "applicable unit" that meet the following:

4.2.1 No specific provision

4.2.1.1 No specific provision

4.2.1.2 Individual generating plant consisting of multiple generating units that is part of the Main Transmission System (RTP) with total generation greater than 100 MVA (gross aggregate nameplate rating).

4.2.2 No specific provision

4.2.3 No specific provision

4.2.4 A technically justified[1] Main Transmission System (RTP) Facility that is not otherwise included in the above Applicability sections 4.2.1, 4.2.2, or 4.2.3 and that is requested by the Transmission Planner.

5. Effective Date:

5.1. Adoption of the standard by the Régie de l'énergie: September 27, 2017

5.2. Adoption of the appendix by the Régie de l'énergie: September 28, 2020

5.3. Effective date of the standard and its appendix in Québec: September 28, 2020

[1] Technical justification is achieved by the Transmission Planner demonstrating that the simulated unit or plant response does not match the measured unit or plant response.

Appendix QC-MOD-026-1
Provisions specific to the standard MOD-026-1 applicable in Québec

Applicable enforcement dates for applicable facilities

Requirements	Applicability	Date of enforcement in Québec
R1 R3 to R6	100% of applicable facilities	January 1st, 2018
R2	30% of applicable facilities	January 1st, 2021
	50% of applicable facilities	October 1st, 2022
	100% of applicable facilities	October 1st, 2025

B. Requirements

No specific provision

C. Measures

No specific provision

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

The Régie de l'énergie is responsible, in Québec, for compliance monitoring with respect to the reliability standard and its appendix that it adopts.

1.2. Evidence Retention

No specific provision

1.3. Compliance Monitoring and Assessment Processes

No specific provision

1.4. Additional Compliance Information

No specific provision

2. Violation Severity Levels

No specific provision

E. Regional Variances

No specific provision

F. Associated Documents

No specific provision

G. References

No specific provision

MOD-026-1 – Attachment 1

No specific provision

Revision History

Version	Date	Action	Change Tracking
0	September 27, 2017	New appendix	New
1	September 28, 2020	Delay from October 1, 2020 to January 1, 2021 of the implementation date applicable to 30% of applicable facilities subject to requirement R2 as per decision D-2020-128	Revision

A. Introduction

1. Title: Verification of Models and Data for Turbine/Governor and Load Control or Active Power/Frequency Control Functions

2. Number: MOD-027-1

3. Purpose: To verify that the turbine/governor and load control or active power/frequency control[1] model and the model parameters, used in dynamic simulations that assess Bulk Electric System (BES) reliability, accurately represent generator unit real power response to system frequency variations.

4. Applicability:

4.1. Functional entities

4.1.1 Generator Owner

4.1.2 Transmission Planner

4.2. Facilities

For the purpose of the requirements contained herein, Facilities that are directly connected to the Bulk Electric System (BES) will be collectively referred to as an "applicable unit" that meet the following:

4.2.1 Generation in the Eastern or Quebec Interconnections with the following characteristics:

4.2.1.1 Individual generating unit greater than 100 MVA (gross nameplate rating).

4.2.1.2 Individual generating plant consisting of multiple generating units that are directly connected at a common BES bus with total generation greater than 100 MVA (gross aggregate nameplate rating).

4.2.2 Generation in the Western Interconnection with the following characteristics:

4.2.2.1 Individual generating unit greater than 75 MVA (gross nameplate rating).

4.2.2.2 Individual generating plant consisting of multiple generating units that are directly connected at a common BES bus with total generation greater than 75 MVA (gross aggregate nameplate rating).

4.2.3 Generation in the ERCOT Interconnection with the following characteristics:

[1] Turbine/governor and load control or active power/frequency control:

a. Turbine/governor and load control applies to conventional synchronous generation.

b. Active power/frequency control applies to inverter connected generators (often found at variable energy plants).

4.2.3.1 Individual generating unit greater than 50 MVA (gross nameplate rating).

4.2.3.2 Individual generating plant consisting of multiple generating units that are directly connected at a common BES bus with total generation greater than 75 MVA (gross aggregate nameplate rating).

5. Effective Date:

5.1. For Requirements R1, and R3 through R5, the first day of the first calendar quarter beyond the date that this standard is approved by applicable regulatory authorities or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities. In those jurisdictions where regulatory approval is not required, the standard shall become effective on the first day of the first calendar quarter beyond the date this standard is approved by the NERC Board of Trustees, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

5.2. For Requirement R2, 30 percent of the entity's applicable unit gross MVA for each Interconnection on the first day of the first calendar quarter that is four years following applicable regulatory approval or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities, or in those jurisdictions where no regulatory approval is required, on the first day of the first calendar quarter that is four years following NERC Board of Trustees adoption or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

5.3. For Requirement R2, 50 percent of the entity's applicable unit gross MVA for each Interconnection on first day of the first calendar quarter that is six years following applicable regulatory approval or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities, or in those jurisdictions where no regulatory approval is required, on the first day of the first calendar quarter that is six years following NERC Board of Trustees adoption or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

5.4. For Requirement R2, 100 percent of the entity's applicable unit gross MVA for each Interconnection on the first day of the first calendar quarter that is 10 years following applicable regulatory approval or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities, or in those jurisdictions where no regulatory approval is required, on the first day of the first calendar quarter that is 10 years following NERC Board of Trustees adoption or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

B. Requirements

R1. Each Transmission Planner shall provide the following requested information to the Generator Owner within 90 calendar days of receiving a written request: *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

- Instructions on how to obtain the list of turbine/governor and load control or active power/frequency control system models that are acceptable to the Transmission Planner for use in dynamic simulation,
- Instructions on how to obtain the dynamic turbine/governor and load control or active power/frequency control function model library block diagrams and/or data sheets for models that are acceptable to the Transmission Planner, or
- Model data for any of the Generator Owner's existing applicable unit specific turbine/governor and load control or active power/frequency control system contained in the Transmission Planner's dynamic database from the current (in-use) models.

R2. Each Generator Owner shall provide, for each applicable unit, a verified turbine/governor and load control or active power/frequency control model, including documentation and data (as specified in Part 2.1) to its Transmission Planner in accordance with the periodicity specified in MOD-027 Attachment 1. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

2.1. Each applicable unit's model shall be verified by the Generator Owner using one or more models acceptable to the Transmission Planner. Verification for individual units rated less than 20 MVA (gross nameplate rating) in a generating plant (per Section 4.2.1.2, 4.2.2.2, or 4.2.3.2) may be performed using either individual unit or aggregate unit model(s) or both. Each verification shall include the following:

2.1.1. Documentation comparing the applicable unit's MW model response to the recorded MW response for either:

- A frequency excursion from a system disturbance that meets MOD-027 Attachment 1 Note 1 with the applicable unit on-line,
- A speed governor reference change with the applicable unit on-line, or
- A partial load rejection test,[2]

2.1.2. Type of governor and load control or active power control/frequency control[3] equipment,

[2] Differences between the control mode tested and the final simulation model must be identified, particularly when analyzing load rejection data. Most controls change gains or have a set point runback which takes effect when the breaker opens. Load or set point controls will also not be in effect once the breaker opens. Some method of accounting for these differences must be presented if the final model is not validated from on-line data under the normal operating conditions under which the model is expected to apply.

[3] Turbine/governor and load control or active power/frequency control:

2.1.3. A description of the turbine (e.g. for hydro turbine - Kaplan, Francis, or Pelton; for steam turbine - boiler type, normal fuel type, and turbine type; for gas turbine - the type and manufacturer; for variable energy plant - type and manufacturer),

2.1.4. Model structure and data for turbine/governor and load control or active power/frequency control, and

2.1.5. Representation of the real power response effects of outer loop controls (such as operator set point controls, and load control but excluding AGC control) that would override the governor response (including blocked or nonfunctioning governors or modes of operation that limit Frequency Response), if applicable.

R3. Each Generator Owner shall provide a written response to its Transmission Planner within 90 calendar days of receiving one of the following items for an applicable unit.

- Written notification, from its Transmission Planner (in accordance with Requirement R5) that the turbine/governor and load control or active power/frequency control model is not "usable,"
- Written comments from its Transmission Planner identifying technical concerns with the verification documentation related to the turbine/governor and load control or active power/frequency control model, or
- Written comments and supporting evidence from its Transmission Planner indicating that the simulated turbine/governor and load control or active power/frequency control response did not approximate the recorded response for three or more transmission system events.

The written response shall contain either the technical basis for maintaining the current model, the model changes, or a plan to perform model verification[4] (in accordance with Requirement R2). *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

R4. Each Generator Owner shall provide revised model data or plans to perform model verification[5] (in accordance with Requirement R2) for an applicable unit to its Transmission Planner within 180 calendar days of making changes to the turbine/governor and load control or active power/frequency control system that alter the equipment response characteristic[6]. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

---

a. Turbine/governor and load control applies to conventional synchronous generation.

b. Active power/frequency control applies to inverter connected generators (often found at variable energy plants).

[4] If verification is performed, the 10 year period as outlined in MOD-027 Attachment 1 is reset.

[5] Ibid.

[6] Control replacement or alteration including software alterations or plant digital control system addition or replacement, plant digital control system software alterations that alter droop, and/or dead band, and/or frequency response and/or a change in the frequency control mode (such as going from droop control to constant MW control, etc).

R5. Each Transmission Planner shall provide a written response to the Generator Owner within 90 calendar days of receiving the turbine/governor and load control or active power/frequency control system verified model information in accordance with Requirement R2 that the model is usable (meets the criteria specified in Parts 5.1 through 5.3) or is not usable.

5.1. The turbine/governor and load control or active power/frequency control function model initializes to compute modeling data without error,

5.2. A no-disturbance simulation results in negligible transients, and

5.3. For an otherwise stable simulation, a disturbance simulation results in the turbine/governor and load control or active power/frequency control model exhibiting positive damping.

If the model is not usable, the Transmission Planner shall provide a technical description of why the model is not usable. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

C. Measures

M1. The Transmission Planner must have and provide the dated request for instructions or data, the transmitted instruction or data, and dated evidence of a written transmittal (e.g., electronic mail message, postal receipt, or confirmation of facsimile) as evidence that it provided the request within 90 calendar days in accordance with Requirement R1.

M2. The Generator Owner must have and provide dated evidence it verified each generator turbine/governor and load control or active power/frequency control model according to Part 2.1 for each applicable unit and a dated transmittal (e.g., electronic mail message, postal receipt, or confirmation of facsimile) as evidence it provided the model, documentation, and data to its Transmission Planner, in accordance with Requirement R2.

M3. Evidence for Requirement R3 must include the Generator Owner's dated written response containing the information identified in Requirement R3 and dated evidence of transmittal (e.g., electronic mail message, postal receipt, or confirmation of facsimile) of the response.

M4. Evidence for Requirement R4 must include, for each of the Generator Owner's applicable units for which system changes specified in Requirement R4 were made, dated revised model data or dated plans to perform a model verification and dated evidence of transmittal (e.g., electronic mail message, postal receipt, or confirmation of facsimile) within 180 calendar days of making changes.

M5. Evidence of Requirement R5 must include, for each model received, the dated response indicating the model was usable or not usable according to the criteria specified in Parts 5.1 through 5.3 and for a model that is not useable, a technical description is the model is not usable, and dated evidence of transmittal (e.g., electronic mail messages, postal receipts, or confirmation of facsimile) that the Generator Owner was notified within 90 calendar days of receipt of model information in accordance with Requirement R5.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

The Regional Entity shall serve as the Compliance Enforcement Authority unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Data Retention

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Generator Owner and Transmission Planner shall each keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation:

- The Transmission Planner shall retain the information/data request and provided response evidence of Requirements R1 and R5, Measures M1 and M5 for 3 calendar years from the date the document was provided.
- The Generator Owner shall retain the latest turbine/governor and load control or active power/frequency control system model verification evidence of Requirement R2, Measure M2.
- The Generator Owner shall retain the information/data request and provided response evidence of Requirements R3, and R4 Measures M3 and M4 for 3 calendar years from the date the document was provided.

If a Generator Owner or Transmission Planner is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.

The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes

Compliance Audit

Self-Certification

Spot Checking

Compliance Investigation

Self-Reporting

Complaint

1.4. Additional Compliance Information

None

2. Violation Severity Levels

R #	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	The Transmission Planner provided the instructions and data to the Generator Owner more than 90 calendar days but less than or equal to 120 calendar days of receiving a written request.	The Transmission Planner provided the instructions and data to the Generator Owner more than 120 calendar days but less than or equal to 150 calendar days of receiving a written request.	The Transmission Planner provided the instructions and data to the Generator Owner more than 150 calendar days but less than or equal to 180 calendar days of receiving a written request.	The Transmission Planner failed to provide the instructions and data to the Generator Owner within 180 calendar days of receiving a written request.
R2	The Generator Owner provided its verified model(s) to its Transmission Planner after the periodicity timeframe specified in MOD-027 Attachment 1 but less than or equal to 90 calendar days late; OR The Generator Owner provided the Transmission Planner a verified model that omitted one of the five Parts identified in Requirement R2, Subparts 2.1.1, through 2.1.5.	The Generator Owner provided its verified model(s) to its Transmission Planner more than 90 calendar days but less than or equal to 180 calendar days late as specified by the periodicity timeframe in MOD-027 Attachment 1; OR The Generator Owner provided the Transmission Planner a verified model that omitted two of the five Parts identified in Requirement R2, Subparts 2.1.1, through 2.1.5.	The Generator Owner provided its verified model(s) to its Transmission Planner more than 180 calendar days but less than or equal to 270 calendar days late as specified by the periodicity timeframe in MOD-027 Attachment 1; OR The Generator Owner provided the Transmission Planner verified models that omitted three of the five Parts identified in Requirement R2, Subparts 2.1.1, through 2.1.5.	The Generator Owner provided its verified model(s) more than 270 calendar days late to its Transmission Planner in accordance with the periodicity specified in MOD-027 Attachment 1; OR The Generator Owner failed to use model(s) acceptable to the Transmission Planner as specified in Requirement R2, Part 2.1; OR The Generator Owner provided the Transmission Planner verified model(s) that omitted four or more of the five Parts identified in Requirement R2, Subparts 2.1.1, through 2.1.5.

R #	Lower VSL	Moderate VSL	High VSL	Severe VSL
R3	The Generator Owner provided a written response more than 90 calendar days but less than or equal to 120 calendar days of receiving written notice.	The Generator Owner provided a written response more than 120 calendar days but less than or equal to 150 calendar days of receiving written notice.	The Generator Owner provided a written response more than 150 calendar days but less than or equal to 180 calendar days of receiving written notice.	The Generator Owner failed to provide a written response within 180 calendar days of receiving written notice; OR The Generator Owner's written response failed to contain either the technical basis for maintaining the current model, or a list of future model changes, or a plan to perform another model verification.
R4	The Generator Owner provided revised model data or plans to perform model verification more than 180 calendar days but less than or equal to 210 calendar days of making changes to the turbine/governor and load control or active power/frequency control system that alter the equipment response characteristic.	The Generator Owner provided revised model data or plans to perform model verification more than 210 calendar days but less than or equal to 240 calendar days of making changes to the turbine/governor and load control or active power/frequency control system that alter the equipment response characteristic.	The Generator Owner provided revised model data or plans to perform model verification more than 240 calendar days but less than or equal to 270 calendar days of making changes to the turbine/governor and load control or active power/frequency control system that alter the equipment response characteristic.	The Generator Owner failed to provide revised model data or failed to provide plans to perform model verification within 270 calendar days of making changes to the turbine/governor and load control or active power/frequency control system that altered the equipment response characteristic.

R #	Lower VSL	Moderate VSL	High VSL	Severe VSL
R5	The Transmission Planner provided a written response to the Generator Owner indicating whether the model is usable or not usable, including a technical description if the model is not usable, more than 90 calendar days but less than or equal to 120 calendar days of receiving verified model information;	The Transmission Planner provided a written response to the Generator Owner indicating whether the model is usable or not usable, including a technical description if the model is not usable, more than 120 calendar days but less than or equal to 150 calendar days of receiving the verified model information; OR The Transmission Planner's written response omitted confirmation for one of the specified model criteria listed in Requirement R5, Parts 5.1 through 5.3.	The Transmission Planner provided a written response to the Generator Owner indicating whether the model is usable or not usable, including a technical description if the model is not usable, more than 150 calendar days but less than or equal to 180 calendar days of receiving the verified model information; OR The Transmission Planner's written response omitted confirmation for two of the specified model criteria listed in Requirement R5, Parts 5.1 through 5.3.	The Transmission Planner failed to provide a written response to the Generator Owner within 180 calendar days of receiving the verified model information; OR The Transmission Planner provided a written response without including confirmation of all specified model criteria listed in Requirement R5, Parts 5.1 through 5.3.

E. Regional Variances

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	February 7, 2013	Adopted by NERC Board of Trustees	New
1	March 20, 2014	FERC Order issued approving MOD-027-1. (Order becomes effective for R1, R3, R4, and R5 on 7/1/14. R2 becomes effective 7/1/18.)	

G. References

The following documents contain technical information beyond the scope of this Standard on turbine/governor and load control or active power/frequency control system functionality, modeling, and testing.

1) IEEE Task Force on Generator Model Validation Testing of the Power System Stability Subcommittee, "Guidelines for Generator Stability Model Validation Testing," IEEE PES General Meeting 2007, paper 07GM1307

2) L. Pereira "New Thermal Governor Model Development: Its Impact on Operation and Planning Studies on the Western Interconnection" IEEE POWER AND ENERGY MAGAZINE, MAY/JUNE 2005

3) D.M. Cabbell, S. Rueckert, B.A. Tuck, and M.C. Willis, "The New Thermal Governor Model Used in Operating and Planning Studies in WECC," in Proc. IEEE PES General Meeting, Denver, CO, 2004

4) S. Patterson, "Importance of Hydro Generation Response Resulting from the New Thermal Modeling-and Required Hydro Modeling Improvements," in Proc. IEEE PES General Meeting, Denver, CO, 2004

5) L. Pereira, D. Kosterev, D. Davies, and S. Patterson, "New Thermal Governor Model Selection and Validation in the WECC," IEEE Trans. Power Syst., vol. 19, no. 1, pp. 517-523, February 2004

6) L. Pereira, J. Undrill, D. Kosterev, D. Davies, and S. Patterson, "A New Thermal Governor Modeling Approach in the WECC," IEEE Trans. Power Syst., vol. 18, no. 2, pp. 819-829, May 2003

7) P. Pourbeik, C. Pink and R. Bisbee, "Power Plant Model Validation for Achieving Reliability Standard Requirements Based on Recorded On-Line Disturbance Data", Proceedings of the IEEE PSCE, March, 2011

MOD-027 Attachment 1 Turbine/Governor and Load Control or Active Power/Frequency Control Model Periodicity		
Row Number	**Verification Condition**	**Required Action**
1	Establishing the initial verification date for an applicable unit. (Requirement R2)	Transmit the verified model, documentation and data to the Transmission Planner on or before the Effective Date. Row 5 applies when calculating generation fleet compliance during the 10year implementation period. See Section A5 for Effective Dates.
2	Subsequent verification for an applicable unit. (Requirement R2)	Transmit the verified model, documentation and data to the Transmission Planner on or before the 10-year anniversary of the last transmittal (per Note 2).
3	Applicable unit is not subjected to a frequency excursion per Note 1 by the date otherwise required to meet the dates per Rows 1, 2, 4, or 6. (This row is only applicable if a frequency excursion from a system disturbance that meets Note 1 is selected for the verification method and the ability to record the applicable unit's real power response to a frequency excursion is installed and expected to be available). (Requirement R2)	Requirement 2 is met with a written statement to that effect transmitted to the Transmission Planner. Transmit the verified model, documentation and data to the Transmission Planner on or before 365 calendar days after a frequency excursion per Note 1 occurs and the recording equipment captures the applicable unit's real power response as expected.
4	Initial verification for a new applicable unit or for an existing applicable unit with new turbine/governor and load control or active power/frequency control equipment installed. (Requirement R2)	Transmit the verified model, documentation and data to the Transmission Planner within 365 calendar days after the commissioning date.

MOD-027 Attachment 1 Turbine/Governor and Load Control or Active Power/Frequency Control Model Periodicity		
Row Number	**Verification Condition**	**Required Action**
5	Existing applicable unit that is equivalent to another applicable unit(s) at the same physical location; AND Each applicable unit has the same MVA nameplate rating; AND The nameplate rating is ≤ 350 MVA; AND Each applicable unit has the same components and settings; AND The model for one of these equivalent applicable units has been verified. (Requirement R2)	Document circumstance with a written statement and include with the verified model, documentation and data provided to the Transmission Planner for the verified equivalent unit. Verify a different equivalent unit during each 10-year verification period. Applies to Row 1 when calculating generation fleet compliance during the 10-year implementation period.
6	The Generator Owner has submitted a verification plan. (Requirement R3 or R4)	Transmit the verified model, documentation and data to the Transmission Planner within 365 calendar days after the submittal of the verification plan.

MOD-027 Attachment 1 Turbine/Governor and Load Control or Active Power/Frequency Control Model Periodicity		
Row Number	**Verification Condition**	**Required Action**
7	Applicable unit is not responsive to both over and under frequency excursion events (The applicable unit does not operate in a frequency control mode, except during normal start up and shut down, that would result in a turbine/governor and load control or active power/frequency control mode response.); OR Applicable unit either does not have an installed frequency control system or has a disabled frequency control system. (Requirement R2)	Requirement 2 is met with a written statement to that effect transmitted to the Transmission Planner. Perform verification per the periodicity specified in Row 4 for a "New Generating Unit" (or new equipment) only if responsive control mode operation for connected operations is established.
8	Existing applicable unit has a current average net capacity factor over the most recent three calendar years, beginning on January 1 and ending on December 31 of 5% or less. (Requirement R2)	Requirement 2 is met with a written statement to that effect transmitted to the Transmission Planner. At the end of this 10 calendar year timeframe, the current average three year net capacity factor (for years 8, 9, and 10) can be examined to determine if the capacity factor exemption can be declared for the next 10 calendar year period. If not eligible for the capacity factor exemption, then model verification must be completed within 365 calendar days of the date the capacity factor exemption expired. For the definition of net capacity factor, refer to Appendix F of the GADS Data Reporting Instructions on the NERC website.

MOD-027 Attachment 1

Turbine/Governor and Load Control or Active Power/Frequency Control Model Periodicity

Row Number	Verification Condition	Required Action

NOTES:

NOTE 1: Unit model verification frequency excursion criteria:

- ≥ 0.05 hertz deviation (nadir point) from scheduled frequency for the Eastern Interconnection with the applicable unit operating in a frequency responsive mode
- ≥ 0.10 hertz deviation (nadir point) from scheduled frequency for the ERCOT and Western Interconnections with the applicable unit operating in a frequency responsive mode
- ≥ 0.15 hertz deviation (nadir point) from scheduled frequency for the Quebec Interconnection with the applicable unit operating in a frequency responsive mode

NOTE 2: Establishing the recurring ten year unit verification period start date:

- The start date is the actual date of submittal of a verified model to the Transmission Planner for the most recently performed unit verification.

NOTE 3: Consideration for early compliance:

Existing turbine/governor and load control or active power/frequency control model verification is sufficient for demonstrating compliance for a 10 year period from the actual transmittal date if either of the following applies:

- The Generator Owner has a verified model that is compliant with the applicable regional policies, guidelines or criteria existing at the time of model verification
- The Generator Owner has an existing verified model that is compliant with the requirements of this standard

Standard MOD-027-1 — Verification of Models and Data for Turbine/Governor and Load Control or Active Power/Frequency Control Functions

Appendix QC-MOD-027-1
Provisions specific to the standard MOD-027-1 applicable in Québec

This appendix establishes specific provisions for the application of the standard in Québec. Provisions of the standard and of its appendix must be read together for the purposes of understanding and interpretation. Where the standard and appendix differ, the appendix shall prevail.

A. Introduction

1. Title: **Verification of Models and Data for Turbine/Governor and Load Control or Active Power/Frequency Control Functions**

2. Number: MOD-027-1

3. Purpose: No specific provision

4. Applicability:

4.1. Functional entities

No specific provision

4.2. Facilities

For the purpose of the requirements contained herein, Facilities that form part of the Main Transmission System (RTP) will be collectively referred as an "applicable unit" that meet the following:

4.2.1 No specific provision

4.2.1.1 No specific provision

4.2.1.2 Individual generating plant consisting of multiple generating units that is part of the Main Transmission System (RTP) with total generation greater than 100 MVA (gross aggregate nameplate rating).

4.2.2 No specific provision

4.2.3 No specific provision

4.2.4 No specific provision

5. Effective Date:

5.1. Adoption of the standard by the Régie de l'énergie: September 27, 2017

5.2. Adoption of the appendix by the Régie de l'énergie: September 28, 2020

5.3. Effective date of the standard and its appendix in Québec: September 28, 2020

Appendix QC-MOD-027-1
Provisions specific to the standard MOD-027-1 applicable in Québec

Applicable enforcement dates for applicable facilities

Requirements	Applicability	Date of enforcement in Québec
R1 R3 to R5	100% of applicable facilities	January 1st, 2018
R2	30% of applicable facilities	April 1st, 2021
	50% of applicable facilities	October 1st, 2022
	100% of applicable facilities	October 1st, 2025

B. Requirements

No specific provision

C. Measures

No specific provision

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

The Régie de l'énergie is responsible, in Québec, for compliance monitoring with respect to the reliability standard and its appendix that it adopts.

1.2. Evidence Retention

No specific provision

1.3. Compliance Monitoring and Assessment Processes

No specific provision

1.4. Additional Compliance Information

No specific provision

2. Violation Severity Levels

No specific provision

E. Regional Variances

No specific provision

F. Associated Documents

No specific provision

G. References

No specific provision

MOD-027-1 – Attachment 1

No specific provision

Revision History

Version	Date	Action	Change Tracking
0	September 27, 2017	New appendix	New
1	September 28, 2020	Delay from October 1, 2020 to April 1, 2021 of the implementation date applicable to 30% of applicable facilities subject to requirement R2 as per decision D-2020-128	Revision

A. Introduction

1. **Title:** **Demand and Energy Data**
2. **Number:** **MOD-031-3**
3. **Purpose:** To provide authority for applicable entities to collect Demand, energy and related data to support reliability studies and assessments and to enumerate the responsibilities and obligations of requestors and respondents of that data.
4. **Applicability:**
   - **4.1. Functional Entities:**
     - **4.1.1** Planning Coordinator
     - **4.1.2** Transmission Planner
     - **4.1.3** Balancing Authority
     - **4.1.4** Resource Planner
     - **4.1.5** Distribution Provider
5. **Effective Date:** See Implementation Plan.

B. Requirements and Measures

R1. Each Planning Coordinator or Balancing Authority that identifies a need for the collection of Total Internal Demand, Net Energy for Load, and Demand Side Management data shall develop and issue a data request to the applicable entities in its area. The data request shall include: *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

- **1.1.** A list of Transmission Planners, Balancing Authorities, and Distribution Providers that are required to provide the data ("Applicable Entities").
- **1.2.** A timetable for providing the data. (A minimum of 30 calendar days must be allowed for responding to the request).
- **1.3.** A request to provide any or all of the following actual data, as necessary:
  - **1.3.1.** Integrated hourly Demands in megawatts for the prior calendar year.
  - **1.3.2.** Monthly and annual integrated peak hour Demands in megawatts for the prior calendar year.
    - **1.3.2.1.** If the annual peak hour actual Demand varies due to weather-related conditions (e.g., temperature, humidity or wind speed), the Applicable Entity shall also provide the weather normalized annual peak hour actual Demand for the prior calendar year.

1.3.3. Monthly and annual Net Energy for Load in gigawatt hours for the prior calendar year.

1.3.4. Monthly and annual peak hour controllable and dispatchable Demand Side Management under the control or supervision of the System Operator in megawatts for the prior calendar year. Three values shall be reported for each hour: 1) the committed megawatts (the amount under control or supervision), 2) the dispatched megawatts (the amount, if any, activated for use by the System Operator), and 3) the realized megawatts (the amount of actual demand reduction).

1.4. A request to provide any or all of the following forecast data, as necessary:

1.4.1. Monthly peak hour forecast Total Internal Demands in megawatts for the next two calendar years.

1.4.2. Monthly forecast Net Energy for Load in gigawatthours for the next two calendar years.

1.4.3. Peak hour forecast Total Internal Demands (summer and winter) in megawatts for ten calendar years into the future.

1.4.4. Annual forecast Net Energy for Load in gigawatthours for ten calendar years into the future.

1.4.5. Total and available peak hour forecast of controllable and dispatchable Demand Side Management (summer and winter), in megawatts, under the control or supervision of the System Operator for ten calendar years into the future.

1.5. A request to provide any or all of the following summary explanations, as necessary,:

1.5.1. The assumptions and methods used in the development of aggregated Peak Demand and Net Energy for Load forecasts.

1.5.2. The Demand and energy effects of controllable and dispatchable Demand Side Management under the control or supervision of the System Operator.

1.5.3. How Demand Side Management is addressed in the forecasts of its Peak Demand and annual Net Energy for Load.

1.5.4. How the controllable and dispatchable Demand Side Management forecast compares to actual controllable and dispatchable Demand Side Management for the prior calendar year and, if applicable, how the assumptions and methods for future forecasts were adjusted.

1.5.5. How the peak Demand forecast compares to actual Demand for the prior calendar year with due regard to any relevant weather-related variations

(e.g., temperature, humidity, or wind speed) and, if applicable, how the assumptions and methods for future forecasts were adjusted.

M1. The Planning Coordinator or Balancing Authority shall have a dated data request, either in hardcopy or electronic format, in accordance with Requirement R1.

R2. Each Applicable Entity identified in a data request shall provide the data requested by its Planning Coordinator or Balancing Authority in accordance with the data request issued pursuant to Requirement R1. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

M2. Each Applicable Entity shall have evidence, such as dated e-mails or dated transmittal letters that it provided the requested data in accordance with Requirement R2.

R3. The Planning Coordinator or the Balancing Authority shall provide the data listed under Requirement R1 Parts 1.3 through 1.5 for their area to the applicable Regional Entity within 75 calendar days of receiving a request for such data, unless otherwise agreed upon by the parties. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

M3. Each Planning Coordinator or Balancing Authority, shall have evidence, such as dated e-mails or dated transmittal letters that it provided the data requested by the applicable Regional Entity in accordance with Requirement R3.

R4. Any Applicable Entity shall, in response to a written request for the data included in parts 1.3-1.5 of Requirement R1 from a Planning Coordinator, Balancing Authority, Transmission Planner or Resource Planner with a demonstrated need for such data in order to conduct reliability assessments of the Bulk Electric System, provide or otherwise make available that data to the requesting entity. This requirement does not modify an entity's obligation pursuant to Requirement R2 to respond to data requests issued by its Planning Coordinator or Balancing Authority pursuant to Requirement R1. Unless otherwise agreed upon, the Applicable Entity: *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

- shall not be required to alter the format in which it maintains or uses the data;
- shall provide the requested data within 45 calendar days of the written request, subject to part 4.1 of this requirement; unless providing the requested data would conflict with the Applicable Entity's confidentiality, regulatory, or security requirements

4.1. If the Applicable Entity does not provide data requested because (1) the requesting entity did not demonstrate a reliability need for the data; or (2) providing the data would conflict with the Applicable Entity's confidentiality, regulatory, or security requirements, the Applicable Entity shall, within 30 calendar days of the written request, provide a written response to the requesting entity specifying the data that is not being provided and on what basis.

M4. Each Applicable Entity identified in Requirement R4 shall have evidence such as dated e-mails or dated transmittal letters that it provided the data requested or provided a written response specifying the data that is not being provided and the basis for not providing the data in accordance with Requirement R4.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

a. Evidence Retention

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Applicable Entity shall keep data or evidence to show compliance with Requirements R1 through R4, and Measures M1 through M4, since the last audit, unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

If an Applicable Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved, or for the time specified above, whichever is longer.

The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

b. Compliance Monitoring and Assessment Processes:

Compliance Audit

Self-Certification

Spot Checking

Compliance Investigation

Self-Reporting

Complaint

c. Additional Compliance Information

None

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	Long-term Planning	Medium	N/A	N/A	N/A	The Planning Coordinator or Balancing Authority developed and issued a data request but failed to include either the entity(s) necessary to provide the data or the timetable for providing the data.
R2	Long-term Planning	Medium	The Applicable Entity, as defined in the data request developed in Requirement R1, failed to provide all of the data requested in Requirement R1 part 1.5.1 through part 1.5.5 OR The Applicable Entity, as defined in the data request developed in Requirement R1, provided the data requested in Requirement R1, but	The Applicable Entity, as defined in the data request developed in Requirement R1, failed to provide one of the requested items in Requirement R1 part 1.3.1 through part 1.3.4 OR The Applicable Entity, as defined in the data request developed in Requirement R1, failed to provide one of the requested items in Requirement R1 part	The Applicable Entity, as defined in the data request developed in Requirement R1, failed to provide two of the requested items in Requirement R1 part 1.3.1 through part 1.3.4 OR The Applicable Entity, as defined in the data request developed in Requirement R1, failed to provide two of the requested items in Requirement R1 part	The Applicable Entity, as defined in the data request developed in Requirement R1, failed to provide three or more of the requested items in Requirement R1 part 1.3.1 through part 1.3.4 OR The Applicable Entity, as defined in the data request developed in Requirement R1, failed to provide three or more of the requested items in Requirement R1 part 1.4.1 through part 1.4.5

			did so after the date indicated in the timetable provided pursuant to Requirement R1 part 1.2 but prior to 6 days after the date indicated in the timetable provided pursuant to Requirement R1 part 1.2.	1.4.1 through part 1.4.5 OR The Applicable Entity, as defined in the data request developed in Requirement R1, provided the data requested in Requirement R1, but did so 6 days after the date indicated in the timetable provided pursuant to Requirement R1 part 1.2 but prior to 11 days after the date indicated in the timetable provided pursuant to Requirement R1 part 1.2.	1.4.1 through part 1.4.5 OR The Applicable Entity, as defined in the data request developed in Requirement R1, provided the data requested in Requirement R1, but did so 11 days after the date indicated in the timetable provided pursuant to Requirement R1 part 1.2 but prior to 15 days after the date indicated in the timetable provided pursuant to Requirement R1 part 1.2.	OR The Applicable Entity, as defined in the data request developed in Requirement R1, failed to provide the data requested in the timetable provided pursuant to Requirement R1 prior to 16 days after the date indicated in the timetable provided pursuant to Requirement R1 part 1.2.
R3	Long-term Planning	Medium	The Planning Coordinator or Balancing Authority, in response to a request by the Regional Entity, made available the data requested, but did so after 75 days	The Planning Coordinator or Balancing Authority, in response to a request by the Regional Entity, made available the data requested, but did so after 80 days	The Planning Coordinator or Balancing Authority, in response to a request by the Regional Entity, made available the data requested, but did so after 85 days	The Planning Coordinator or Balancing Authority, in response to a request by the Regional Entity, failed to make available the data requested prior to 91 days

			from the date of request but prior to 81 days from the date of the request.	from the date of request but prior to 86 days from the date of the request.	from the date of request but prior to 91 days from the date of the request.	or more from the date of the request.
R4	Long-term Planning	Medium	The Applicable Entity provided or otherwise made available the data to the requesting entity but did so after 45 days from the date of request but prior to 51 days from the date of the request OR The Applicable Entity that is not providing the data requested provided a written response specifying the data that is not being provided and on what basis but did so after 30 days of the written request but prior to 36 days of the written request.	The Applicable Entity provided or otherwise made available the data to the requesting entity but did so after 50 days from the date of request but prior to 56 days from the date of the request OR The Applicable Entity that is not providing the data requested provided a written response specifying the data that is not being provided and on what basis but did so after 35 days of the written request but prior to 41 days of the written request.	The Applicable Entity provided or otherwise made available the data to the requesting entity but did so after 55 days from the date of request but prior to 61 days from the date of the request OR The Applicable Entity that is not providing the data requested provided a written response specifying the data that is not being provided and on what basis but did so after 40 days of the written request but prior to 46 days of the written request.	The Applicable Entity failed to provide or otherwise make available the data to the requesting entity within 60 days from the date of the request OR The Applicable Entity that is not providing the data requested failed to provide a written response specifying the data that is not being provided and on what basis within 45 days of the written request.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	May 6, 2014	Adopted by the NERC Board of Trustees	
1	February 19, 2015	FERC order approving MOD-031-1	
2	November 5, 2015	Adopted by the NERC Board of Trustees	
2	February 18, 2016	FERC order approving MOD-031-2. Docket No. RD16-1-000	
3	February 6, 2020	Adopted by the NERC Board of Trustees	Revisions under Project 2017-07
3	October 30,2020	FERC order approving MOD-031-3 Docket No. RD20-4-000	
3	April 1, 2021	Effective Date	

Guidelines and Technical Basis

Rationale

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for R1:

Rationale for R1: To ensure that when Planning Coordinators (PCs) or Balancing Authorities (BAs) request data (R1), they identify the entities that must provide the data (Applicable Entity in part 1.1), the data to be provided (parts 1.3 – 1.5) and the due dates (part 1.2) for the requested data.

For Requirement R1 part 1.3.2.1, if the Demand does not vary due to weather-related conditions (e.g., temperature, humidity or wind speed), or the weather assumed in the forecast was the same as the actual weather, the weather normalized actual Demand will be the same as the actual demand reported for Requirement R1 part 1.3.2. Otherwise the annual peak hour weather normalized actual Demand will be different from the actual demand reported for Requirement R1 part 1.3.2.

Balancing Authorities are included here to reflect a practice in the WECC Region where BAs are the entity that perform this requirement in lieu of the PC.

Rationale for R2:

This requirement will ensure that entities identified in Requirement R1, as responsible for providing data, provide the data in accordance with the details described in the data request developed in accordance with Requirement R1. In no event shall the Applicable Entity be required to provide data under this requirement that is outside the scope of parts 1.3 - 1.5 of Requirement R1.

Rationale for R3:

This requirement will ensure that the Planning Coordinator or when applicable, the Balancing Authority, provides the data requested by the Regional Entity.

Rationale for R4:

This requirement will ensure that the Applicable Entity will make the data requested by the Planning Coordinator or Balancing Authority in Requirement R1 available to other applicable entities (Planning Coordinator, Balancing Authority, Transmission Planner or Resource Planner) unless providing the data would conflict with the Applicable Entity's confidentiality, regulatory, or security requirements. The sharing of documentation of the supporting methods and assumptions used to develop forecasts as well as information-sharing activities will improve the efficiency of planning practices and support the identification of needed system reinforcements.

The obligation to share data under Requirement R4 does not supersede or otherwise modify any of the Applicable Entity's existing confidentiality obligations. For instance, if an entity is prohibited from providing any of the requested data pursuant to confidentiality provisions of an Open Access Transmission Tariff or a contractual arrangement, Requirement R4 does not require the Applicable Entity to provide the data to a requesting entity. Rather, under Part 4.1, the Applicable Entity must simply provide written notification to the requesting entity that it will not be providing the data and the basis for not providing the data. If the Applicable Entity is subject to confidentiality obligations that allow the Applicable Entity to share the data only if certain conditions are met, the Applicable Entity shall ensure that those conditions are met within the 45-day time period provided in Requirement R4, communicate with the requesting entity regarding an extension of the 45-day time period so as to meet all those conditions, or provide justification under Part 4.1 as to why those conditions cannot be met under the circumstances.

Appendix MOD-031-3-QC-1
Specific provisions applicable in Québec for standard MOD-031-3 — Demand and Energy Data

This appendix establishes specific provisions for the application of the standard in Québec. Provisions of the standard and of this appendix must be read jointly for comprehension and interpretation purposes. Where the standard and appendix differ, the appendix shall prevail.

A. Introduction

1. Title: No specific provision

2. Number: No specific provision

3. Purpose: No specific provision

4. Applicability:

Functional Entities

No specific provision

Facilities

No specific provision

5. Effective Date:

5.1. Adoption of the standard by the Régie de l'énergie: June 28, 2022

5.2. Adoption of the appendix by the Régie de l'énergie: June 28, 2022

5.3. Effective date of the standard and its appendix in Québec: October 1, 2022

B. Requirements and measures

No specific provision

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

In Québec, "Compliance Enforcement Authority" means the Régie de l'énergie in its roles of monitoring and enforcing compliance with respect to the Reliability Standard and to this appendix.

1.2 Evidence retention

No specific provision

1.3 Compliance Monitoring and Assessment Processes

The Régie de l'énergie establishes the monitoring processes used to evaluate data or information for the purpose of determining compliance or non-compliance with the Reliability Standard and with this appendix.

1.4 Additional Compliance Information

No specific provision

Table of Compliance Elements

No specific provision

D. Regional Differences

No specific provision.

E. Interpretations

No specific provision

F. Associated Documents

No specific provision

Guidelines and Technical Basis

No specific provision

Version history

Version	Date	Action	Change Tracking
1	June 28, 2022	New appendix as per decision D-2022-085	New

A. Introduction

1. **Title: Data for Power System Modeling and Analysis**

2. **Number: MOD-032-1**

3. **Purpose:** To establish consistent modeling data requirements and reporting procedures for development of planning horizon cases necessary to support analysis of the reliability of the interconnected transmission system.

4. **Applicability:**

   4.1. Functional Entities:

   4.1.1 Balancing Authority

   4.1.2 Generator Owner

   4.1.3 Load Serving Entity

   4.1.4 Planning Authority and Planning Coordinator (hereafter collectively referred to as "Planning Coordinator")

   This proposed standard combines "Planning Authority" with "Planning Coordinator" in the list of applicable functional entities. The NERC Functional Model lists "Planning Coordinator" while the registration criteria list "Planning Authority," and they are not yet synchronized. Until that occurs, the proposed standard applies to both Planning Authority and Planning Coordinator.

   4.1.5 Resource Planner

   4.1.6 Transmission Owner

   4.1.7 Transmission Planner

   4.1.8 Transmission Service Provider

5. **Effective Date:**

MOD-032-1, Requirement R1 shall become effective on the first day of the first calendar quarter that is 12 months after the date that the standard is approved by an applicable governmental authority or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, MOD-032-1, Requirement R1 shall become effective on the first day of the first calendar quarter that is 12 months after the date the standard is adopted by the NERC Board of Trustees or as otherwise provided for in that jurisdiction.

MOD-032-1, Requirements R2, R3, and R4 shall become effective on the first day of the first calendar quarter that is 24 months after the date that the standard is approved by an applicable governmental authority or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority

is not required, MOD-032-1, Requirements R2, R3, and R4 shall become effective on the first day of the first calendar quarter that is 24 months after the date the standard is adopted by the NERC Board of Trustees or as otherwise provided for in that jurisdiction.

6. Background:

MOD-032-1 exists in conjunction with MOD-033-1, both of which are related to system-level modeling and validation. Reliability Standard MOD-032-1 is a consolidation and replacement of existing MOD-010-0, MOD-011-0, MOD-012-0, MOD-013-1, MOD-014-0, and MOD-015-0.1, and it requires data submission by applicable data owners to their respective Transmission Planners and Planning Coordinators to support the Interconnection-wide case building process in their Interconnection. Reliability Standard MOD-033-1 is a new standard, and it requires each Planning Coordinator to implement a documented process to perform model validation within its planning area.

The transition and focus of responsibility upon the Planning Coordinator function in both standards are driven by several recommendations and FERC directives from FERC Order No. 693, which are discussed in greater detail in the rationale sections of the standards. One of the most recent and significant set of recommendations came from the NERC Planning Committee's System Analysis and Modeling Subcommittee (SAMS). SAMS proposed several improvements to the modeling data standards, to include consolidation of the standards (the SAMS whitepaper is available from the December 2012 NERC Planning Committee's agenda package, item 3.4, beginning on page 99, here: http://www.nerc.com/comm/PC/Agendas%20Highlights%20and%20Minutes%20DL/2012/2012_Dec_PC%20Agenda.pdf).

B. Requirements and Measures

R1. Each Planning Coordinator and each of its Transmission Planners shall jointly develop steady-state, dynamics, and short circuit modeling data requirements and reporting procedures for the Planning Coordinator's planning area that include: *[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*

1.1. The data listed in Attachment 1.

1.2. Specifications of the following items consistent with procedures for building the Interconnection-wide case(s):

1.2.1. Data format;

1.2.2. Level of detail to which equipment shall be modeled;

1.2.3. Case types or scenarios to be modeled; and

1.2.4. A schedule for submission of data at least once every 13 calendar months.

1.3. Specifications for distribution or posting of the data requirements and reporting procedures so that they are available to those entities responsible for providing the data.

M1. Each Planning Coordinator and Transmission Planner shall provide evidence that it has jointly developed the required modeling data requirements and reporting procedures specified in Requirement R1.

R2. Each Balancing Authority, Generator Owner, Load Serving Entity, Resource Planner, Transmission Owner, and Transmission Service Provider shall provide steady-state, dynamics, and short circuit modeling data to its Transmission Planner(s) and Planning Coordinator(s) according to the data requirements and reporting procedures developed by its Planning Coordinator and Transmission Planner in Requirement R1. For data that has not changed since the last submission, a written confirmation that the data has not changed is sufficient. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

M2. Each registered entity identified in Requirement R2 shall provide evidence, such as email records or postal receipts showing recipient and date, that it has submitted the required modeling data to its Transmission Planner(s) and Planning Coordinator(s); or written confirmation that the data has not changed.

R3. Upon receipt of written notification from its Planning Coordinator or Transmission Planner regarding technical concerns with the data submitted under Requirement R2, including the technical basis or reason for the technical concerns, each notified Balancing Authority, Generator Owner, Load Serving Entity, Resource Planner, Transmission Owner, or Transmission Service Provider shall respond to the notifying Planning Coordinator or Transmission Planner as follows: *[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*

3.1. Provide either updated data or an explanation with a technical basis for maintaining the current data;

3.2. Provide the response within 90 calendar days of receipt, unless a longer time period is agreed upon by the notifying Planning Coordinator or Transmission Planner.

M3. Each registered entity identified in Requirement R3 that has received written notification from its Planning Coordinator or Transmission Planner regarding technical concerns with the data submitted under Requirement R2 shall provide evidence, such as email records or postal receipts showing recipient and date, that it has provided either updated data or an explanation with a technical basis for maintaining the current data to its Planning Coordinator or Transmission Planner within 90 calendar days of receipt (or within the longer time period agreed upon by the notifying Planning Coordinator or Transmission Planner), or a statement that it has not received written notification regarding technical concerns with the data submitted.

R4. Each Planning Coordinator shall make available models for its planning area reflecting data provided to it under Requirement R2 to the Electric Reliability Organization (ERO) or its designee to support creation of the Interconnection-wide case(s) that includes the Planning Coordinator's planning area. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

M4. Each Planning Coordinator shall provide evidence, such as email records or postal receipts showing recipient and date, that it has submitted models for its planning area reflecting data provided to it under Requirement R2 when requested by the ERO or its designee.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

"Compliance Enforcement Authority" means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The applicable entity shall keep data or evidence to show compliance with Requirements R1 through R4, and Measures M1 through M4, since the last audit, unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

If an applicable entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved, or for the time specified above, whichever is longer.

The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

Refer to the NERC Rules of Procedure for a list of compliance monitoring and assessment processes.

1.4. Additional Compliance Information

None

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Long-term Planning**	**Lower**	The Planning Coordinator and Transmission Planner(s) developed steady-state, dynamics, and short circuit modeling data requirements and reporting procedures, but failed to include less than or equal to 25% of the required components specified in Requirement R1.	The Planning Coordinator and Transmission Planner(s) developed steady-state, dynamics, and short circuit modeling data requirements and reporting procedures, but failed to include greater than 25% but less than or equal to 50% of the required components specified in Requirement R1.	The Planning Coordinator and Transmission Planner(s) developed steady-state, dynamics, and short circuit modeling data requirements and reporting procedures, but failed to include greater than 50% but less than or equal to 75% of the required components specified in Requirement R1.	The Planning and Transmission Planner(s) Coordinator did not develop any steady-state, dynamics, and short circuit modeling data requirements and reporting procedures required by Requirement R1; OR The Planning Coordinator and Transmission Planner(s) developed steady-state, dynamics, and short circuit modeling data requirements and reporting procedures, but failed to include greater than 75% of the required components specified

						in Requirement R1.
R2	**Long-term Planning**	**Medium**	The Balancing Authority, Generator Owner, Load Serving Entity, Resource Planner, Transmission Owner, or Transmission Service Provider provided steady-state, dynamics, and short circuit modeling data to its Transmission Planner(s) and Planning Coordinator(s), but failed to provide less than or equal to 25% of the required data specified in Attachment 1; OR The Balancing Authority, Generator Owner, Load Serving Entity, Resource Planner, Transmission Owner, or Transmission Service Provider provided	The Balancing Authority, Generator Owner, Load Serving Entity, Resource Planner, Transmission Owner, or Transmission Service Provider provided steady-state, dynamics, and short circuit modeling data to its Transmission Planner(s) and Planning Coordinator(s), but failed to provide greater than 25% but less than or equal to 50% of the required data specified in Attachment 1; OR The Balancing Authority, Generator Owner, Load Serving Entity, Resource Planner, Transmission Owner, or Transmission Service	The Balancing Authority, Generator Owner, Load Serving Entity, Resource Planner, Transmission Owner, or Transmission Service Provider provided steady-state, dynamics, and short circuit modeling data to its Transmission Planner(s) and Planning Coordinator(s), but failed to provide greater than 50% but less than or equal to 75% of the required data specified in Attachment 1; OR The Balancing Authority, Generator Owner, Load Serving Entity, Resource Planner, Transmission Owner, or Transmission Service	The Balancing Authority, Generator Owner, Load Serving Entity, Resource Planner, Transmission Owner, or Transmission Service Provider did not provide any steady-state, dynamics, and short circuit modeling data to its Transmission Planner(s) and Planning Coordinator(s); OR The Balancing Authority, Generator Owner, Load Serving Entity, Resource Planner, Transmission Owner, or Transmission Service Provider provided steady-state, dynamics, and short circuit modeling data to its Transmission

			steady-state, dynamics, and short circuit modeling data to its Transmission Planner(s) and Planning Coordinator(s), but less than or equal to 25% of the required data failed to meet data format, shareability, level of detail, or case type specifications; OR The Balancing Authority, Generator Owner, Load Serving Entity, Resource Planner, Transmission Owner, or Transmission Service Provider failed to provide steady-state, dynamics, and short circuit modeling data to its Transmission Planner(s) and Planning Coordinator(s) within the schedule specified	Provider provided steady-state, dynamics, and short circuit modeling data to its Transmission Planner(s) and Planning Coordinator(s), but greater than 25% but less than or equal to 50% of the required data failed to meet data format, shareability, level of detail, or case type specifications; OR The Balancing Authority, Generator Owner, Load Serving Entity, Resource Planner, Transmission Owner, or Transmission Service Provider failed to provide steady-state, dynamics, and short circuit modeling data to its Transmission Planner(s) and Planning	Provider provided steady-state, dynamics, and short circuit modeling data to its Transmission Planner(s) and Planning Coordinator(s), but greater than 50% but less than or equal to 75% of the required data failed to meet data format, shareability, level of detail, or case type specifications; OR The Balancing Authority, Generator Owner, Load Serving Entity, Resource Planner, Transmission Owner, or Transmission Service Provider failed to provide steady-state, dynamics, and short circuit modeling data to its Transmission Planner(s) and Planning	Planner(s) and Planning Coordinator(s), but failed to provide greater than 75% of the required data specified in Attachment 1; OR The Balancing Authority, Generator Owner, Load Serving Entity, Resource Planner, Transmission Owner, or Transmission Service Provider provided steady-state, dynamics, and short circuit modeling data to its Transmission Planner(s) and Planning Coordinator(s), but greater than 75% of the required data failed to meet data format, shareability, level of detail, or case type specifications;

			by the data requirements and reporting procedures but did provide the data in less than or equal to 15 calendar days after the specified date.	Coordinator(s) within the schedule specified by the data requirements and reporting procedures but did provide the data in greater than 15 but less than or equal to 30 calendar days after the specified date.	Coordinator(s) within the schedule specified by the data requirements and reporting procedures but did provide the data in greater than 30 but less than or equal to 45 calendar days after the specified date.	OR The Balancing Authority, Generator Owner, Load Serving Entity, Resource Planner, or Transmission Service Provider failed to provide steady-state, dynamics, and short circuit modeling data to its Transmission Planner(s) and Planning Coordinator(s) within the schedule specified by the data requirements and reporting procedures but did provide the data in greater than 45 calendar days after the specified date.
R3	**Long-term Planning**	**Lower**	The Balancing Authority, Generator Owner, Load Serving Entity, Resource Planner, Transmission Owner, or Transmission Service	The Balancing Authority, Generator Owner, Load Serving Entity, Resource Planner, Transmission Owner, or Transmission Service	The Balancing Authority, Generator Owner, Load Serving Entity, Resource Planner, Transmission Owner, or Transmission Service	The Balancing Authority, Generator Owner, Load Serving Entity, Resource Planner, Transmission Owner, or Transmission Service

			Provider failed to provide a written response to its Transmission Planner(s) or Planning Coordinator(s) according to the specifications of Requirement R4 within 90 calendar days (or within a longer period agreed upon by the notifying Planning Coordinator or Transmission Planner), but did provide the response within 105 calendar days (or within 15 calendar days after the longer period agreed upon by the notifying Planning Coordinator or Transmission Planner).	Provider failed to provide a written response to its Transmission Planner(s) or Planning Coordinator(s) according to the specifications of Requirement R4 within 90 calendar days (or within a longer period agreed upon by the notifying Planning Coordinator or Transmission Planner), but did provide the response within greater than 105 calendar days but less than or equal to 120 calendar days (or within greater than 15 calendar days but less than or equal to 30 calendar days after the longer period agreed upon by the notifying Planning Coordinator or Transmission Planner).	Provider failed to provide a written response to its Transmission Planner(s) or Planning Coordinator(s) according to the specifications of Requirement R4 within 90 calendar days (or within a longer period agreed upon by the notifying Planning Coordinator or Transmission Planner), but did provide the response within greater than 120 calendar days but less than or equal to 135 calendar days (or within greater than 30 calendar days but less than or equal to 45 calendar days after the longer period agreed upon by the notifying Planning Coordinator or Transmission Planner).	Provider failed to provide a written response to its Transmission Planner(s) or Planning Coordinator(s) according to the specifications of Requirement R4 within 135 calendar days (or within a longer period agreed upon by the notifying Planning Coordinator or Transmission Planner).

R4	**Long-term Planning**	**Medium**	The Planning Coordinator made available the required data to the ERO or its designee but failed to provide less than or equal to 25% of the required data in the format specified by the ERO or its designee.	The Planning Coordinator made available the required data to the ERO or its designee but failed to provide greater than 25% but less than or equal to 50% of the required data in the format specified by the ERO or its designee.	The Planning Coordinator made available the required data to the ERO or its designee but failed to provide greater than 50% but less than or equal to 75% of the required data in the format specified by the ERO or its designee.	The Planning Coordinator made available the required data to the ERO or its designee but failed to provide greater than 75% of the required data in the format specified by the ERO or its designee.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

MOD-032-01 – ATTACHMENT 1:

Data Reporting Requirements

The table, below, indicates the information that is required to effectively model the interconnected transmission system for the Near-Term Transmission Planning Horizon and Long-Term Transmission Planning Horizon. Data must be shareable on an interconnection-wide basis to support use in the Interconnection-wide cases. A Planning Coordinator may specify additional information that includes specific information required for each item in the table below. Each functional entity[1] responsible for reporting the respective data in the table is identified by brackets "[functional entity]" adjacent to and following each data item. The data reported shall be as identified by the bus number, name, and/or identifier that is assigned in conjunction with the PC, TO, or TP.

steady-state *(Items marked with an asterisk indicate data that vary with system operating state or conditions. Those items may have different data provided for different modeling scenarios)*	**dynamics** *(If a user-written model(s) is submitted in place of a generic or library model, it must include the characteristics of the model, including block diagrams, values and names for all model parameters, and a list of all state variables)*	**short circuit**
1. Each bus [TO] a. nominal voltage b. area, zone and owner 2. Aggregate Demand[2] [LSE] a. real and reactive power* b. in-service status* 3. Generating Units[3] [GO, RP (for future planned resources only)] a. real power capabilities - gross maximum and minimum values b. reactive power capabilities - maximum and minimum values at	1. Generator [GO, RP (for future planned resources only)] 2. Excitation System [GO, RP(for future planned resources only)] 3. Governor [GO, RP(for future planned resources only)] 4. Power System Stabilizer [GO, RP(for future planned resources only)] 5. Demand [LSE]	1. Provide for all applicable elements in column "steady-state" [GO, RP, TO] a. Positive Sequence Data b. Negative Sequence Data c. Zero Sequence Data 2. Mutual Line Impedance Data [TO] 3. Other information requested by the Planning Coordinator or Transmission Planner necessary for modeling

[1] For purposes of this attachment, the functional entity references are represented by abbreviations as follows: Balancing Authority (BA), Generator Owner (GO), Load Serving Entity (LSE), Planning Coordinator (PC), Resource Planner (RP), Transmission Owner (TO), Transmission Planner (TP), and Transmission Service Provider (TSP).

[2] For purposes of this item, aggregate Demand is the Demand aggregated at each bus under item 1 that is identified by a Transmission Owner as a load serving bus. A Load Serving Entity is responsible for providing this information, generally through coordination with the Transmission Owner.

[3] Including synchronous condensers and pumped storage.

steady-state *(Items marked with an asterisk indicate data that vary with system operating state or conditions. Those items may have different data provided for different modeling scenarios)*	**dynamics** *(If a user-written model(s) is submitted in place of a generic or library model, it must include the characteristics of the model, including block diagrams, values and names for all model parameters, and a list of all state variables)*	**short circuit**
real power capabilities in 3a above c. station service auxiliary load for normal plant configuration (provide data in the same manner as that required for aggregate Demand under item 2, above). d. regulated bus* and voltage set point* (as typically provided by the TOP) e. machine MVA base f. generator step up transformer data (provide same data as that required for transformer under item 6, below) g. generator type (hydro, wind, fossil, solar, nuclear, etc) h. in-service status* 4. AC Transmission Line or Circuit [TO] a. impedance parameters (positive sequence) b. susceptance (line charging) c. ratings (normal and emergency)* d. in-service status* 5. DC Transmission systems [TO] 6. Transformer (voltage and phase-shifting) [TO] a. nominal voltages of windings b. impedance(s) c. tap ratios (voltage or phase angle)* d. minimum and maximum tap position limits e. number of tap positions (for both the ULTC and NLTC) f. regulated bus (for voltage regulating transformers)* g. ratings (normal and emergency)* h. in-service status* 7. Reactive compensation (shunt capacitors and reactors) [TO] a. admittances (MVars) of each capacitor and reactor b. regulated voltage band limits* (if mode of operation not fixed) c. mode of operation (fixed, discrete, continuous, etc.) d. regulated bus* (if mode of operation not fixed) e. in-service status* 8. Static Var Systems [TO]	6. Wind Turbine Data [GO] 7. Photovoltaic systems [GO] 8. Static Var Systems and FACTS [GO, TO, LSE] 9. DC system models [TO] 10. Other information requested by the Planning Coordinator or Transmission Planner necessary for modeling purposes. [BA, GO, LSE, TO, TSP]	purposes. [BA, GO, LSE, TO, TSP]

steady-state *(Items marked with an asterisk indicate data that vary with system operating state or conditions. Those items may have different data provided for different modeling scenarios)*	**dynamics** *(If a user-written model(s) is submitted in place of a generic or library model, it must include the characteristics of the model, including block diagrams, values and names for all model parameters, and a list of all state variables)*	**short circuit**
a. reactive limits b. voltage set point* c. fixed/switched shunt, if applicable d. in-service status* 9. Other information requested by the Planning Coordinator or Transmission Planner necessary for modeling purposes. [BA, GO, LSE, TO, TSP]		

Guidelines and Technical Basis

For purposes of jointly developing steady-state, dynamics, and short circuit modeling data requirements and reporting procedures under Requirement R1, if a Transmission Planner (TP) and Planning Coordinator (PC) mutually agree, a TP may collect and aggregate some or all data from providing entities, and the TP may then provide that data directly to the PC(s) on behalf of the providing entities. The submitting entities are responsible for getting the data to both the TP and the PC, but nothing precludes them from arriving at mutual agreements for them to provide it to the TP, who then provides it to the PC. Such agreement does not relieve the submitting entity from responsibility under the standard, nor does it make the consolidating entity liable for the submitting entities' compliance under the standard (in essence, nothing precludes parties from agreeing to consolidate or act as a conduit to pass the data, and it is in fact encouraged in certain circumstances, but the requirement is aimed at the act of submitting the data). Notably, there is no requirement for the TP to provide data to the PC. The intent, in part, is to address potential concerns from entities that they would otherwise be responsible for the quality, nature, and sufficiency of the data provided by other entities.

The requirement in Part 1.3 to include specifications for distribution or posting of the data requirements and reporting procedures could be accomplished in many ways, to include posting on a Web site, distributing directly, or through other methods that the Planning Coordinator and each of its Transmission Planners develop.

An entity submitting data per the requirements of this standard who needs to determine the PC for the area, as a starting point, should contact the local Transmission Owner (TO) for information on the TO's PC. Typically, the PC will be the same for both the local TO and those entities connected to the TO's system. If this is not the case, the local TO's PC can typically provide contact information on other PCs in the area. If the entity (e.g., a Generator Owner [GO]) is requesting connection of a new generator, the entity can determine who the PC is for that area at the time a generator connection request is submitted. Often the TO and PC are the same entity, or the TO can provide information on contacting the PC. The entity should specify as the reason for the request to the TO that the entity needs to provide data to the PC according to this standard. Nothing in the proposed requirement language of this standard is intended to preclude coordination between entities such that one entity, serving only as a conduit, provides the other entity's data to the PC. This can be accomplished if it is mutually agreeable by, for example, the GO (or other entity), TP, and the PC. This does not, however, relieve the original entity from its obligations under the standard to provide data, nor does it pass on the compliance obligation of the entity. The original entity is still accountable for making sure that the data has been provided to the PC according to the requirements of this standard.

The standard language recognizes that differences exist among the Interconnections. Presently, the Eastern/Quebec and Texas Interconnections build seasonal cases on an annual basis, while the Western Interconnection builds cases on a continuous basis throughout the year. The intent of the standard is not to change established processes and procedures in each of the Interconnections, but to create a framework to support both what is already in place or

what it may transition into in the future, and to provide further guidance in a common platform for the collection of data that is necessary for the building of the Interconnection-wide case(s).

The construct that these standards replace did not specifically list which Functional Entities were required to provide specific data. Attachment 1 specifically identifies the entities responsible for the data required for the building of the Interconnection-wide case(s).

Rationale:

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for R1:

This requirement consolidates the concepts from the original data requirements from MOD-011-0, Requirement R1, and MOD-013-0, Requirement R1. The original requirements specified types of steady-state and dynamics data necessary to model and analyze the steady-state conditions and dynamic behavior or response within each Interconnection. The original requirements, however, did not account for the collection of short circuit data also required to perform short circuit studies. The addition of short circuit data also addresses the outstanding directive from FERC Order No. 890, paragraph 290.

In developing a performance-based standard that would address the data requirements and reporting procedures for model data, it was prohibitively difficult to account for all of the detailed technical concerns associated with the preparation and submittal of model data given that many of these concerns are dependent upon evolving industry modeling needs and software vendor terminology and product capabilities.

This requirement establishes the Planning Coordinator jointly with its Transmission Planners as the developers of technical model data requirements and reporting procedures to be followed by the data owners in the Planning Coordinator's planning area. FERC Order No. 693, paragraphs 1155 and 1162, also direct that the standard apply to Planning Coordinators. The inclusion of Transmission Planners in the applicability section is intended to ensure that the Transmission Planners are able to participate jointly in the development of the data requirements and reporting procedures.

This requirement is also consistent with the recommendations from the NERC System Analysis and Modeling Subcommittee (SAMS) White Paper titled "Proposed Improvements for NERC MOD Standards", available from the December 2012 NERC Planning Committee's agenda package, item 3.4, beginning on page 99, here:

Aside from recommendations in support of strengthening and improving MOD-010 through MOD-015, the SAMS paper included the following suggested improvements:

1) reduce the quantity of MOD standards;
2) add short circuit data as a requirement to the MOD standards; and
3) supply data and models:

a. add requirement identifying who provides and who receives data;
b. identify acceptability;
c. standard format;
d. how to deal with new technologies (user written models if no standard model exists); and
e. shareability.

4) These suggested improvements are addressed by combining the existing standards into two new standards, one standard for the submission and collection of data, and one for the validation of the planning models. Adding the requirement for the submittal of short circuit data is also an improvement from the existing standards, consistent with FERC Order No. 890, paragraph 290. In supplying data, the approach clearly identifies what data is required and which Functional Entity is required to provide the data.
5) The requirement uses an attachment approach to support data collection. The attachment specifically lists the entities that are required to provide each type of data and the steady-state, dynamics, and short circuit data that is required.
6) Finally, the decision to combine steady-state, dynamics, and short circuit data requirements into one requirement rather than three reflects that they all support the requirement of submission of data in general.

Rationale for R2:

This requirement satisfies the directive from FERC Order No. 693, paragraph 1155, which directs that "the planning authority should be included in this Reliability Standard because the planning authority is the entity responsible for the coordination and integration of transmission facilities and resource plans, as well as one of the entities responsible for the integrity and consistency of the data."

Rationale for R3:

In order to maintain a certain level of accuracy in the representation of a power system, the data that is submitted must be correct, periodically checked, and updated. Data used to perform steady-state, dynamics, and short circuit studies can change, for example, as a result of new planned transmission construction (in comparison to as-built information) or changes performed during the restoration of the transmission network due to weather-related events. One set of data that changes on a more frequent basis is load data, and updates to load data are needed when new improved forecasts are created.

This requirement provides a mechanism for the Planning Coordinator and Transmission Planner (that does not exist in the current standards) to collect corrected data from the entities that have the data. It provides a feedback loop to address technical concerns related to the data when the Planning Coordinator or Transmission Planner identifies technical concerns, such as concerns about the usability of data or simply that the data is not in the correct format and cannot be used. The requirement also establishes a time-frame for response to address timeliness.

Rationale for R4:

This requirement will replace MOD-014 and MOD-015.

This requirement recognizes the differences among Interconnections in model building processes, and it creates an obligation for Planning Coordinators to make available data for its planning area.

The requirement creates a clear expectation that Planning Coordinators will make available data that they collect under Requirement R2 in support of their respective Interconnection-wide case(s). While different entities in each Interconnection create the Interconnection-wide case(s), the requirement to submit the data to the "ERO or its designee" supports a framework whereby NERC, in collaboration and agreement with those other organizations, can designate the appropriate organizations in each Interconnection to build the specific Interconnection-wide case(s). It does not prescribe a specific group or process to build the larger Interconnection-wide case(s), but only requires the Planning Coordinators to make available data in support of their creation, consistent with the SAMS Proposed Improvements to NERC MOD Standards (at page 3) that, "industry best practices and existing processes should be considered in the development of requirements, *as many entities are successfully coordinating their efforts.*" (Emphasis added).

This requirement is about the Planning Coordinator's obligation to make information available for use in the Interconnection-wide case(s); it is not a requirement to build the Interconnection-wide case(s).

For example, under current practice, the Eastern Interconnection Reliability Assessment Group (ERAG) builds the Eastern Interconnection and Quebec Interconnection-wide cases, the Western Electricity Coordinating Council (WECC) builds the Western Interconnection-wide cases, and the Electric Reliability Council of Texas (ERCOT) builds the Texas Interconnection-wide cases. This requirement does not require a change to that construct, and, assuming continued agreement by those organizations, ERAG, WECC, and ERCOT could be the "designee" for each Interconnection contemplated by this requirement. Similarly, the requirement does not prohibit transition, and the requirement remains for the Planning Coordinators to make available the information to the ERO or to whomever the ERO has coordinated with and designated as the recipient of such information for purposes of creation of each of the Interconnection–wide cases.

Version History

Version	Date	Action	Change Tracking
1	February 6, 2014	Adopted by the NERC Board of Trustees.	Developed to consolidate and replace MOD-010-0, MOD -011-0, MOD-012-0, MOD-013-1, MOD-014-0, and MOD-015-0.1
1	May 1, 2014	FERC Order issued approving	See Implementation Plan

		MOD-032-1.	posted on the Reliability Standards web page for details on enforcement dates for Requirements.

Appendix QC-MOD-032-1
Provisions specific to the standard MOD-032-1 applicable in Québec

This appendix establishes specific provisions for the application of the standard in Québec. Provisions of the standard and of its appendix must be read together for the purposes of understanding and interpretation. Where the standard and appendix differ, the appendix shall prevail.

A. Introduction

1. Title: **Data for Power System Modeling and Analysis**

2. Number: MOD-032-1

3. Purpose: No specific provision

4. Applicability:

4.1. Functional entities

No specific provision

5. Effective Date:

5.1. Adoption of the standard by the Régie de l'énergie: December 22, 2016

5.2. Adoption of the appendix by the Régie de l'énergie: December 22, 2016

5.3. Effective date of the standard and its appendix in Québec:

R1: April 1, 2017

R2, R3, R4: January 1, 2018

6. Background: No specific provision

B. Requirements and Measures

No specific provision

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

The Régie de l'énergie is responsible, in Québec, for compliance monitoring with respect to the reliability standard and its appendix that it adopts.

1.2. Evidence Retention

No specific provision

1.3. Compliance Monitoring and Assessment Processes

Compliance Audit

Self-Certification

Spot Check

Compliance Investigation

Self-Reporting

Periodic Data Submittal

Exception Reporting

Investigation following a complaint

1.4. Additional Compliance Information

No specific provision

Table of Compliance Elements

No specific provision

D. Regional Variances

No specific provision

E. Interpretations

No specific provision

F. Associated Documents

No specific provision

MOD-032-1 – Attachment 1

No specific provision

Guidelines and Technical Basis

No specific provision

Revision History

Version	Date	Action	Change Tracking
0	December 22, 2016	New appendix	New

A. Introduction

1. **Title: Steady-State and Dynamic System Model Validation**

2. **Number: MOD-033-2**

3. **Purpose:** To establish consistent validation requirements to facilitate the collection of accurate data and building of planning models to analyze the reliability of the interconnected transmission system.

4. **Applicability:**

   4.1. Functional Entities:

   4.1.1 Planning Coordinator

   4.1.2 Reliability Coordinator

   4.1.3 Transmission Operator

5. **Effective Date:** See Implementation Plan.

B. Requirements and Measures

R1. Each Planning Coordinator shall implement a documented data validation process that includes the following attributes: *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

1.1. Comparison of the performance of the Planning Coordinator's portion of the existing system in a planning power flow model to actual system behavior, represented by a state estimator case or other Real-time data sources, at least once every 24 calendar months through simulation;

1.2. Comparison of the performance of the Planning Coordinator's portion of the existing system in a planning dynamic model to actual system response, through simulation of a dynamic local event, at least once every 24 calendar months (use a dynamic local event that occurs within 24 calendar months of the last dynamic local event used in comparison, and complete each comparison within 24 calendar months of the dynamic local event). If no dynamic local event occurs within the 24 calendar months, use the next dynamic local event that occurs;

1.3. Guidelines the Planning Coordinator will use to determine unacceptable differences in performance under Part 1.1 or 1.2; and

1.4. Guidelines to resolve the unacceptable differences in performance identified under Part 1.3.

M1. Each Planning Coordinator shall provide evidence that it has a documented validation process according to Requirement R1 as well as evidence that demonstrates the implementation of the required components of the process.

R2. Each Reliability Coordinator and Transmission Operator shall provide actual system behavior data (or a written response that it does not have the requested data) to any Planning Coordinator performing validation under Requirement R1 within 30 calendar days of a written request, such as, but not limited to, state estimator case or other Real-time data (including disturbance data recordings) necessary for actual system response validation. *[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*

M2. Each Reliability Coordinator and Transmission Operator shall provide evidence, such as email notices or postal receipts showing recipient and date that it has distributed the requested data or written response that it does not have the data, to any Planning Coordinator performing validation under Requirement R1 within 30 days of a written request in accordance with Requirement R2; or a statement by the Reliability Coordinator or Transmission Operator that it has not received notification regarding data necessary for validation by any Planning Coordinator.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

"Compliance Enforcement Authority" means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The applicable entity shall keep data or evidence to show compliance with Requirements R1 through R2, and Measures M1 through M2, since the last audit, unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

If an applicable entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved, or for the time specified above, whichever is longer.

The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

Refer to Section 3.0 of Appendix 4C of the NERC Rules of Procedure for a list of compliance monitoring and assessment processes.

1.4. Additional Compliance Information

None

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	Long-term Planning	Medium	The Planning Coordinator documented and implemented a process to validate data but did not address one of the four required topics under Requirement R1; OR The Planning Coordinator did not perform simulation as required by part 1.1 within 24 calendar months but did perform the simulation within 28 calendar months; OR The Planning Coordinator did not perform simulation as	The Planning Coordinator documented and implemented a process to validate data but did not address two of the four required topics under Requirement R1; OR The Planning Coordinator did not perform simulation as required by part 1.1 within 24 calendar months but did perform the simulation in greater than 28 calendar months but less than or equal to 32 calendar months; OR	The Planning Coordinator documented and implemented a process to validate data but did not address three of the four required topics under Requirement R1; OR The Planning Coordinator did not perform simulation as required by part 1.1 within 24 calendar months but did perform the simulation in greater than 32 calendar months but less than or equal to 36 calendar months; OR	The Planning Coordinator did not have a validation process at all or did not document or implement any of the four required topics under Requirement R1; OR The Planning Coordinator did not validate its portion of the system in the power flow model as required by part 1.1 within 36 calendar months; OR The Planning Coordinator did not perform simulation as required by part 1.2 within 36 calendar

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			required by part 1.2 within 24 calendar months (or the next dynamic local event in cases where there is more than 24 months between events) but did perform the simulation within 28 calendar months.	The Planning Coordinator did not perform simulation as required by part 1.2 within 24 calendar months (or the next dynamic local event in cases where there is more than 24 months between events) but did perform the simulation in greater than 28 calendar months but less than or equal to 32 calendar months.	The Planning Coordinator did not perform simulation as required by part 1.2 within 24 calendar months (or the next dynamic local event in cases where there is more than 24 months between events) but did perform the simulation in greater than 32 calendar months but less than or equal to 36 calendar months.	months (or the next dynamic local event in cases where there is more than 24 months between events).
R2	**Long-term Planning**	**Lower**	The Reliability Coordinator or Transmission Operator did not provide requested actual system behavior data (or a written response that it does not have the requested data) to a requesting Planning	The Reliability Coordinator or Transmission Operator did not provide requested actual system behavior data (or a written response that it does not have the requested data) to a requesting Planning	The Reliability Coordinator or Transmission Operator did not provide requested actual system behavior data (or a written response that it does not have the requested data) to a requesting Planning	The Reliability Coordinator or Transmission Operator did not provide requested actual system behavior data (or a written response that it does not have the requested data) to a requesting Planning

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Coordinator within 30 calendar days of the written request, but did provide the data (or written response that it does not have the requested data) in less than or equal to 45 calendar days.	Coordinator within 30 calendar days of the written request, but did provide the data (or written response that it does not have the requested data) in greater than 45 calendar days but less than or equal to 60 calendar days.	Coordinator within 30 calendar days of the written request, but did provide the data (or written response that it does not have the requested data) in greater than 60 calendar days but less than or equal to 75 calendar days.	Coordinator within 75 calendar days; OR The Reliability Coordinator or Transmission Operator provided a written response that it does not have the requested data, but actually had the data.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Requirement R1:

The requirement focuses on the results-based outcome of developing a process for and performing a validation, but does not prescribe a specific method or procedure for the validation outside of the attributes specified in the requirement. For further information on suggested validation procedures, see "Procedures for Validation of Powerflow and Dynamics Cases" produced by the NERC Model Working Group.

The specific process is left to the judgment of the Planning Coordinator, but the Planning Coordinator is required to develop and include in its process guidelines for evaluating discrepancies between actual system behavior or response and expected system performance for determining whether the discrepancies are unacceptable.

For the validation in part 1.1, the state estimator case or other Real-time data should be taken as close to system peak as possible. However, other snapshots of the system could be used if deemed to be more appropriate by the Planning Coordinator. While the requirement specifies "once every 24 calendar months," entities are encouraged to perform the comparison on a more frequent basis.

In performing the comparison required in part 1.1, the Planning Coordinator may consider, among other criteria:

1. System load;
2. Transmission topology and parameters;
3. Voltage at major buses; and
4. Flows on major transmission elements.

The validation in part 1.1 would include consideration of the load distribution and load power factors (as applicable) used in the power flow models. The validation may be made using metered load data if state estimator cases are not available. The comparison of system load distribution and load power factors shall be made on an aggregate company or power flow zone level at a minimum but may also be made on a bus by bus, load pocket (e.g., within a Balancing Authority), or smaller area basis as deemed appropriate by the Planning Coordinator.

The scope of dynamics model validation is intended to be limited, for purposes of part 1.2, to the Planning Coordinator's planning area, and the intended emphasis under the requirement is on local events or local phenomena, not the whole Interconnection.

The validation required in part 1.2 may include simulations that are to be compared with actual system data and may include comparisons of:

- Voltage oscillations at major buses
- System frequency (for events with frequency excursions)
- Real and reactive power oscillations on generating units and major inter-area ties

Determining when a dynamic local event might occur may be unpredictable, and because of the analytic complexities involved in simulation, the time parameters in part 1.2 specify that the comparison period of "at least once every 24 calendar months" is intended to both provide for at least 24 months between dynamic local events used in the comparisons and that comparisons must be completed within 24 months of the date of the dynamic local event used. This clarification ensures that PCs will not face a timing scenario that makes it impossible to comply. If the time referred to the completion time of the comparison, it would be possible for an event to occur in month 23 since the last comparison, leaving only one month to complete the comparison. With the 30 day timeframe in Requirement R2 for TOPs or RCs to provide actual system behavior data (if necessary in the comparison), it would potentially be impossible to complete the comparison within the 24 month timeframe.

In contrast, the requirement language clarifies that the time frame between dynamic local events used in the comparisons should be within 24 months of each other (or, as specified at the end of part 1.2, in the event more than 24 months passes before the next dynamic local event, the comparison should use the next dynamic local event that occurs). Each comparison must be completed within 24 months of the dynamic local event used. In this manner, the potential problem with a "month 23" dynamic local event described above is resolved. For example, if a PC uses for comparison a dynamic local event occurring on day 1 of month 1, the PC has 24 calendar months from that dynamic local event's occurrence to complete the comparison. If the next dynamic event the PC chooses for comparison occurs in month 23, the PC has 24 months from that dynamic local event's occurrence to complete the comparison.

Part 1.3 requires the PC to include guidelines in its documented validation process for determining when discrepancies in the comparison of simulation results with actual system results are unacceptable. The PC may develop the guidelines required by parts 1.3 and 1.4 itself, reference other established guidelines, or both. For the power flow comparison, as an example, this could include a guideline the Planning Coordinator will use that flows on 500 kV lines should be within 10% or 100 MW, whichever is larger. It could be different percentages or MW amounts for different voltage levels. Or, as another example, the guideline for voltage comparisons could be that it must be within 1%. But the guidelines the PC includes within its documented validation process should be meaningful for the Planning Coordinator's system. Guidelines for the dynamic event comparison may be less precise. Regardless, the comparison should indicate that the conclusions drawn from the two results should be consistent. For example, the guideline could state that the simulation result will be plotted on the same graph as the actual system response. Then the two plots could be given a visual inspection to see if they look similar or not. Or a guideline could be defined such that the rise time of the transient response in the simulation should be within 20% of the rise time of the actual system response. As for the power flow guidelines, the dynamic comparison criteria should be meaningful for the Planning Coordinator's system.

The guidelines the PC includes in its documented validation process to resolve differences in Part 1.4 could include direct coordination with the data owner, and, if necessary, through the provisions of MOD-032-1, Requirement R3 (i.e., the validation performed under this requirement could identify technical concerns with the data). In other words, while this standard is focused on validation, results of the validation may identify data provided under the

modeling data standard that needs to be corrected. If a model with estimated data or a generic model is used for a generator, and the model response does not match the actual response, then the estimated data should be corrected or a more detailed model should be requested from the data provider.

While the validation is focused on the Planning Coordinator's planning area, the model for the validation should be one that contains a wider area of the Interconnection than the Planning Coordinator's area. If the simulations can be made to match the actual system responses by reasonable changes to the data in the Planning Coordinator's area, then the Planning Coordinator should make those changes in coordination with the data provider. However, for some disturbances, the data in the Planning Coordinator's area may not be what is causing the simulations to not match actual responses. These situations should be reported to the Electric Reliability Organization (ERO). The guidelines the Planning Coordinator includes under Part 1.4 could cover these situations.

Rationale:

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for R1:

In FERC Order No. 693, paragraph 1210, the Commission directed inclusion of "a requirement that the models be validated against actual system responses." Furthermore, the Commission directs in paragraph 1211, "that actual system events be simulated and if the model output is not within the accuracy required, the model shall be modified to achieve the necessary accuracy." Paragraph 1220 similarly directs validation against actual system responses relative to dynamics system models. In FERC Order 890, paragraph 290, the Commission states that "the models should be updated and benchmarked to actual events." Requirement R1 addresses these directives.

Requirement R1 requires the Planning Coordinator to implement a documented data validation process to validate data in the Planning Coordinator's portion of the existing system in the steady-state and dynamic models to compare performance against expected behavior or response, which is consistent with the Commission directives. The validation of the full Interconnection-wide cases is left up to the Electric Reliability Organization (ERO) or its designees, and is not addressed by this standard. The following items were chosen for the validation requirement:

A. Comparison of performance of the existing system in a planning power flow model to actual system behavior; and

B. Comparison of the performance of the existing system in a planning dynamics model to actual system response.

Implementation of these validations will result in more accurate power flow and dynamic models. This, in turn, should result in better correlation between system flows and voltages

seen in power flow studies and the actual values seen by system operators during outage conditions. Similar improvements should be expected for dynamics studies, such that the results will more closely match the actual responses of the power system to disturbances.

Validation of model data is a good utility practice, but it does not easily lend itself to Reliability Standards requirement language. Furthermore, it is challenging to determine specifications for thresholds of disturbances that should be validated and how they are determined. Therefore, this requirement focuses on the Planning Coordinator performing validation pursuant to its process, which must include the attributes listed in parts 1.1 through 1.4, without specifying the details of "how" it must validate, which is necessarily dependent upon facts and circumstances. Other validations are best left to guidance rather than standard requirements.

Rationale for R2:
The Planning Coordinator will need actual system behavior data in order to perform the validations required in R1. The Reliability Coordinator or Transmission Operator may have this data. Requirement R2 requires the Reliability Coordinator and Transmission Operator to supply actual system data, if it has the data, to any requesting Planning Coordinator for purposes of model validation under Requirement R1.

This could also include information the Reliability Coordinator or Transmission Operator has at a field site. For example, if a PMU or DFR is at a generator site and it is recording the disturbance, the Reliability Coordinator or Transmission Operator would typically have that data.

Version History

Version	Date	Action	Change Tracking
1	February 6, 2014	Adopted by the NERC Board of Trustees.	Developed as a new standard for system validation to address outstanding directives from FERC Order No. 693 and recommendations from several other sources.
1	May 1, 2014	FERC Order issued approving MOD-033-1.	
2	February 6, 2020	Adopted by the NERC Board of Trustees.	Revisions under Project 2017-07
2	October 30, 2020	FERC Order approving MOD-033-2. Docket No. RD20-4-000	

2	April 1, 2021	Effective Date	

Appendix MOD-033-2-QC-1
Specific provisions applicable in Québec for standard
MOD-033-2 — Steady-State and Dynamic System Model Validation

This appendix establishes specific provisions for the application of the standard in Québec. Provisions of the standard and of this appendix must be read jointly comprehension and interpretation purposes. Where the standard and appendix differ, the appendix shall prevail.

A. Introduction

1. Title: No specific provision

2. Number: No specific provision

3. Purpose: No specific provision

4. Applicability:

4.1. Functional entities

No specific provision

5. Effective Date:

5.1. Adoption of the standard by the Régie de l'énergie: June 28, 2022

5.2. Adoption of this appendix by the Régie de l'énergie: June 28, 2022

5.3. Effective date of the standard and its appendix in Québec: October 1, 2022

B. Requirements and Measures

No specific provision

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

In Québec, "Compliance Enforcement Authority" means the Régie de l'énergie in its roles of monitoring and enforcing compliance with respect to the Reliability Standard and to this appendix.

1.2. Evidence Retention

No specific provision

1.3. Compliance Monitoring and Assessment Processes

The Régie de l'énergie establishes the monitoring processes used to evaluate data or information for the purpose of determining compliance or non-compliance with the Reliability Standard and with this appendix.

1.4. Additional Compliance Information

No specific provision

Table of Compliance Elements

No specific provision

D. Regional Variances

No specific provision

E. Interpretations

No specific provision

F. Associated Documents

No specific provision

Guidelines and Technical Basis

No specific provision

Version history

Version	Date	Action	Change Tracking
1	June 28, 2022	New appendix as per decision D-2022-085	New

A. Introduction

1. **Title:** **Operating Personnel Credentials**

2. **Number:** **PER-003-2**

3. **Purpose:** To ensure that System Operators performing the reliability-related tasks of the Reliability Coordinator, Balancing Authority and Transmission Operator are certified through the NERC System Operator Certification Program when filling a Real-time operating position responsible for control of the Bulk Electric System.

4. **Applicability:**

   4.1. Functional Entities:

   4.1.1. Reliability Coordinator

   4.1.2. Transmission Operator

   4.1.3. Balancing Authority

5. **Effective Date:** See Implementation Plan for standard PER-003-2.

B. Requirements and Measures

R1. Each Reliability Coordinator shall staff its Real-time operating positions performing Reliability Coordinator reliability-related tasks with System Operators who have demonstrated minimum competency in the areas listed by obtaining and maintaining a valid NERC Reliability Operator certificate [(1)(2)]: *[Risk Factor: High][Time Horizon: Real-time Operations]*

1.1. Areas of Competency

1.1.1. Resource and demand balancing

1.1.2. Transmission operations

1.1.3. Emergency preparedness and operations

1.1.4. System operations

1.1.5. Protection and control

1.1.6. Voltage and reactive

1.1.7. Interchange scheduling and coordination

1.1.8. Interconnection reliability operations and coordination

---

[1] Non-NERC certified personnel performing any reliability-related task of a real-time operating position must be under the direct supervision of a NERC Certified System Operator stationed at that operating position; the NERC Certified System Operator at that operating position has ultimate responsibility for the performance of the reliability-related tasks.

[2] The NERC certificates referenced in this standard pertain to those certificates identified in the NERC System Operator Certification Program Manual.

M1. Each Reliability Coordinator shall have the following evidence to show that it staffed its Real-time operating positions performing reliability-related tasks with System Operators who have demonstrated the applicable minimum competency by obtaining and maintaining the appropriate, valid NERC certificate:

M1.1 A list of Real-time operating positions.

M1.2 A list of System Operators assigned to its Real-time operating positions.

M1.3 A copy of each of its System Operator's NERC certificate or NERC certificate number with expiration date which demonstrates compliance with the applicable Areas of Competency.

M1.4 Work schedules, work logs, or other equivalent evidence showing which System Operators were assigned to work in Real-time operating positions.

R2. Each Transmission Operator shall staff its Real-time operating positions performing Transmission Operator reliability-related tasks with System Operators who have demonstrated minimum competency in the areas listed by obtaining and maintaining one of the following valid NERC certificates [(1)][(2)]: *[Risk Factor: High][Time Horizon: Real-time Operations]*:

2.1. Areas of Competency

2.1.1. Transmission operations

2.1.2. Emergency preparedness and operations

2.1.3. System operations

2.1.4. Protection and control

2.1.5. Voltage and reactive

2.2. Certificates

- Reliability Operator
- Balancing, Interchange and Transmission Operator
- Transmission Operator

M2. Each Transmission Operator shall have the following evidence to show that it staffed its Real-time operating positions performing reliability-related tasks with System Operators who have demonstrated the applicable minimum competency by obtaining and maintaining the appropriate, valid NERC certificate:

---

[1] Non-NERC certified personnel performing any reliability-related task of a real-time operating position must be under the direct supervision of a NERC Certified System Operator stationed at that operating position; the NERC Certified System Operator at that operating position has ultimate responsibility for the performance of the reliability-related tasks.

[2] The NERC certificates referenced in this standard pertain to those certificates identified in the NERC System Operator Certification Program Manual.

M2.1 A list of Real-time operating positions.

M2.2 A list of System Operators assigned to its Real-time operating positions.

M2.3 A copy of each of its System Operator's NERC certificate or NERC certificate number with expiration date which demonstrates compliance with the applicable Areas of Competency.

M2.4 Work schedules, work logs, or other equivalent evidence showing which System Operators were assigned to work in Real-time operating positions.

R3. Each Balancing Authority shall staff its Real-time operating positions performing Balancing Authority reliability-related tasks with System Operators who have demonstrated minimum competency in the areas listed by obtaining and maintaining one of the following valid NERC certificates [(1)(2)]: *[Risk Factor: High][Time Horizon: Real-time Operations]*:

3.1. Areas of Competency

3.1.1. Resources and demand balancing

3.1.2. Emergency preparedness and operations

3.1.3. System operations

3.1.4. Interchange scheduling and coordination

3.2. Certificates

- Reliability Operator
- Balancing, Interchange and Transmission Operator
- Balancing and Interchange Operator

M3. Each Balancing Authority shall have the following evidence to show that it staffed its Real-time operating positions performing reliability-related tasks with System Operators who have demonstrated the applicable minimum competency by obtaining and maintaining the appropriate, valid NERC certificate:

M3.1 A list of Real-time operating positions.

M3.2 A list of System Operators assigned to its Real-time operating positions.

M3.3 A copy of each of its System Operator's NERC certificate or NERC certificate number with expiration date which demonstrates compliance with the applicable Areas of Competency.

---

[1] Non-NERC certified personnel performing any reliability-related task of a real-time operating position must be under the direct supervision of a NERC Certified System Operator stationed at that operating position; the NERC Certified System Operator at that operating position has ultimate responsibility for the performance of the reliability-related tasks.

[2] The NERC certificates referenced in this standard pertain to those certificates identified in the NERC System Operator Certification Program Manual.

M3.4 Work schedules, work logs, or other equivalent evidence showing which System Operators were assigned to work in Real-time operating positions.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority:
"Compliance Enforcement Authority" means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention:
The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

- Each Reliability Coordinator, Transmission Operator and Balancing Authority shall keep data or evidence for three years or since its last compliance audit, whichever time frame is the greatest.

1.3. Compliance Monitoring and Enforcement Program
As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	N/A	N/A	N/A	The Reliability Coordinator failed to staff each Real-time operating position performing Reliability Coordinator reliability-related tasks with a System Operator having a valid NERC certificate as defined in Requirement R1.
R2.	N/A	N/A	N/A	The Transmission Operator failed to staff each Real-time operating position performing Transmission Operator reliability-related tasks with a System Operator having a valid NERC certificate as defined in Requirement R2, Part 2.2.
R3.	N/A	N/A	N/A	The Balancing Authority failed to staff each Real-time operating position performing Balancing Authority reliability-related tasks with a System Operator having a valid NERC certificate as defined in Requirement R3, Part 3.2.

D. Regional Variances

None.

E. Associated Documents

Implementation Plan

Version History

Version	Date	Action	Change Tracking
0	April 1, 2005	Effective Date	New
1	February 17, 2011	Complete revision under Project 2007-04	Revision
1	February 17, 2011	Adopted by Board of Trustees	
1	September 15, 2011	FERC Order issued by FERC approving PER-003-1 (effective date of the Order is September 15, 2011)	
2	May 10, 2018	Added footnote to requirements	Revision
2	May 10, 2018	Adopted by Board of Trustees	Revision
2	November 21, 2018	FERC Letter Order approving PER-003-2. Docket No. RD18-9-000	

Appendix PER-003-2-QC-1

Specific provisions applicable in Québec for standard PER-003-2 – Operating Personnel Credentials

This appendix establishes specific provisions for the application of the standard in Québec. Provisions of the standard and of this appendix must be read jointly for comprehension and interpretation purposes. Where the standard and appendix differ, the appendix shall prevail.

A. Introduction

1. Title: No specific provisions.

2. Number: No specific provisions.

3. Purpose: No specific provisions.

4. Applicability:

4.1. Functional entities

No specific provisions.

5. Effective dates for Québec:

5.1. Adoption of the standard by the Régie de l'énergie: May 28, 2021

5.2. Adoption of the appendix by the Régie de l'énergie: May 28, 2021

5.3. Effective date of the standard and appendix for Québec: July 1st, 2021

B. Requirements and measures

No specific provisions.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

In Québec, "Compliance Enforcement Authority" means the Régie de l'énergie in its roles of monitoring and enforcing compliance with respect to the Reliability Standard and to this appendix.

1.2. Evidence Retention

No specific provisions.

1.3. Compliance Monitoring and Enforcement Program

The Régie de l'énergie establishes the monitoring processes used to evaluate data or information for the purpose of determining compliance or non-compliance with the Reliability Standard and with this appendix.

2. Violation Severity Levels

No specific provisions.

D. Regional Variances

No specific provisions.

E. Associated Documents

No specific provisions.

Version history

Version	Date	Action	Change tracking
1	May 28, 2021	New appendix as per decision D-2021-070 and D-2021-070R.	New

A. Introduction

1. **Title:** **Operations Personnel Training**

2. **Number:** PER-005-2

3. **Purpose:** To ensure that personnel performing or supporting Real-time operations on the Bulk Electric System are trained using a systematic approach.

4. **Applicability:**

   4.1. Functional Entities:

   4.1.1 Reliability Coordinator

   4.1.2 Balancing Authority

   4.1.3 Transmission Operator

   4.1.4 Transmission Owner that has:

   4.1.4.1 Personnel, excluding field switching personnel, who can act independently to operate or direct the operation of the Transmission Owner's Bulk Electric System transmission Facilities in Real-time.

   4.1.5 Generator Operator that has:

   4.1.5.1 Dispatch personnel at a centrally located dispatch center who receive direction from the Generator Operator's Reliability Coordinator, Balancing Authority, Transmission Operator, or Transmission Owner, and may develop specific dispatch instructions for plant operators under their control. These personnel do not include plant operators located at a generator plant site or personnel at a centrally located dispatch center who relay dispatch instructions without making any modifications.

5. **Effective Date:**

   5.1. This standard shall become effective the first day of the first calendar quarter that is 24 months beyond the date that this standard is approved by an applicable governmental authority or is otherwise provided for in a jurisdiction where approval by an applicable authority is required for a standard to go into effect.

   Where approval by an applicable governmental authority is not required, this standard shall become effective on the first day of the first calendar quarter that is 24 months after the date the standard is adopted by the NERC Board of Trustees or as otherwise provided for in that jurisdiction.

B. Requirements and Measures

R1. Each Reliability Coordinator, Balancing Authority, and Transmission Operator shall use a systematic approach to develop and implement a training program for its System Operators as follows: *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

1.1. Each Reliability Coordinator, Balancing Authority, and Transmission Operator shall create a list of Bulk Electric System (BES) company-specific Real-time reliability-related tasks based on a defined and documented methodology.

1.1.1. Each Reliability Coordinator, Balancing Authority, and Transmission Operator shall review, and update if necessary, its list of BES company-specific Real-time reliability-related tasks identified in part 1.1 each calendar year.

1.2. Each Reliability Coordinator, Balancing Authority, and Transmission Operator shall design and develop training materials according to its training program, based on the BES company-specific Real-time reliability-related task list created in part 1.1.

1.3. Each Reliability Coordinator, Balancing Authority, and Transmission Operator shall deliver training to its System Operators according to its training program.

1.4. Each Reliability Coordinator, Balancing Authority, and Transmission Operator shall conduct an evaluation each calendar year of the training program established in Requirement R1 to identify any needed changes to the training program and shall implement the changes identified.

M1. Each Reliability Coordinator, Balancing Authority, and Transmission Operator shall have available for inspection evidence of using a systematic approach to develop and implement a training program for its System Operators, as specified in Requirement R1.

M1.1 Each Reliability Coordinator, Balancing Authority, and Transmission Operator shall have available for inspection its methodology and its BES company-specific Real-time reliability-related task list, with the date of the last review, as specified in Requirement R1 part 1.1 and part 1.1.1.

M1.2 Each Reliability Coordinator, Balancing Authority, and Transmission Operator shall have available for inspection training materials, as specified in Requirement R1 part 1.2.

M1.3 Each Reliability Coordinator, Balancing Authority, and Transmission Operator shall have available for inspection System Operator training records showing the names of the people trained, the title of the training delivered, and the dates of delivery to show that it delivered the training, as specified in Requirement R1 part 1.3.

M1.4 Each Reliability Coordinator, Balancing Authority, and Transmission Operator shall have available for inspection evidence (such as instructor observations, trainee feedback, supervisor feedback, course evaluations, learning assessments, or internal audit results) that it performed an evaluation of its training program each calendar year, as specified in Requirement R1 part 1.4.

R2. Each Transmission Owner shall use a systematic approach to develop and implement a training program for its personnel identified in Applicability Section 4.1.4.1 of this standard as follows: *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

2.1. Each Transmission Owner shall create a list of BES company-specific Real-time reliability-related tasks based on a defined and documented methodology.

2.1.1. Each Transmission Owner shall review, and update if necessary, its list of BES company-specific Real-time reliability-related tasks identified in part 2.1 each calendar year.

2.2. Each Transmission Owner shall design and develop training materials according to its training program, based on the BES company-specific Real-time reliability-related task list created in part 2.1.

2.3. Each Transmission Owner shall deliver training to its personnel identified in Applicability Section 4.1.4.1 of this standard according to its training program.

2.4. Each Transmission Owner shall conduct an evaluation each calendar year of the training program established in Requirement R2 to identify any needed changes to the training program and shall implement the changes identified.

M2. Each Transmission Owner shall have available for inspection evidence of using a systematic approach to develop and implement a training program for its applicable personnel, as specified in Requirement R2.

M2.1 Each Transmission Owner shall have available for inspection its methodology and its BES company-specific Real-time reliability-related task list, with the date of the last review, as specified in Requirement R2 part 2.1.

M2.2 Each Transmission Owner shall have available for inspection training materials, as specified in Requirement R2 part 2.2.

M2.3 Each Transmission Owner shall have available for inspection training records showing the names of the people trained, the title of the training delivered, and the dates of delivery to show that it delivered the training, as specified in Requirement R2 part 2.3.

M2.4 Each Transmission Owner shall have available for inspection evidence (such as instructor observations, trainee feedback, supervisor feedback, course evaluations, learning assessments, or internal audit results) that it performed an evaluation of its training program each calendar year, as specified in Requirement R2 part 2.4.

R3. Each Reliability Coordinator, Balancing Authority, Transmission Operator, and Transmission Owner shall verify, at least once, the capabilities of its personnel, identified in Requirement R1 or Requirement R2, assigned to perform each of the BES company-specific Real-time reliability-related tasks identified under Requirement R1 part 1.1 or Requirement R2 part 2.1. *[Violation Risk Factor: High] [Time Horizon: Long-term Planning]*

3.1. Within six months of a modification or addition of a BES company-specific Real-time reliability-related task, each Reliability Coordinator, Balancing Authority, Transmission Operator, and Transmission Owner shall verify the capabilities of each of its personnel identified in Requirement R1 or Requirement R2 to perform the new or modified BES company-specific Real-time reliability-related tasks identified in Requirement R1 part 1.1 or Requirement R2 part 2.1.

M3. Each Reliability Coordinator, Balancing Authority, Transmission Operator, and Transmission Owner shall have available for inspection evidence to show that it verified the capabilities of each of its personnel, identified in Requirement R1 or Requirement R2, assigned to perform each of the BES company-specific Real-time reliability-related tasks identified under Requirement R1 part 1.1 or Requirement R2 part 2.1. This evidence may be documents such as records showing capability to perform BES company-specific Real-time reliability-related tasks with the employee name and date; supervisor check sheets showing the employee name, date, and BES company-specific Real-time reliability-related task completed; or the results of learning assessments.

M3.1 Each Reliability Coordinator, Balancing Authority, Transmission Operator, or Transmission Owner shall present evidence that it verified the capabilities of applicable personnel to perform new or modified BES company-specific Real-time reliability-related tasks within 6 months of a modification or addition of a BES company-specific Real-time reliability-related task.

R4. Each Reliability Coordinator, Balancing Authority, Transmission Operator, and Transmission Owner that (1) has operational authority or control over Facilities with established Interconnection Reliability Operating Limits (IROLs), or (2) has established protection systems or operating guides to mitigate IROL violations, shall provide its personnel identified in Requirement R1 or Requirement R2 with emergency operations training using simulation technology such as a simulator, virtual technology, or other technology that replicates the operational behavior of the BES. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

4.1. A Reliability Coordinator, Balancing Authority, Transmission Operator, or Transmission Owner that did not previously meet the criteria of Requirement R4, shall comply with Requirement R4 within 12 months of meeting the criteria.

M4. Each Reliability Coordinator, Balancing Authority, Transmission Operator, and Transmission Owner shall have available for inspection training records that provide evidence that personnel identified in Requirement R1 or Requirement R2 completed

training that includes the use of simulation technology, as specified in Requirement R4.

M4.1 Each Reliability Coordinator, Balancing Authority, Transmission Operator, and Transmission Owner shall have available for inspection training records that provide evidence that personnel identified in Requirement R1 or Requirement R2 completed training that included the use of simulation technology, as specified in Requirement R4, within 12 months of meeting the criteria of Requirement R4.

R5. Each Reliability Coordinator, Balancing Authority, and Transmission Operator shall use a systematic approach to develop and implement training for its identified Operations Support Personnel on how their job function(s) impact those BES company-specific Real-time reliability-related tasks identified by the entity pursuant to Requirement R1 part 1.1. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

5.1 Each Reliability Coordinator, Balancing Authority, and Transmission Operator shall conduct an evaluation each calendar year of the training established in Requirement R5 to identify and implement changes to the training.

M5. Each Reliability Coordinator, Balancing Authority, and Transmission Operator shall have available for inspection evidence that Operations Support Personnel completed training in accordance with its systematic approach. This evidence may be documents such as training records showing successful completion of training. Documentation of training shall include employee name and date of training.

M5.1 Each Reliability Coordinator, Balancing Authority, and Transmission Operator shall have available for inspection evidence (such as instructor observations, trainee feedback, supervisor feedback, course evaluations, learning assessments, or internal audit results) that it performed an evaluation each calendar year, as specified in Requirement R5 part 5.1.

R6. Each Generator Operator shall use a systematic approach to develop and implement training to its personnel identified in Applicability Section 4.1.5.1 of this standard, on how their job function(s) impact the reliable operations of the BES during normal and emergency operations. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

6.1. Each Generator Operator shall conduct an evaluation each calendar year of the training established in Requirement R6 to identify and implement changes to the training.

M6. Each Generator Operator shall have available for inspection evidence that its applicable personnel completed training in accordance with its systematic approach. This evidence may be documents such as training records showing successful completion of training. Documentation of training shall include employee name and date of training.

M6.1 Each Generator Operator shall have available for inspection evidence (such as instructor observations, trainee feedback, supervisor feedback, course evaluations, learning assessments, or internal audit results) that it performed an evaluation each calendar year, as specified in Requirement R6 part 6.1.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the compliance enforcement authority may ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

Each Reliability Coordinator, Balancing Authority, Transmission Operator Transmission Owner, and Generator Operator shall keep data or evidence to show compliance for three years or since its last compliance audit, whichever time frame is greater, unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

If a Reliability Coordinator, Balancing Authority, Transmission Operator Transmission Owner, or Generator Operator is found non-compliant, it shall keep information related to the non-compliance until found compliant.

The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audit

Self-Certification

Spot Checking

Compliance Investigation

Self-Reporting

Complaint

1.4. Additional Compliance Information

None

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Long-term Planning**	**Medium**	**None**	The Reliability Coordinator, Balancing Authority, or Transmission Operator failed to review or update, if necessary, its BES company-specific Real-time reliability-related task list each calendar year. (1.1.1.) OR The Reliability Coordinator, Balancing Authority, or Transmission Operator, failed to evaluate its training program each calendar year to identify needed changes to its training program(s). (1.4) OR The Reliability Coordinator, Balancing Authority, or Transmission Operator, failed to implement the identified changes to the training program(s). (1.4.)	The Reliability Coordinator, Balancing Authority, or Transmission Operator failed to use a systematic approach to develop and implement a training program. (R1) OR The Reliability Coordinator, Balancing Authority, or Transmission Operator failed to design and develop training materials based on the BES company-specific Real-time reliability-related task lists. (1.2)	The Reliability Coordinator, Balancing Authority, or Transmission Operator failed to create a BES company-specific Real-time reliability-related task list. (1.1.) OR The Reliability Coordinator, Balancing Authority, or Transmission Operator failed to deliver training based on the BES company-specific Real-time reliability-related task lists. (1.3)
R2	**Long-term Planning**	**Medium**	**None**	The Transmission Owner failed to review or update, if necessary, its company-specific Real-time reliability-	The Transmission Owner failed to use a systematic approach to develop and implement a training program. (R2)	The Transmission Owner failed to create a BES company-specific Real-time reliability-related task list. (2.1.) OR

				related task list each calendar year. (2.1.1.) OR The Transmission Owner failed to evaluate its training program each calendar year to identify needed changes to its training program(s). (2.4) OR The Transmission Owner failed to implement the identified changes to the training program(s). (2.4.)	OR The Transmission Owner failed to design and develop training materials based on the BES company-specific Real-time reliability-related task lists. (2.2)	The Transmission Owner failed to deliver training based on the BES company-specific Real-time reliability-related task lists. (2.3)
R3	**Long-term Planning**	**High**	**None**	The Reliability Coordinator, Balancing Authority, Transmission Operator, or Transmission Owner verified the capabilities of at least 90% but less than 100% of its personnel identified in Requirements R1 or Requirement R2 to perform all of their assigned BES company-specific Real-time reliability-related tasks. (R3)	The Reliability Coordinator, Balancing Authority, Transmission Operator, or Transmission Owner verified the capabilities of at least 70% but less than 90% of its personnel identified in Requirements R1 or Requirement R2 to perform all of their assigned BES company-specific Real-time reliability-related tasks. (R3) OR The Reliability Coordinator, Balancing Authority, Transmission Operator, or Transmission Owner failed to verify the capabilities of its personnel identified in Requirements R1 or Requirement	The Reliability Coordinator, Balancing Authority, Transmission Operator, or Transmission Owner verified the capabilities of less than 70% of its personnel identified in Requirements R1 or Requirement R2 to perform all of their assigned BES company-specific Real-time reliability-related tasks. (R3)

					R2 to perform each new or modified task within six months of making a modification to its BES company-specific Real-time reliability-related task list. (3.1)	
R4	**Long-term Planning**	**Medium**	**None**	**None**	**None**	The Reliability Coordinator, Balancing Authority, Transmission Operator, or Transmission Owner that meet the criteria of Requirement R4 did not provide its personnel identified in Requirement R1 or Requirement R2 with emergency operations training using simulation technology such as a simulator, virtual technology, or other technology that replicates the operational behavior of the BES. (R4) OR The Reliability Coordinator, Balancing Authority, Transmission Operator, or Transmission Owner did not provide its personnel identified in Requirement R1 or Requirement R2 with emergency operations training using simulation technology such as a simulator, virtual technology, or other technology that replicates the operational behavior of the BES within twelve months of meeting the criteria of Requirement R4. (R4.1)

R5	**Long-term Planning**	**Medium**	**None**	The Reliability Coordinator, Balancing Authority, or Transmission Operator failed to evaluate its training established in Requirement R5 each calendar year. (5.1)	The Reliability Coordinator, Balancing Authority, or Transmission Operator failed to develop training for its Operations Support Personnel. (R5) OR The Reliability Coordinator, Balancing Authority, or Transmission Operator developed training but failed to use a systematic approach. (R5)	The Reliability Coordinator, Balancing Authority, or Transmission Operator failed to implement training for its Operations Support Personnel. (R5)
R6	**Long-term Planning**	**Medium**	**None**	The Generator Operator failed to evaluate its training established in Requirement R6 each calendar year. (6.1)	The Generator Operator failed to develop training for its personnel. (R6) OR The Generator Operator developed training but failed to use a systematic approach. (R6)	The Generator Operator failed to implement the training for its personnel identified in Requirement R6. (R6)

Guidelines and Technical Basis

Requirement R1 and R2:

Any systematic approach to training will determine: 1) the skills and knowledge needed to perform BES company-specific Real-time reliability-related tasks; 2) what training is needed to achieve those skills and knowledge; 3) if the learner can perform the BES company-specific Real-time reliability-related task(s) acceptably in either a training or on-the-job environment; and 4) if the training is effective, and make adjustments as necessary.

Reference #1: Determining Task Performance Requirements

The purpose of this reference is to provide guidance for a performance standard that describes the desired outcome of a task. A standard for acceptable performance should be in either measurable or observable terms. Clear standards of performance are necessary for an individual to know when he or she has completed the task and to ensure agreement between employees and their supervisors on the objective of a task. Performance standards answer the following questions:

How timely must the task be performed?

Or

How accurately must the task be performed?

Or

With what quality must it be performed?

Or

What response from the customer must be accomplished?

When a performance standard is quantifiable, successful performance is more easily demonstrated. For example, in the following task statement, the criteria for successful performance is to return system loading to within normal operating limits, which is a number that can be easily verified.

> Given a System Operating Limit violation on the transmission system, implement the correct procedure for the circumstances to mitigate loading to within normal operating limits.

Even when the outcome of a task cannot be measured as a number, it may still be observable. The next example contains performance criteria that is qualitative in nature, that is, it can be verified as either correct or not, but does not involve a numerical result.

> Given a tag submitted for scheduling, ensure that all transmission rights are assigned to the tag per the company Tariff and in compliance with NERC and NAESB standards.

Reference #2: Systematic Approach to Training References:
The following list of hyperlinks identifies references for the NERC Standard PER-005 to assist with the application of a systematic approach to training:

(1) DOE-HDBK-1078-94, A Systematic Approach to Training

http://www.publicpower.org/files/PDFs/DOEHandbookTrainingProgramSystematicApproach.pdf

(2) DOE-HDBK-1074-95, January 1995, Alternative Systematic Approaches to Training, U.S. Department of Energy, Washington, D.C. 20585 FSC 6910

http://www.catagle.com/112-1/download_php-spec_DOE-HDBK-1074-95_003254_1.htm

(3) ADDIE – 1975, Florida State University

http://www.nwlink.com/~donclark/history_isd/addie.html

(4) DOE Standard - Table-Top Needs Analysis
DOE-HDBK-1103-96

http://energy.gov/sites/prod/files/2013/06/f2/hdbk1103.pdf

Reference #3: Recognized Operator Training Topics
See Appendix A – Recognized Operator Training Topics within the NERC System Operator Certification Program Manual.
http://www.nerc.com/pa/Train/SysOpCert/Documents/SOC_Program_Manual_February_2012_Final.pdf

Reference #4: Definitions of Simulation and Simulators

Georgia Institute of Technology – Modeling & Simulation for Systems Engineering
http://www.pe.gatech.edu/conted/servlet/edu.gatech.conted.course.ViewCourseDetails?COURSE_ID=840

University of Central Florida – Institute for Simulation & Training
Just what is "simulation" anyway (or, Simulation 101)?
And what about "modeling"?
But what does IST do with simulations?
http://www.ist.ucf.edu/overview.htm

Rationale:

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for System Operator:

The definition of the existing NERC Glossary Term “System Operator" has been modified to remove Generator Operator (GOP) in response to Project 2010-16.

The term “System Operator” contains another NERC Glossary term “Control Center”, which was approved by FERC on November 22, 2013. The inclusion of GOPs within the approved definition of Control Center does not bring GOPs into the System Operator definition. The System Operator definition specifies that it only applies to Balancing Authority (BA), Transmission Operator (TOP) or Reliability Coordinator (RC) personnel.

The modifications to the definition of “System Operator” do not affect other standards; see the PER-005-2 White Paper, which cross checks System Operator with other NERC Standards.

Rationale for Operations Support Personnel:

The term Operations Support Personnel is used to identify those support personnel of Reliability Coordinators (RC), Balancing Authorities (BA), or Transmission Operators (TOP) that FERC identified in Order No. 693.

Rationale for TO:

Extending the applicability to TOs is necessary to address the FERC directive that the ERO develop formal training requirements for local transmission control center operator personnel. In Order No. 742 at P 62, the Commission clarified its understanding that local control center personnel *“exercise control over a significant portion of the Bulk-Power System under the supervision of the personnel of the registered transmission operator. The supervision may take the form of directive specific step-by-step instructions and at other times may take the form of the implementation of predefined operating procedures. In all cases, the Commission continued, the local transmission control center personnel must understand what they are required to do in the performance of their duties to perform them effectively on a timely basis. Thus, omitting such local transmission control center personnel from the PER-005-1 training requirements creates a reliability gap.”* See FERC Order 693 at P 1343 and 1347.

Rationale for GOP:

Extending the applicability to Generator Operators (GOPs) that have dispatch personnel at a centrally located dispatch center is necessary to address the FERC directive that the ERO develop specific requirements addressing the scope, content and duration appropriate for certain GOP personnel. The Commission explains in Order No. 693 at P 1359 that “*although a generator operator typically receives instructions from a balancing authority, it is essential that generator operator personnel have appropriate training to understand those instructions,*

particularly in an emergency situation in which instructions may be succinct and require immediate action." Order No. 742 further clarified that the directive "*applies to generator operator personnel at a centrally-located dispatch center who receive direction and then develop specific dispatch instructions for plant operators under their control. Plant operators located at the generator plant site are not required to be trained in PER-005-2."* Based on the FERC order, this applicability section clarifies which GOP personnel are subject to the standard.

Rationale for changes to R2:

Transmission Owners personnel at local transmission control centers have been added to the PER standard and are subject to Requirements R2, R3 and R4 of PER-005-2. The reason for adding Transmission Owners is to address Order No. 693 and Order No. 742 FERC directives to include local transmission control center operator personnel.

Rationale for R3:

This Requirement was brought forward from the previous version with the addition of Transmission Owners. It provides an entity with an opportunity to create a baseline from which to assess training needs as it develops a systematic approach.

Rationale for changes to R4:

The requirement mandates the use of specific training technologies. It does not require training on Interconnection Reliability Operating Limits (IROLs). The standard allows entities that gain operational authority or control over a Facility with IROLs or established protection systems or operating guides to mitigate IROL violations within 12 months to comply with Requirement R4 to provide them sufficient time to obtain simulation technology.

The requirement to provide a minimum of 32 hours of Emergency Operations training has been removed since the appropriate number of hours would be identified as part of the systematic approach in Requirement R1 and Requirement R2 through the analysis phase and outlined in a continuous education section of their training program. Any additional hours may be duplicative or repetitive for the entity in providing training to its personnel. Requirement R4.1 covers the FERC directive for the creation of an implementation plan for simulation technology.

Rationale for R5:

This is a new requirement applicable to Operations Support Personnel. In FERC Order No. 742, the Commission noted that NERC, in developing Reliability Standard PER-005-1, did not comply with the directive in FERC Order No. 693 to expand the applicability of training requirements to include operations planning and operation support staff who carry out outage planning and assessments and those who develop System Operating Limits (SOL), Interconnection Reliability Operating Limits (IROL), or operating nomograms for Real-time operations. This requirement contemplates that entities will look to the systematic approach already developed under Requirement R1. The entity can use the list created from Requirement R1 and select the BES company-specific Real-time reliability-related tasks with which Operations Support Personnel are involved.

Application Guidelines

Rationale for R6:

This requirement requires the training of certain GOP dispatch personnel on how their job function(s) impact the reliable operations of the BES during normal and emergency operations. This requirement mandates the use of a systematic approach which allows for each entity to tailor its training to the needs of its organization.

This is a new requirement applicable to certain GOPs as described in the applicability section. In FERC Order No. 742, the Commission noted that in developing proposed Reliability Standard PER-005-1, NERC did not comply with the directive in FERC Order No. 693 to expand the applicability of training requirements to include GOPs centrally-located at a generation dispatch center with a direct impact on the reliable operation of the BES. The Commission acknowledged that the training for GOPs need not be as extensive as the training for TOPs and BAs. FERC also stated that the systematic approach to training methodology is flexible enough to build on existing training programs by validating and supplementing the existing training content, where necessary, using systematic methods.

Version History

Version	Date	Action	Change Tracking
1	2/10/2009	Adopted by the NERC Board of Trustees	
1	11/18/2010	FERC Approved	
1	8/26/2013	Updated VSLs based on June 24, 2013 approval.	
2	2/6/2014	Adopted by the NERC Board of Trustees	
2	6/19/2014	FERC Approved	

Appendix QC-PER-005-2
Provisions specific to the standard PER-005-2 applicable in Québec

This appendix establishes specific provisions for the application of the standard in Québec. Provisions of the standard and of its appendix must be read together for the purposes of understanding and interpretation. Where the standard and appendix differ, the appendix shall prevail.

A. Introduction

1. **Title:** Operations Personnel Training

2. **Number:** PER-005-2

3. **Purpose:** No specific provision

4. **Applicability:**

   Functional Entities

   No specific provision

   Facilities

   In the application of this standard, all references to the terms "Bulk Electric System" or "BES" shall be replaced by the terms "Main Transmission System" or "RTP" respectively.

5. **Effective Date:**

   5.1. Adoption of the standard by the Régie de l'énergie: December 22, 2016

   5.2. Adoption of the appendix by the Régie de l'énergie: December 22, 2016

   5.3. Effective date of the standard and its appendix in Québec: July 1, 2018

B. Requirements and Measures

No specific provision

C. Compliance

1. **Compliance Monitoring Process**

   1.1. Compliance Enforcement Authority

   The Régie de l'énergie is responsible, in Québec, for compliance enforcement with respect to the reliability standard and its appendix that it adopts.

   1.2. Evidence Retention

   No specific provision

   1.3. Compliance Monitoring and Assessment Processes

   No specific provision

   1.4. Additional Compliance Information

   No specific provision

Appendix QC-PER-005-2
Provisions specific to the standard PER-005-2 applicable in Québec

Table of Compliance Elements

No specific provision

D. Regional Variances

No specific provision

E. Interpretations

No specific provision

F. Associated Documents

No specific provision

Guidelines and Technical Basis

No specific provision

Revision History

Revision	Adoption Date	Action	Change Tracking
0	December 22, 2016	New appendix	New

A. Introduction

1. **Title:** **Specific Training for Personnel**

2. **Number:** **PER-006-1**

3. **Purpose:** To ensure that personnel are trained on specific topics essential to reliability to perform or support Real-time operations of the Bulk Electric System.

4. **Applicability:**

   4.1. Functional Entities:

   4.1.1. Generator Operator that has:

   4.1.1.1. Plant personnel who are responsible for the Real-time control of a generator and receive Operating Instruction(s) from the Generator Operator's Reliability Coordinator, Balancing Authority, Transmission Operator, or centrally located dispatch center.

5. **Effective Date:** See Implementation Plan for Project 2007-06.2.

B. Requirements and Measures

R1. Each Generator Operator shall provide training to personnel identified in Applicability section 4.1.1.1. on the operational functionality of Protection Systems and Remedial Action Schemes (RAS) that affect the output of the generating Facility(ies) it operates. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

M1. Each Generator Operator shall have available for inspection, evidence that the applicable personnel completed training. This evidence may be documents such as training records showing successful completion of training that includes training materials, the name of the person, and date of training.

C. Compliance

1. **Compliance Monitoring Process**

   1.1. Compliance Enforcement Authority:

   "Compliance Enforcement Authority" means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

   1.2. Evidence Retention:

   The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last

audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

- The Generator Operator shall keep data or evidence of Requirement R1 for the current year and three previous calendar years.

1.3. Compliance Monitoring and Enforcement Program

As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	The Generator Operator failed to provide training as described in Requirement R1 to the greater of: • one applicable personnel at a single Facility, or • 5% or less of the total applicable personnel of the Generator Operator.	The Generator Operator failed to provide training as described in Requirement R1 to the greater of: • two applicable personnel at a single Facility, or • more than 5% and less than or equal to 10% of the total applicable personnel of the Generator Operator.	The Generator Operator failed to provide training as described in Requirement R1 to the greater of: • three applicable personnel at a single Facility, or • more than 10% and less than or equal to 15% of the total applicable personnel of the Generator Operator.	The Generator Operator failed to provide training as described in Requirement R1 to the greater of: • five or more applicable personnel at a single Facility, or • more than 15% of the total applicable personnel of the Generator Operator. **OR** The Generator Operator failed to provide training as described in Requirement R1 to its applicable personnel.

D. Regional Variances

None.

E. Associated Documents

Project 2007-06.2 Implementation Plan[1]

[1] http://www.nerc.com/pa/Stand/Project200706_2SystemProtectionCoordinationDL/Project_2007_06_2_Imp_Plan_Draft_1_2016_03_10_Clean.pdf

Version History

Version	Date	Action	Change Tracking
1	August 11, 2016	Adopted by the NERC Board of Trustees	New standard developed under Project 2007-06.2
1	June 7, 2018	FERC Order issued approving PER-006-1. Docket No. RM16-22-000.	
1	August 13,2018	FERC Approved	
1	October 1, 2020	Effective Date	Effective dates delayed to April 1, 2021 due to COVID-19 per FERC Order
1	April 1, 2021	Effective Date	

Guidelines and Technical Basis

Requirement R1

The Generator Operator (GOP) monitors and controls its generating Facilities in Real-time to maintain reliability. To accomplish this, applicable plant personnel responsible for Real-time control of a generating Facility must be trained on how the operational functionality of Protection Systems and Remedial Action Schemes (RAS) are applied and the affects they may have on a generating Facility. Although, training does not have to be Facility-specific, the standard applies to plant operating personnel associated with the specific Facility to which they have Real-time control. This does not include plant personnel not responsible for Real-time control (e.g., fuel or coal handlers, electricians, machinists, or maintenance staff).

A periodicity for training is not specified in Requirement R1 because the GOP must ensure its plant personnel who have Real-time control of a generator are trained. The Generator Operator must also ensure it provides applicable training that results from changes to the operational functionality of the Protection Systems and Remedial Action Schemes that affect the output of the generation Facility(ies).

The phrase “operational functionality” focuses the training on how Protection Systems operate and prevent possible damage to Elements. It also addresses how RAS detects pre-determined BES conditions and automatically takes corrective actions.

Considerations for operational functionality may include, but are not limited to the following:

- Purpose of protective relays and RAS
- Zones of protection
- Protection communication systems (e.g., line current differential, direct transfer trip, etc.)
- Voltage and current inputs
- Station dc supply associated with protective functions
- Resulting actions – tripping/closing of breakers; tripping of a generator step-up (GSU) transformer; or generator ramping/tripping control functions

Requirement R1 focuses on the operational functionality of Protection Systems and Remedial Action Schemes specific to the generating plant and not the Bulk Electric System.

This requirement focuses on those systems that are related to the electrical output of the generator. Protective systems which trip breakers serving station auxiliary loads (e.g., such as pumps, fans, or fuel handling equipment) are not included in the scope of this training. Furthermore, protection of secondary unit substation (SUS) or low voltage switchgear transformers and relays protecting other downstream plant electrical distribution system components are not in the scope of this training, even if a trip of these devices might eventually result in a trip of the generating unit.

Rationale

Rationale for Requirement R1: Protection Systems and Remedial Action Schemes (RAS) are an integral part of reliable Bulk Electric System (BES) operation. This requirement addresses the reliability objective of ensuring that Generator Operator (GOP) plant operating personnel understand the operational functionality of Protection Systems and RAS and their effects on generating Facilities.

Appendix PER-006-1-QC-1

Specific provisions applicable in Québec for standard PER-006-1 – Specific Training for Personnel

This appendix establishes specific provisions for the application of the standard in Québec. Provisions of the standard and of this appendix must be read jointly for comprehension and interpretation purposes. Where the standard and appendix differ, the appendix shall prevail.

A. Introduction

1. **Title:** No specific provisions.

2. **Number:** No specific provisions.

3. **Purpose:** No specific provisions.

4. **Applicability:**

   4.1. Functional Entities

   No specific provisions in regard to applicable entities.

   The Facilities subject to this standard are the Facilities of the Main Transmission System (RTP).

5. **Effective dates for Québec:**

   5.1. Adoption of the standard by the Régie de l'énergie: May 28, 2021

   5.2. Adoption of the appendix by the Régie de l'énergie: May 28, 2021

   5.3. Effective date of the standard and appendix for Québec: July 1st, 2023

B. Requirements and measures

No specific provisions.

C. Compliance

1. **Compliance Monitoring Process**

   1.1. Compliance Enforcement Authority

   In Québec, "Compliance Enforcement Authority" means the Régie de l'énergie in its roles of monitoring and enforcing compliance with respect to the Reliability Standard and to this appendix.

   1.2. Evidence Retention

   No specific provisions.

   1.3. Compliance Monitoring and Enforcement Program

   The Régie de l'énergie establishes the monitoring processes used to evaluate data or information for the purpose of determining compliance or non-compliance with the Reliability Standard and with this appendix.

2. **Violation Severity Levels**

   No specific provisions.

D. Regional Variances

No specific provisions.

E. Associated Documents

No specific provisions.

Guidelines and Technical Basis

In the application of this standard, all references to the terms "Bulk Electric System" or "BES" shall be replaced by the terms "Main Transmission System" or "RTP" respectively.

Rationale

In the application of this standard, all references to the terms "Bulk Electric System" or "BES" shall be replaced by the terms "Main Transmission System" or "RTP" respectively.

Version history

Version	Date	Action	Change tracking
1	May 28, 2021	New appendix as per decision D-2021-070 and D-2021-070R.	New

A. Introduction

1. **Title:** Disturbance Monitoring and Reporting Requirements
2. **Number:** PRC-002-5
3. **Purpose:** To have adequate data available to facilitate analysis of Bulk Electric System (BES) Disturbances.
4. **Applicability:**
   - **4.1. Functional Entities:**
     - **4.1.1.** Reliability Coordinator
     - **4.1.2.** Transmission Owner
     - **4.1.3.** Generator Owner
   - **4.2. Facilities:** BES Elements, excluding Inverter-Based Resources.[1]
5. **Effective Date:** See Implementation Plan

[1] Disturbance monitoring and reporting requirements for Inverter-Based Resources are addressed in PRC-028.

B. Requirements and Measures

R1. Each Transmission Owner shall: *[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*

1.1. Identify BES buses for which sequence of events recording (SER) and fault recording (FR) data is required by using the methodology in PRC-002-5, Attachment 1.

1.2. Notify the other owners of BES Elements directly connected[2] to those BES buses, that SER or FR data is required for those BES Elements, only if the Transmission Owner who identified the BES buses in Part 1.1 does not have SER or FR data. This notification is required within 90 calendar days of completion of Part 1.1.

1.3. Re-evaluate all BES buses at least once every five calendar years in accordance with Part 1.1 and notify other owners in accordance with Part 1.2.

M1. The Transmission Owner for Requirement R1, Part 1.1 has a dated (electronic or hard copy) list of BES buses for which SER and FR data is required, identified in accordance with PRC-002-5, Attachment 1; has dated (electronic or hard copy) evidence that it notified other owners in accordance with Requirement R1, Part 1.2; and evidence that all BES buses have been re-evaluated within the required intervals under Requirement R1, Part 1.3.

R2. Each Transmission Owner and Generator Owner shall have SER data for circuit breaker position (open/close) for each circuit breaker it owns directly connected to the BES buses identified in Requirement R1 and associated with the BES Elements at those BES buses. *[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*

M2. The Transmission Owner or Generator Owner has evidence (electronic or hard copy) of SER data for circuit breaker position as specified in Requirement R2. Evidence may include, but is not limited to: (1) documents describing the device interconnections and configurations which may include a single design standard as representative for common installations; or (2) actual data recordings; or (3) station drawings.

R3. Each Transmission Owner and Generator Owner shall have FR data to determine the following electrical quantities for each triggered FR for the BES Elements it owns directly connected to the BES buses identified in Requirement R1: *[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*

3.1. Phase-to-neutral voltage for each phase of each specified BES bus.

3.2. Each phase current and the residual or neutral current for the following BES Elements:

3.2.1. Transformers that have a low-side operating voltage of 100 kV or above.

[2] For the purposes of this standard, "directly connected" BES Elements are BES Elements connected at the same voltage level within the same physical location sharing a common ground grid with the BES bus identified under Attachment 1. Transformers that have a low-side operating voltage of less than 100 kV are excluded.

3.2.2. Transmission Lines.

M3. The Transmission Owner or Generator Owner has evidence (electronic or hard copy) of FR data that is sufficient to determine electrical quantities as specified in Requirement R3. Evidence may include, but is not limited to: (1) documents describing the device specifications and configurations which may include a single design standard as representative for common installations; or (2) actual data recordings or derivations; or (3) station drawings.

R4. Each Transmission Owner and Generator Owner shall have FR data as specified in Requirement R3 that meets the following: *[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*

4.1. A single record or multiple records that include:

- A pre-trigger record length of at least two cycles and a total record length of at least 30 cycles for the same trigger point, or
- At least two cycles of the pre-trigger data, the first three cycles of the post-trigger data, and the final cycle of the fault as seen by the fault recorder.

4.2. A minimum recording rate of 16 samples per cycle.

4.3. Trigger settings for at least the following:

4.3.1. Neutral (residual) overcurrent.

4.3.2. Phase undervoltage or overcurrent.

M4. The Transmission Owner or Generator Owner has evidence (electronic or hard copy) that FR data meets Requirement R4. Evidence may include, but is not limited to: (1) documents describing the device specification (R4, Part 4.2) and device configuration or settings (R4, Parts 4.1 and 4.3), or (2) actual data recordings or derivations.

R5. Each Reliability Coordinator shall: *[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*

5.1. Identify BES Elements for which dynamic Disturbance recording (DDR) data is required, including the following:

5.1.1. Synchronous generating resource(s) with:

5.1.1.1. Gross individual nameplate rating greater than or equal to 500 MVA.

5.1.1.2. Gross individual nameplate rating greater than or equal to 300 MVA where the gross plant/facility aggregate nameplate rating is greater than or equal to 1,000 MVA.

5.1.2. Any one BES Element that is part of a stability (angular or voltage) related System Operating Limit (SOL).

5.1.3. Each terminal of a high voltage direct current (HVDC) circuit with a nameplate rating greater than or equal to 300 MVA, on the alternating current (AC) portion of the converter.

5.1.4. One or more BES Elements that are part of an Interconnection Reliability Operating Limit (IROL).

5.1.5. Any one BES Element within a major voltage sensitive area as defined by an area with an in-service undervoltage load shedding (UVLS) program.

5.2. Identify a minimum DDR coverage, inclusive of those BES Elements identified in Part 5.1, of at least:

5.2.1. One BES Element; and

5.2.2. One BES Element per 3,000 MW of the Reliability Coordinator's historical simultaneous peak System Demand.

5.3. Notify all owners of identified BES Elements, within 90 calendar days of completion of Part 5.1, that their respective BES Elements require DDR data.

5.4. Re-evaluate all BES Elements within its Reliability Coordinator Area at least once every five calendar years in accordance with Parts 5.1 and 5.2, and notify owners in accordance with Part 5.3.

M5. The Reliability Coordinator has a dated (electronic or hard copy) list of BES Elements for which DDR data is required, developed in accordance with Requirement R5, Part 5.1 and Part 5.2; and re-evaluated in accordance with Part 5.4. The Reliability Coordinator has dated evidence (electronic or hard copy) that each Transmission Owner or Generator Owner has been notified in accordance with Requirement 5, Part 5.3. Evidence may include, but is not limited to letters, emails, electronic files, or hard copy records demonstrating transmittal of information.

R6. Each Transmission Owner shall have DDR data to determine the following electrical quantities for each BES Element it owns for which it received notification as identified in Requirement R5: *[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*

6.1. One phase-to-neutral or positive sequence voltage.

6.2. The phase current for the same phase at the same voltage corresponding to the voltage in Requirement R6, Part 6.1, or the positive sequence current.

6.3. Real Power and Reactive Power flows expressed on a three-phase basis corresponding to all circuits where current measurements are required.

6.4. Frequency of any one of the voltage(s) in Requirement R6, Part 6.1.

M6. The Transmission Owner has evidence (electronic or hard copy) of DDR data to determine electrical quantities as specified in Requirement R6. Evidence may include, but is not limited to: (1) documents describing the device specifications and configurations, which may include a single design standard as representative for

common installations; or (2) actual data recordings or derivations; or (3) station drawings.

R7. Each Generator Owner shall have DDR data to determine the following electrical quantities for each BES Element it owns for which it received notification as identified in Requirement R5: *[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*

7.1. One phase-to-neutral, phase-to-phase, or positive sequence voltage at either the generator step-up transformer (GSU) high-side or low-side voltage level.

7.2. The phase current for the same phase at the same voltage corresponding to the voltage in Requirement R7, Part 7.1, phase current(s) for any phase-to-phase voltages, or positive sequence current.

7.3. Real Power and Reactive Power flows expressed on a three-phase basis corresponding to all circuits where current measurements are required.

7.4. Frequency of at least one of the voltages in Requirement R7, Part 7.1.

M7. The Generator Owner has evidence (electronic or hard copy) of DDR data to determine electrical quantities as specified in Requirement R7. Evidence may include, but is not limited to: (1) documents describing the device specifications and configurations, which may include a single design standard as representative for common installations; or (2) actual data recordings or derivations; or (3) station drawings.

R8. Each Transmission Owner and Generator Owner responsible for DDR data for the BES Elements identified in Requirement R5 shall have continuous data recording and storage. If the equipment was installed prior to the effective date of the Reliability Standard PRC-002-2[3] and is not capable of continuous recording, triggered records must meet the following: *[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*

8.1. Triggered record lengths of at least three minutes.

8.2. At least one of the following three triggers:

- Off nominal frequency trigger set at:

	Low	High
○ Eastern Interconnection	<59.75 Hz	>61.0 Hz
○ Western Interconnection	<59.55 Hz	>61.0 Hz
○ ERCOT Interconnection	<59.35 Hz	>61.0 Hz
○ Quebec Interconnection	<58.55 Hz	>61.5 Hz

- Rate of change of frequency trigger set at:

○ Eastern Interconnection	< -0.03125 Hz/sec	>0.125 Hz/sec

[3] The effective date of the Reliability Standard PRC-002-2 in the U.S. was July 1, 2016. The effective date may be different for other jurisdictions.

○ Western Interconnection	< -0.05625 Hz/sec	>0.125 Hz/sec
○ ERCOT Interconnection	< -0.08125 Hz/sec	>0.125 Hz/sec
○ Quebec Interconnection	< -0.18125 Hz/sec	>0.1875 Hz/sec

- Undervoltage trigger set no lower than 85 percent of normal operating voltage for a duration of 5 seconds.

M8. Each Transmission Owner and Generator Owner has dated evidence (electronic or hard copy) of data recordings and storage in accordance with Requirement R8. Evidence may include, but is not limited to: (1) documents describing the device specifications and configurations, which may include a single design standard as representative for common installations; or (2) actual data recordings.

R9. Each Transmission Owner and Generator Owner responsible for DDR data for the BES Elements identified in Requirement R5 shall have DDR data that meet the following: *[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*

9.1. Input sampling rate of at least 960 samples per second.

9.2. Output recording rate of electrical quantities of at least 30 times per second.

M9. The Transmission Owner or Generator Owner has evidence (electronic or hard copy) that DDR data meets Requirement R9. Evidence may include, but is not limited to: (1) documents describing the device specification, device configuration, or settings (R9, Part 9.1; R9, Part 9.2); or (2) actual data recordings (R9, Part 9.2).

R10. Each Transmission Owner and Generator Owner shall time synchronize all SER and FR data for the BES buses identified in Requirement R1 and DDR data for the BES Elements identified in Requirement R5 to meet the following: *[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*

10.1. Synchronization to Coordinated Universal Time (UTC) with or without a local time offset.

10.2. Synchronized device clock accuracy within ± 2 milliseconds of UTC.

M10. The Transmission Owner or Generator Owner has evidence (electronic or hard copy) of time synchronization described in Requirement R10. Evidence may include, but is not limited to: (1) documents describing the device specification, configuration, or setting; (2) time synchronization indication or status; or 3) station drawings.

R11. Each Transmission Owner and Generator Owner shall provide, upon request, all SER and FR data for the BES buses identified in Requirement R1 and DDR data for the BES Elements identified in Requirement R5 to the Reliability Coordinator, Regional Entity, or NERC in accordance with the following: *[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*

11.1. Data will be retrievable for the period of 10 calendar days, inclusive of the day the data was recorded.

11.2. Data subject to Part 11.1 will be provided within 30 calendar days of a request unless an extension is granted by the requestor.

11.3. SER data will be provided in ASCII Comma Separated Value (CSV) format following Attachment 2.

11.4. FR data will be provided either in CSV format with appropriate headers or in electronic files that are formatted in conformance with C37.111, IEEE Standard Common Format for Transient Data Exchange (COMTRADE), revision C37.111-1999 or later.

11.5. DDR data will be provided either in CSV format with appropriate headers or in electronic files that are formatted in conformance with C37.111, IEEE Standard Common Format for Transient Data Exchange (COMTRADE), revision C37.111-1999 or later.

11.6. Data files will be named in conformance with C37.232, IEEE Standard for Common Format for Naming Time Sequence Data Files (COMNAME), revision C37.232-2011 or later.

M11. The Transmission Owner or Generator Owner has evidence (electronic or hard copy) that data was submitted upon request in accordance with Requirement R11. Evidence may include, but is not limited to: (1) dated transmittals to the requesting entity with formatted records; (2) documents describing data storage capability, device specification, configuration, or settings; or (3) actual data recordings.

R12. Each Transmission Owner and Generator Owner shall, upon the discovery of a failure of the recording capability for the SER, FR or DDR data: *[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*

- Restore the recording capability within 90 calendar days, or
- Submit a Corrective Action Plan (CAP) to the Regional Entity within 90 calendar days and then implement it according to CAP timeline.

M12. The Transmission Owner or Generator Owner has dated evidence (electronic or hard copy) that meets Requirement R12. Evidence may include, but is not limited to: (1) dated reports of discovery of a failure, (2) documentation noting the date the data recording was restored, (3) SCADA records, or (4) dated CAP transmittals to the Regional Entity and evidence that it implemented the CAP.

R13. Each Transmission Owner and Generator Owner shall: *[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*

13.1. Within three (3) calendar years of completing a re-evaluation or receiving notification under Requirement R1, Part 1.3, have SER or FR data as applicable for BES Elements directly connected to the identified BES buses.

13.2. Within three (3) calendar years of receiving notification under Requirement R5, Part 5.4, have DDR data for BES Elements identified during the re-evaluation.

M13. The Transmission Owner or Generator Owner has dated evidence (electronic or hard copy) that meets Requirement R13. Evidence may include, but is not limited to: letters, emails, drawings, or settings files.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: "Compliance Enforcement Authority" means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Transmission Owner, Generator Owner, and Reliability Coordinator shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation:

The Transmission Owner shall retain evidence of Requirement R1, for five calendar years.

The Reliability Coordinator shall retain evidence of Requirement R5, for five calendar years.

The Transmission Owner shall retain evidence of Requirement R6, for three calendar years.

The Generator Owner shall retain evidence of Requirement R7, for three calendar years.

The Transmission Owner and Generator Owner shall retain evidence of Requirements R2, R3, R4, R8, R9, R10, R11, and R12, for three calendar years.

The Transmission Owner and Generator Owner as applicable shall retain evidence of Requirement R13, for five calendar years.

If a Transmission Owner, Generator Owner, or Reliability Coordinator is found non-compliant, it shall keep information related to the non-compliance until mitigation is completed and approved or for the time specified above, whichever is longer.

The Compliance Enforcement Authority shall keep the last audit records, and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers

to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	The Transmission Owner identified the BES buses as directed by Requirement R1, Part 1.1 or Part 1.3 for more than 80 percent, but less than 100 percent of the required BES buses that they own. OR The Transmission Owner evaluated the BES buses as directed by Requirement R1, Part 1.1 or Part 1.3, but was late by 30 calendar days or less. OR The Transmission Owner as directed by Requirement R1, Part 1.2 was late in notifying the other owners that their BES Elements require SER or FR data by 10 calendar days or less.	The Transmission Owner identified the BES buses as directed by Requirement R1, Part 1.1 or Part 1.3 for more than 70 percent, but less than or equal to 80 percent of the required BES buses that they own. OR The Transmission Owner evaluated the BES buses as directed by Requirement R1, Part 1.1 or Part 1.3, but was late by greater than 30 calendar days and less than or equal to 60 calendar days. OR The Transmission Owner as directed by Requirement R1, Part 1.2 was late in notifying the other owners that their BES Elements require SER or FR data by greater than 10 calendar	The Transmission Owner identified the BES buses as directed by Requirement R1, Part 1.1 or Part 1.3 for more than 60 percent, but less than or equal to 70 percent of the required BES buses that they own. OR The Transmission Owner evaluated the BES buses as directed by Requirement R1, Part 1.1 or Part 1.3, but was late by greater than 60 calendar days and less than or equal to 90 calendar days. OR The Transmission Owner as directed by Requirement R1, Part 1.2 was late in notifying the other owners that their BES Elements require SER or FR data by greater than	The Transmission Owner identified the BES buses as directed by Requirement R1, Part 1.1 or Part 1.3 for less than or equal to 60 percent of the required BES buses that they own. OR The Transmission Owner evaluated the BES buses as directed by Requirement R1, Part 1.1 or Part 1.3, but was late by greater than 90 calendar days. OR The Transmission Owner as directed by Requirement R1, Part 1.2 was late in notifying one or more other owners that their BES Elements require SER or FR data by greater than 30 calendar days.

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		days, but less than or equal to 20 calendar days.	20 calendar days, but less than or equal to 30 calendar days.	
R2	Each Transmission Owner or Generator Owner as directed by Requirement R2 had more than 80 percent, but less than 100 percent of the total SER data for circuit breaker position (open/close) for each of the circuit breakers at the BES buses identified in Requirement R1.	Each Transmission Owner or Generator Owner as directed by Requirement R2 had more than 70 percent, but less than or equal to 80 percent of the total SER data for circuit breaker position (open/close) for each of the circuit breakers at the BES buses identified in Requirement R1.	Each Transmission Owner or Generator Owner as directed by Requirement R2 had more than 60 percent but less than or equal to 70 percent of the total SER data for circuit breaker position (open/close) for each of the circuit breakers at the BES buses identified in Requirement R1.	Each Transmission Owner or Generator Owner as directed by Requirement R2 for less than or equal to 60 percent of the total SER data for circuit breaker position (open/close) for each of the circuit breakers at the BES buses identified in Requirement R1.
R3	The Transmission Owner or Generator Owner had FR data as directed by Requirement R3, Parts 3.1 and 3.2 that covers more than 80 percent, but less than 100 percent of the total required electrical quantities, which is the product of the total number of monitored BES	The Transmission Owner or Generator Owner had FR data as directed by Requirement R3, Parts 3.1 and 3.2 that covers more than 70 percent, but less than or equal to 80 percent of the total required electrical quantities, which is the product of the total number of monitored BES	The Transmission Owner or Generator Owner had FR data as directed by Requirement R3, Parts 3.1 and 3.2 that covers more than 60 percent, but less than or equal to 70 percent of the total required electrical quantities, which is the product of the total	The Transmission Owner or Generator Owner had FR data as directed by Requirement R3, Parts 3.1 and 3.2 that covers less than or equal to 60 percent of the total required electrical quantities, which is the product of the total number of monitored BES

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	Elements and the number of specified electrical quantities for each BES Element.	Elements and the number of specified electrical quantities for each BES Element.	number of monitored BES Elements and the number of specified electrical quantities for each BES Element.	Elements and the number of specified electrical quantities for each BES Element.
R4	The Transmission Owner or Generator Owner had FR data that meets more than 80 percent, but less than 100 percent of the total recording parameters as specified in Requirement R4.	The Transmission Owner or Generator Owner had FR data that meets more than 70 percent, but less than or equal to 80 percent of the total recording parameters as specified in Requirement R4.	The Transmission Owner or Generator Owner had FR data that meets more than 60 percent, but less than or equal to 70 percent of the total recording parameters as specified in Requirement R4.	The Transmission Owner or Generator Owner had FR data that meets less than or equal to 60 percent of the total recording parameters as specified in Requirement R4.
R5	The Reliability Coordinator identified the BES Elements for which DDR data is required as directed by Requirement R5 for more than 80 percent, but less than 100 percent of the required BES Elements included in Part 5.1. OR	The Reliability Coordinator identified the BES Elements for which DDR data is required as directed by Requirement R5 for more than 70 percent, but less than or equal to 80 percent of the required BES Elements included in Part 5.1. OR	The Reliability Coordinator identified the BES Elements for which DDR data is required as directed by Requirement R5 for more than 60 percent, but less than or equal to 70 percent of the required BES Elements included in Part 5.1. OR	The Reliability Coordinator identified the BES Elements for which DDR data is required as directed by Requirement R5 for less than or equal to 60 percent of the required BES Elements included in Part 5.1. OR

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	The Reliability Coordinator identified the BES Elements for DDR as directed by Requirement R5, Part 5.1 or Part 5.4, but was late by 30 calendar days or less. OR The Reliability Coordinator as directed by Requirement R5, Part 5.3 was late in notifying the owners that their BES Elements require DDR data by 10 calendar days or less.	The Reliability Coordinator identified the BES Elements for DDR as directed by Requirement R5, Part 5.1 or Part 5.4, but was late by greater than 30 calendar days and less than or equal to 60 calendar days. OR The Reliability Coordinator as directed by Requirement R5, Part 5.3 was late in notifying the owners that their BES Elements require DDR data by greater than 10 calendar days, but less than or equal to 20 calendar days.	The Reliability Coordinator identified the BES Elements for DDR as directed by Requirement R5, Part 5.1 or Part 5.4, but was late by greater than 60 calendar days and less than or equal to 90 calendar days. OR The Reliability Coordinator as directed by Requirement R5, Part 5.3 was late in notifying the owners that their BES Elements require DDR data by greater than 20 calendar days, but less than or equal to 30 calendar days.	The Reliability Coordinator identified the BES Elements for DDR as directed by Requirement R5, Part 5.1 or Part 5.4, but was late by greater than 90 calendar days. OR The Reliability Coordinator as directed by Requirement R5, Part 5.3 was late in notifying one or more owners that their BES Elements require DDR data by greater than 30 calendar days. OR The Reliability Coordinator failed to ensure a minimum DDR coverage per Part 5.2.
R6	The Transmission Owner had DDR data as directed by Requirement R6, Parts 6.1 through 6.4 that	The Transmission Owner had DDR data as directed by Requirement R6, Parts 6.1 through 6.4 for more	The Transmission Owner had DDR data as directed by Requirement R6, Parts 6.1 through 6.4 for more	The Transmission Owner had DDR data as directed by Requirement R6, Parts 6.1 through 6.4 for less

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	covered more than 80 percent, but less than 100 percent of the total required electrical quantities, which is the product of the total number of applicable BES Elements and the number of specified electrical quantities for each applicable BES Element.	than 70 percent, but less than or equal to 80 percent of the total required electrical quantities, which is the product of the total number of applicable BES Elements and the number of specified electrical quantities for each applicable BES Element.	than 60 percent, but less than or equal to 70 percent of the total required electrical quantities, which is the product of the total number of applicable BES Elements and the number of specified electrical quantities for each applicable BES Element.	than 60 percent of the total required electrical quantities, which is the product of the total number of applicable BES Elements and the number of specified electrical quantities for each applicable BES Element.
R7	The Generator Owner had DDR data as directed by Requirement R7, Parts 7.1 through 7.4 that covers more than 80 percent, but less than 100 percent of the total required electrical quantities, which is the product of the total number of applicable BES Elements and the number of specified electrical quantities for each applicable BES Element.	The Generator Owner had DDR data as directed by Requirement R7, Parts 7.1 through 7.4 for more than 70 percent, but less than or equal to 80 percent of the total required electrical quantities, which is the product of the total number of applicable BES Elements and the number of specified electrical quantities for each applicable BES Element.	The Generator Owner had DDR data as directed by Requirement R7, Parts 7.1 through 7.4 for more than 60 percent, but less than or equal to 70 percent of the total required electrical quantities, which is the product of the total number of applicable BES Elements and the number of specified electrical quantities for each applicable BES Element.	The Generator Owner had DDR data as directed by Requirement R7, Parts 7.1 through 7.4 for less than 60 percent of the total required electrical quantities, which is the product of the total number of applicable BES Elements and the number of specified electrical quantities for each applicable BES Element.

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R8	The Transmission Owner or Generator Owner had continuous or non-continuous DDR data, as directed in Requirement R8, for more than 80 percent, but less than 100 percent of the BES Elements they own as determined in Requirement R5.	The Transmission Owner or Generator Owner had continuous or non-continuous DDR data, as directed in Requirement R8, for more than 70 percent, but less than or equal to 80 percent of the BES Elements they own as determined in Requirement R5.	The Transmission Owner or Generator Owner had continuous or non-continuous DDR data, as directed in Requirement R8, for more than 60 percent, but less than or equal to 70 percent of the BES Elements they own as determined in Requirement R5.	The Transmission Owner or Generator Owner failed to have continuous or non-continuous DDR data, as directed in Requirement R8, for the BES Elements they own as determined in Requirement R5.
R9	The Transmission Owner or Generator Owner had DDR data that meets more than 80 percent, but less than 100 percent of the total recording properties as specified in Requirement R9.	The Transmission Owner or Generator Owner had DDR data that meets more than 70 percent, but less than or equal to 80 percent of the total recording properties as specified in Requirement R9.	The Transmission Owner or Generator Owner had DDR data that meets more than 60 percent, but less than or equal to 70 percent of the total recording properties as specified in Requirement R9.	The Transmission Owner or Generator Owner had DDR data that meets less than or equal to 60 percent of the total recording properties as specified in Requirement R9.
R10	The Transmission Owner or Generator Owner had time synchronization per Requirement R10, Parts 10.1 and 10.2 for SER, FR, and DDR data for more	The Transmission Owner or Generator Owner had time synchronization per Requirement R10, Parts 10.1 and 10.2 for SER, FR, and DDR data for more	The Transmission Owner or Generator Owner had time synchronization per Requirement R10, Parts 10.1 and 10.2 for SER, FR, and DDR data for more	The Transmission Owner or Generator Owner failed to have time synchronization per Requirement R10, Parts 10.1 and 10.2 for SER, FR,

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	than 90 percent, but less than 100 percent of the BES buses identified in Requirement R1 and BES Elements identified in Requirement R5 as directed by Requirement R10.	than 80 percent, but less than or equal to 90 percent of the BES buses identified in Requirement R1 and BES Elements identified in Requirement R5 as directed by Requirement R10.	than 70 percent, but less than or equal to 80 percent of the BES buses identified in Requirement R1 and BES Elements identified in Requirement R5 as directed by Requirement R10.	and DDR data for less than or equal to 70 percent of the BES buses identified in Requirement R1 and BES Elements identified in Requirement R5 as directed by Requirement R10.
R11	The Transmission Owner or Generator Owner as directed by Requirement R11, Part 11.2 provided the requested data more than one to 10 calendar days late. OR The Transmission Owner or Generator Owner as directed by Requirement R11 provided more than 90 percent, but less than 100 percent of the requested data. OR	The Transmission Owner or Generator Owner as directed by Requirement R11, Part 11.2 provided the requested data more than 11 to 20 calendar days late. OR The Transmission Owner or Generator Owner as directed by Requirement R11 provided more than 80 percent, but less than or equal to 90 percent of the requested data. OR The Transmission Owner or Generator Owner as	The Transmission Owner or Generator Owner as directed by Requirement R11, Part 11.2 provided the requested data more than 21 to 30 calendar days late. OR The Transmission Owner or Generator Owner as directed by Requirement R11 provided more than 70 percent, but less than or equal to 80 percent of the requested data. OR	The Transmission Owner or Generator Owner as directed by Requirement R11, Part 11.2 provided the requested data more than 30 calendar days late. OR The Transmission Owner or Generator Owner as directed by Requirement R11 failed to provide less than or equal to 70 percent of the requested data. OR The Transmission Owner or Generator Owner as

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	The Transmission Owner or Generator Owner as directed by Requirement R11, Parts 11.3 through 11.6 provided more than 90 percent of the data, but less than 100 percent of the data in the proper data format.	directed by Requirement R11, Parts 11.3 through 11.6 provided more than 80 percent of the data, but less than or equal to 90 percent of the data in the proper data format.	The Transmission Owner or Generator Owner as directed by Requirement R11, Parts 11.3 through 11.6 provided more than 70 percent of the data, but less than or equal to 80 percent of the data in the proper data format.	directed by Requirement R11, Parts 11.3 through 11.6 provided less than or equal to 70 percent of the data in the proper data format.
R12	The Transmission Owner or Generator Owner as directed by Requirement R12 reported a failure and provided a Corrective Action Plan to the Regional Entity more than 90 calendar days, but less than or equal to 100 calendar days after discovery of the failure.	The Transmission Owner or Generator Owner as directed by Requirement R12 reported a failure and provided a Corrective Action Plan to the Regional Entity more than 100 calendar days, but less than or equal to 110 calendar days after discovery of the failure.	The Transmission Owner or Generator Owner as directed by Requirement R12 reported a failure and provided a Corrective Action Plan to the Regional Entity more than 110 calendar days, but less than or equal to 120 calendar days after discovery of the failure. OR The Transmission Owner or Generator Owner as directed by Requirement R12 submitted a CAP to	The Transmission Owner or Generator Owner as directed by Requirement R12 failed to report a failure and provide a Corrective Action Plan to the Regional Entity more than 120 calendar days after discovery of the failure. OR Transmission Owner or Generator Owner as directed by Requirement R12 failed to restore the recording capability and

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			the Regional Entity but failed to implement it.	failed to submit a CAP to the Regional Entity.
R13		The Transmission Owner or Generator Owner had data, as applicable, for the BES buses identified during the re-evaluation per Requirement R1, Part 1.3 and was late by less than or equal to 6 months. OR The Transmission Owner or Generator Owner had data, as applicable, for the BES Elements identified during the re-evaluation per Requirement R5, Part 5.4 and was late by less than or equal to 6 months.	The Transmission Owner or Generator Owner had data, as applicable, for the BES buses identified during the re-evaluation per Requirement R1, Part 1.3 and was late by greater than 6 months but less than or equal to 12 months. OR The Transmission Owner or Generator Owner had data, as applicable, for the BES Elements identified during the re-evaluation per Requirement R5, Part 5.4 and was late by greater than 6 months but less than or equal to 12 months.	The Transmission Owner or Generator Owner had data, as applicable, for the BES buses identified during the re-evaluation per Requirement R1, Part 1.3 and was late by greater than 12 months. OR The Transmission Owner or Generator Owner had data, as applicable, for the BES Elements identified during the re-evaluation per Requirement R5, Part 5.4 and was late by greater than 12 months.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

NERC Reliability Standard PRC-002-5: Implementation Plan.

G. References

IEEE C37.111: Common format for transient data exchange (COMTRADE) for power Systems.

IEEE C37.232-2011, IEEE Standard for Common Format for Naming Time Sequence Data Files (COMNAME). Standard published 11/09/2011 by IEEE.

NERC Reliability Standard PRC-002-5: Technical Rationale.

NPCC SP6 Report Synchronized Event Data Reporting, revised March 31, 2005.

U.S.-Canada Power System Outage Task Force, Final Report on the August 14, 2003, Blackout in the United States and Canada: Causes and Recommendations (2004).

U.S.-Canada Power System Outage Task Force Interim Report: Causes of the August 14th Blackout in the United States and Canada (Nov. 2003).

Version History

Version	Date	Action	Change Tracking
0	February 8, 2005	Adopted by NERC Board of Trustees	New
1	August 2, 2006	Adopted by NERC Board of Trustees	Revised
2	November 13, 2014	Adopted by NERC Board of Trustees	Revised under Project 2007-11 and merged with PRC-018-1.
2	September 24, 2015	FERC approved PRC-005-4. Docket No. RM15-4-000; Order No. 814	
3	May 13, 2021	Adopted by NERC Board of Trustees	Revised
4	February 16, 2023	Adopted by NERC Board of Trustees	Revised under Project 2021-04
4	April 14, 2023	FERC Oder Approving PRC-002-4 Docket No. RD23-4-000.	
4	April 14, 2023	Effective Date	April 1, 2024
5	October 8, 2024	Adopted by NERC Board of Trustees	Revised under Project 2021-04
5	February 20, 2025	FERC approved PRC-002-5. Docket Nos. RD25-1-000 and RD25-2-000	

Attachment 1

Methodology for Selecting Buses for Capturing Sequence of Events Recording (SER) and Fault Recording (FR) Data

(Requirement R1)

To identify monitored Bulk Electric System (BES) buses for SER and FR data required by Requirement 1, each Transmission Owner shall follow sequentially, unless otherwise noted, the steps listed below:

Step 1. Determine a complete list of BES buses that it owns. Refer to section 4.2 Facilities for exclusion.

For the purposes of this standard, a single BES bus includes physical buses with breakers connected at the same voltage level within the same physical location sharing a common ground grid. These buses may be modeled or represented by a single node in fault studies. For example, ring bus or breaker-and-a-half bus configurations are considered to be a single bus.

Step 2. Reduce the list to those BES buses that have a maximum available calculated three-phase short circuit MVA of 1,500 MVA or greater. If there are no buses on the resulting list, proceed to Step 7.

Step 3. Determine the 11 BES buses on the list with the highest maximum available calculated three-phase short circuit MVA level. If the list has 11 or fewer buses, proceed to Step 7.

Step 4. Calculate the median MVA level of the 11 BES buses determined in Step 3.

Step 5. Multiply the median MVA level determined in Step 4 by 20 percent.

Step 6. Reduce the BES buses on the list to only those that have a maximum available calculated three-phase short circuit MVA higher than the greater of:

- 1,500 MVA or
- 20 percent of median MVA level determined in Step 5.

Step 7. <u>If there are no BES buses on the list:</u> the procedure is complete, and no FR and SER data will be required. Proceed to Step 9.

<u>If the list has 1 or more but less than or equal to 11 BES buses:</u> FR and SER data is required at the BES bus with the highest maximum available calculated three-phase short circuit MVA as determined in Step 3.

During re-evaluation per Requirement R1, Part 1.3, if the three-phase short circuit MVA of the newly identified BES bus is within 15% of the three-phase short circuit MVA of the currently applicable BES bus with SER and FR data then it is not necessary to change the applicable BES bus. Proceed to Step 9.

<u>If the list has more than 11 BES buses:</u> SER and FR data is required on at least the 10 percent of the BES buses determined in Step 6 with the highest maximum

available calculated three-phase short circuit MVA. Proceed to Step 8.

Step 8. SER and FR data is required at additional BES buses on the list determined in Step 6. The aggregate of the number of BES buses determined in Step 7 and this Step will be at least 20 percent of the BES buses determined in Step 6.

The additional BES buses are selected, at the Transmission Owner's discretion, to provide maximum wide-area coverage for SER and FR data. The following BES bus locations are recommended:

- Electrically distant buses or electrically distant from other Disturbance Monitoring Equipment (DME) devices.
- Voltage sensitive areas.
- Cohesive load and generation zones.
- BES buses with a relatively high number of incident Transmission circuits.
- BES buses with reactive power devices.
- Major Facilities interconnecting outside the Transmission Owner's area.

Step 9. The list of monitored BES buses for SER and FR data for Requirement R1 is the aggregate of the BES buses determined in Steps 7 and 8.

Attachment 2

Sequence of Events Recording (SER) Data Format

(Requirement R11, Part 11.3)

Date, Time, Local Time Code, Substation, Device, State[4]

08/27/13, 23:58:57.110, -5, Sub 1, Breaker 1, Close

08/27/13, 23:58:57.082, -5, Sub 2, Breaker 2, Close

08/27/13, 23:58:47.217, -5, Sub 1, Breaker 1, Open

08/27/13, 23:58:47.214, -5, Sub 2, Breaker 2, Open

[4] "OPEN" and "CLOSE" are used as examples. Other terminology such as TRIP, TRIP TO LOCKOUT, RECLOSE, etc. is also acceptable.

High Level Requirement Overview

Requirement	Entity	Identify BES Buses	Notification	SER	FR	5 Year Re-evaluation
R1	TO	X	X	X	X	X
R2	TO | GO			X		
R3	TO | GO				X	
R4	TO | GO				X	

Requirement	Entity	Identify BES Elements	Notification	DDR	5 Year Re-evaluation
R5	RC	X	X	X	X
R6	TO			X	
R7	GO			X	
R8	TO | GO			X	
R9	TO | GO			X	

Requirement	Entity	Time Synchronization	Provide SER, FR, DDR Data	SER, FR, DDR Availability
R10	TO | GO	X		
R11	TO | GO		X	
R12	TO | GO			X

Requirement	Entity	Implementation
R13	TO | GO	X

Appendix PRC-002-5-QC-1
Specific provisions applicable in Québec for standard PRC-002-5 – Disturbance Monitoring and Reporting Requirements

This appendix establishes specific provisions for the application of the standard in Québec. Provisions of the standard and of this appendix must be read jointly for comprehension and interpretation purposes. Where the standard and appendix differ, the appendix shall prevail.

A. Introduction

1. Title: No specific provisions.

2. Number: No specific provisions.

3. Purpose: No specific provisions.

4. Applicability: In the application of this standard, all reference to the term "Bulk Electric System" or "BES" shall be replaced by the terms "Main Transmission System" or "RTP" respectively.

The Facilities subject to this standard are the Facilities of the Main Transmission System (RTP).

4.1. Functional Entities:

No specific provisions.

4.2. Facilities:

No specific provisions.

5. Effective Date:

5.1. Adoption of the standard by the Régie de l'énergie: February 10, 2026

5.2. Adoption of the appendix by the Régie de l'énergie: February 10, 2026

5.3. Effective date of the standard and its appendix in Québec: July 1, 2026

B. Requirements and Measures

No specific provisions.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

In Québec, "Compliance Enforcement Authority" means the Régie de l'énergie in its roles of monitoring and enforcing compliance with respect to the Reliability Standard and to this appendix.

1.2. Evidence Retention

No specific provisions.

1.3. Compliance Monitoring and Enforcement Program

The Régie de l'énergie establishes the monitoring processes used to evaluate data or information for the purpose of determining compliance or non-compliance with the reliability standard and with this appendix.

Violation Severity Levels

No specific provisions.

D. Regional Variances

No specific provisions.

E. Interpretations

No specific provisions.

F. Associated Documents

No specific provisions.

G. References

No specific provisions.

Attachment 1

No specific provisions.

Attachment 2

No specific provisions.

High Level Requirement Overview

No specific provisions.

Version History

Version	Date	Action	Change Tracking
1	February 10, 2026	New Appendix as per decision D-2026-010.	New

A. Introduction

1. **Title:** Protection System Misoperation Identification and Correction

2. **Number:** PRC-004-6

3. **Purpose:** Identify and correct the causes of Misoperations of Protection Systems for Bulk Electric System (BES) Elements.

4. **Applicability:**

   4.1. Functional Entities:

   4.1.1 Transmission Owner

   4.1.2 Generator Owner

   4.1.3 Distribution Provider

   4.2. Facilities:

   4.2.1 Protection Systems for BES Elements, with the following exclusions:

   4.2.1.1 Non-protective functions that are embedded within a Protection System.

   4.2.1.2 Protective functions intended to operate as a control function during switching.[1]

   4.2.1.3 Special Protection Systems (SPS).

   4.2.1.4 Remedial Action Schemes (RAS).

   4.2.1.5 Protection Systems of individual dispersed power producing resources identified under Inclusion I4 of the BES definition where the Misoperations affected an aggregate nameplate rating of less than or equal to 75 MVA of BES Facilities.

   4.2.2 Underfrequency load shedding (UFLS) that is intended to trip one or more BES Elements.

   4.2.3 Undervoltage load shedding (UVLS) that is intended to trip one or more BES Elements.

5. **Effective Date:** See Implementation Plan.

[1] For additional information and examples, see the "Non-Protective Functions" and "Control Functions" sections in the Application Guidelines.

B. Requirements and Measures

R1. Each Transmission Owner, Generator Owner, and Distribution Provider that owns a BES interrupting device that operated under the circumstances in Parts 1.1 through 1.3 shall, within 120 calendar days of the BES interrupting device operation, identify whether its Protection System component(s) caused a Misoperation: *[Violation Risk Factor: High][Time Horizon: Operations Assessment, Operations Planning]*

1.1 The BES interrupting device operation was caused by a Protection System or by manual intervention in response to a Protection System failure to operate; and

1.2 The BES interrupting device owner owns all or part of the Composite Protection System; and

1.3 The BES interrupting device owner identified that its Protection System component(s) caused the BES interrupting device(s) operation or was caused by manual intervention in response to its Protection System failure to operate.

M1. Each Transmission Owner, Generator Owner, and Distribution Provider shall have dated evidence that demonstrates it identified the Misoperation of its Protection System component(s), if any, that meet the circumstances in Requirement R1, Parts 1.1, 1.2, and 1.3 within the allotted time period. Acceptable evidence for Requirement R1, including Parts 1.1, 1.2, and 1.3 may include, but is not limited to the following dated documentation (electronic or hardcopy format): reports, databases, spreadsheets, emails, facsimiles, lists, logs, records, declarations, analyses of sequence of events, relay targets, Disturbance Monitoring Equipment (DME) records, test results, or transmittals.

R2. Each Transmission Owner, Generator Owner, and Distribution Provider that owns a BES interrupting device that operated shall, within 120 calendar days of the BES interrupting device operation, provide notification as described in Parts 2.1 and 2.2. *[Violation Risk Factor: High][Time Horizon: Operations Assessment, Operations Planning]*

2.1 For a BES interrupting device operation by a Composite Protection System or by manual intervention in response to a Protection System failure to operate, notification of the operation shall be provided to the other owner(s) that share Misoperation identification responsibility for the Composite Protection System under the following circumstances:

2.1.1 The BES interrupting device owner shares the Composite Protection System ownership with any other owner; and

2.1.2 The BES interrupting device owner has determined that a Misoperation occurred or cannot rule out a Misoperation; and

2.1.3 The BES interrupting device owner has determined that its Protection System component(s) did not cause the BES interrupting device(s) operation or cannot determine whether its Protection System components caused the BES interrupting device(s) operation.

2.2 For a BES interrupting device operation by a Protection System component intended to operate as backup protection for a condition on another entity's BES Element, notification of the operation shall be provided to the other Protection System owner(s) for which that backup protection was provided.

M2. Each Transmission Owner, Generator Owner, and Distribution Provider shall have dated evidence that demonstrates notification to the other owner(s), within the allotted time period for either Requirement R2, Part 2.1, including subparts 2.1.1, 2.1.2, and 2.1.3 and Requirement R2, Part 2.2. Acceptable evidence for Requirement R2, including Parts 2.1 and 2.2 may include, but is not limited to the following dated documentation (electronic or hardcopy format): emails, facsimiles, or transmittals.

R3. Each Transmission Owner, Generator Owner, and Distribution Provider that receives notification, pursuant to Requirement R2 shall, within the later of 60 calendar days of notification or 120 calendar days of the BES interrupting device(s) operation, identify whether its Protection System component(s) caused a Misoperation. *[Violation Risk Factor: High][Time Horizon: Operations Assessment, Operations Planning]*

M3. Each Transmission Owner, Generator Owner, and Distribution Provider shall have dated evidence that demonstrates it identified whether its Protection System component(s) caused a Misoperation within the allotted time period. Acceptable evidence for Requirement R3 may include, but is not limited to the following dated documentation (electronic or hardcopy format): reports, databases, spreadsheets, emails, facsimiles, lists, logs, records, declarations, analyses of sequence of events, relay targets, DME records, test results, or transmittals.

R4. Reserved.

M4. Reserved.

R5. Each Transmission Owner, Generator Owner, and Distribution Provider that owns the Protection System component(s) that caused the Misoperation shall, within 60 calendar days of first identifying a cause of the Misoperation: [*Violation Risk Factor: High*] [*Time Horizon: Operations Planning, Long-Term Planning*]

- Develop a Corrective Action Plan (CAP) for the identified Protection System component(s), and an evaluation of the CAP's applicability to the entity's other Protection Systems including other locations; or
- Explain in a declaration why corrective actions are beyond the entity's control or would not improve BES reliability, and that no further corrective actions will be taken.

M5. Each Transmission Owner, Generator Owner, and Distribution Provider shall have dated evidence that demonstrates it developed a CAP and an evaluation of the CAP's applicability to other Protection Systems and locations, or a declaration in accordance with Requirement R5. Acceptable evidence for Requirement R5 may include, but is not limited to the following dated documentation (electronic or hardcopy format): CAP and evaluation, or declaration.

R6. Each Transmission Owner, Generator Owner, and Distribution Provider shall

implement each CAP developed in Requirement R5, and update each CAP if actions or timetables change, until completed. *[Violation Risk Factor: High][Time Horizon: Operations Planning, Long-Term Planning]*

M6. Each Transmission Owner, Generator Owner, and Distribution Provider shall have dated evidence that demonstrates it implemented each CAP, including updating actions or timetables. Acceptable evidence for Requirement R6 may include, but is not limited to the following dated documentation (electronic or hardcopy format): records that document the implementation of each CAP and the completion of actions for each CAP including revision history of each CAP. Evidence may also include work management program records, work orders, and maintenance records.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Transmission Owner, Generator Owner, and Distribution Provider shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation.

- The Transmission Owner, Generator Owner, and Distribution Provider shall retain evidence of Requirements R1, R2, and R3, Measures M1, M2, and M3 for a minimum of 12 calendar months following the completion of each Requirement.
- The Transmission Owner, Generator Owner, and Distribution Provider shall retain evidence of Requirement R5, Measure M5, including any supporting analysis per Requirements R1, R2, and R3, for a minimum of 12 calendar months following completion of each CAP, completion of each evaluation, and completion of each declaration.
- The Transmission Owner, Generator Owner, and Distribution Provider shall retain evidence of Requirement R6, Measure M6 for a minimum of 12 calendar months following completion of each CAP.

If a Transmission Owner, Generator Owner, or Distribution Provider is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved, or for the time specified above, whichever is longer.

The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes

- Compliance Audit
- Self-Certification
- Spot Checking

- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information

None.

Violation Severity Levels

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	Operations Assessment, Operations Planning	High	The responsible entity identified whether its Protection System component(s) caused a Misoperation in accordance with Requirement R1, but in more than 120 calendar days and less than or equal to 150 calendar days of the BES interrupting device operation.	The responsible entity identified whether its Protection System component(s) caused a Misoperation in accordance with Requirement R1, but in more than 150 calendar days and less than or equal to 165 calendar days of the BES interrupting device operation.	The responsible entity identified whether its Protection System component(s) caused a Misoperation in accordance with Requirement R1, but in more than 165 calendar days and less than or equal to 180 calendar days of the BES interrupting device operation.	The responsible entity identified whether its Protection System component(s) caused a Misoperation in accordance with Requirement R1, but in more than 180 calendar days of the BES interrupting device operation. OR The responsible entity failed to identify whether its Protection System component(s) caused a Misoperation in accordance with Requirement R1.

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R2.	Operations Assessment, Operations Planning	High	The responsible entity notified the other owner(s) of the Protection System component(s) in accordance with Requirement R2, but in more than 120 calendar days and less than or equal to 150 calendar days of the BES interrupting device operation.	The responsible entity notified the other owner(s) of the Protection System component(s) in accordance with Requirement R2, but in more than 150 calendar days and less than or equal to 165 calendar days of the BES interrupting device operation.	The responsible entity notified the other owner(s) of the Protection System component(s) in accordance with Requirement R2, but in more than 165 calendar days and less than or equal to 180 calendar days of the BES interrupting device operation.	The responsible entity notified the other owner(s) of the Protection System component(s) in accordance with Requirement R2, but in more than 180 calendar days of the BES interrupting device operation. OR The responsible entity failed to notify one or more of the other owner(s) of the Protection System component(s) in accordance with Requirement R2.

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R3.	Operations Assessment, Operations Planning	High	The responsible entity identified whether or not its Protection System component(s) caused a Misoperation in accordance with Requirement R3, but was less than or equal to 30 calendar days late.	The responsible entity identified whether or not its Protection System component(s) caused a Misoperation in accordance with Requirement R3, but was greater than 30 calendar days and less than or equal to 45 calendar days late.	The responsible entity identified whether or not its Protection System component(s) caused a Misoperation in accordance with Requirement R3, but was greater than 45 calendar days and less than or equal to 60 calendar days late.	The responsible entity identified whether or not its Protection System component(s) caused a Misoperation in accordance with Requirement R3, but was greater than 60 calendar days late. OR The responsible entity failed to identify whether or not a Misoperation of its Protection System component(s) occurred in accordance with Requirement R3.
R4. Reserved.						

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R5.	Operations Planning, Long-Term Planning	High	The responsible entity developed a CAP, or explained in a declaration in accordance with Requirement R5, but in more than 60 calendar days and less than or equal to 70 calendar days of first identifying a cause of the Misoperation. OR (See next page)	The responsible entity developed a CAP, or explained in a declaration in accordance with Requirement R5, but in more than 70 calendar days and less than or equal to 80 calendar days of first identifying a cause of the Misoperation. OR (See next page)	The responsible entity developed a CAP, or explained in a declaration in accordance with Requirement R5, but in more than 80 calendar days and less than or equal to 90 calendar days of first identifying a cause of the Misoperation. OR (See next page)	The responsible entity developed a CAP, or explained in a declaration in accordance with Requirement R5, but in more than 90 calendar days of first identifying a cause of the Misoperation. OR The responsible entity failed to develop a CAP or explain in a declaration in accordance with Requirement R5. OR

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			The responsible entity developed an evaluation in accordance with Requirement R5, but in more than 60 calendar days and less than or equal to 70 calendar days of first identifying a cause of the Misoperation.	The responsible entity developed an evaluation in accordance with Requirement R5, but in more than 70 calendar days and less than or equal to 80 calendar days of first identifying a cause of the Misoperation.	The responsible entity developed an evaluation in accordance with Requirement R5, but in more than 80 calendar days and less than or equal to 90 calendar days of first identifying a cause of the Misoperation.	The responsible entity developed an evaluation in accordance with Requirement R5, but in more than 90 calendar days of first identifying a cause of the Misoperation. OR The responsible entity failed to develop an evaluation in accordance with Requirement R5.
R6.	Operations Planning, Long-Term Planning	High	The responsible entity implemented, but failed to update a CAP, when actions or timetables changed, in accordance with Requirement R6.	N/A	N/A	The responsible entity failed to implement a CAP in accordance with Requirement R6.

D. Regional Variances

None.

E. Associated Documents

NERC System Protection and Controls Subcommittee of the NERC Planning Committee, Assessment of Standards: PRC-003-1 – Regional Procedure for Analysis of Misoperations of Transmission and Generation Protection Systems, PRC-004-1 – Analysis and Mitigation of Transmission and Generation Protection Misoperations, PRC-016-1 – Special Protection System Misoperations, May 22, 2009.[2]

Version History

Version	Date	Action	Change Tracking
0	April 1, 2005	Effective Date	New
1	December 1, 2005	1. Changed incorrect use of certain hyphens (-) to "en dash" (–) and "em dash (—)." 2. Added "periods" to items where appropriate. 3. Changed "Timeframe" to "Time Frame" in item D, 1.2.	01/20/06
1a	February 17, 2011	Adopted by NERC Board of Trustees	Project 2009-17 interpretation adding Appendix 1 - Interpretation regarding applicability of standard to protection of radially connected transformers
1a	September 26, 2011	Appended FERC-approved interpretation of R1 and R3 to version 1	FERC's Order approving the interpretation of R1 and R3 is effective as of September 26, 2011
2	August 5, 2010	Adopted by NERC Board of Trustees	Project 2010-12 modifications to address Order No. 693 Directives contained in paragraph 1469

[2] (http://www.nerc.com/comm/PC/System%20Protection%20and%20Control%20Subcommittee%20SPCS%20DL/PRC-003-004-016%20Report.pdf).

Version	Date	Action	Change Tracking
2a	September 26, 2011	Appended FERC-approved interpretation of R1 and R3 to version 2	FERC's Order approving the interpretation of R1 and R3 is effective as of September 26, 2011
2.1a	February 9, 2012	Adopted by NERC Board of Trustees	Errata change under Project 2010-07 to add "…and generator interconnection Facility…"
3	August 14, 2014	Adopted by NERC Board of Trustees	Revision under Project 2010-05.1
4	November 13, 2014	Adopted by NERC Board of Trustees	Applicability revision under Project 2014-01 to clarify application of Requirements to BES dispersed power producing resources
5	May 7, 2015	Adopted by NERC Board of Trustees	Revision under Project 2008-02.2
5(i)	June 22, 2015	Adopted by NERC Board of Trustees	Revision to VRF designations from "Medium" to "High" for Requirements R1 through R6, in compliance with the Federal Energy Regulatory Commission's directive in N. Am. Elec. Reliability Corp., 151 FERC ¶ 61,129 (2015)
6	May 9, 2019	Adopted by the NERC Board of Trustees	R4 retired under Project 2018-03 Standards Efficiency Review Retirements.
6	September 17, 2020	FERC Order issued approving PRC-004-6. Docket No. RM19-16-000, RM19-17-000	

Guidelines and Technical Basis

Introduction

This standard addresses the reliability issues identified in the letter[3] from Gerry Cauley, NERC President and CEO, dated January 7, 2011.

> "Nearly all major system failures, excluding perhaps those caused by severe weather, have misoperations of relays or automatic controls as a factor contributing to the propagation of the failure. …Relays can misoperate, either operate when not needed or fail to operate when needed, for a number of reasons. First, the device could experience an internal failure – but this is rare. Most commonly, relays fail to operate correctly due to incorrect settings, improper coordination (of timing and set points) with other devices, ineffective maintenance and testing, or failure of communications channels or power supplies. Preventable errors can be introduced by field personnel and their supervisors or more programmatically by the organization."

The standard also addresses the findings in the *2011 Risk Assessment of Reliability Performance*[4]; July 2011.

> "…a number of multiple outage events were initiated by protection system Misoperations. These events, which go beyond their design expectations and operating procedures, represent a tangible threat to reliability. A deeper review of the root causes of dependent and common mode events, which include three or more automatic outages, is a high priority for NERC and the industry."

The *State of Reliability 2014*[5] report continued to identify Protection System Misoperations as a significant contributor to automatic transmission outage severity. The report recommended completion of the development of PRC-004-3 as part of the solution to address Protection System Misoperations.

Definitions

The Misoperation definition is based on the IEEE/PSRC Working Group I3 "Transmission Protective Relay System Performance Measuring Methodology[6]." Misoperations of a Protection System include failure to operate, slowness in operating, or operating when not required either during a Fault or non-Fault condition.

For reference, a "Protection System" is defined in the *Glossary of Terms Used in NERC Reliability Standards* ("NERC Glossary") as:

---

[3] (http://www.nerc.com/pa/Stand/Project%20201005%20Protection%20System%20Misoperations%20DL/20110209130708-Cauley%20letter.pdf).

[4] "2011 Risk Assessment of Reliability Performance." NERC. (http://www.nerc.com/files/2011_RARPR_FINAL.pdf. July 2011). Pg. 3.

[5] "State of Reliability 2014." NERC. (http://www.nerc.com/pa/Stand/Pages/RelaibilityCoordinationProject20066.aspx). May 2014. Pg. 18 of 106.

[6] "Transmission Protective Relay System Performance Measuring Methodology." Working Group I3 of Power System Relaying Committee of IEEE Power Engineering Society. 1999.

- Protective relays which respond to electrical quantities,
- Communications systems necessary for correct operation of protective functions,
- Voltage and current sensing devices providing inputs to protective relays,
- Station dc supply associated with protective functions (including station batteries, battery chargers, and non-battery-based dc supply), and
- Control circuitry associated with protective functions through the trip coil(s) of the circuit breakers or other interrupting devices.

A BES interrupting device is a BES Element, typically a circuit breaker or circuit switcher that has the capability to interrupt fault current. Although BES interrupting device mechanisms are not part of a Protection System, the standard uses the operation of a BES interrupting device by a Protection System to initiate the review for Misoperation.

The following two definitions are being proposed for inclusion in the NERC Glossary:

> **Composite Protection System –** *The total complement of Protection System(s) that function collectively to protect an Element. Backup protection provided by a different Element's Protection System(s) is excluded.*

The Composite Protection System definition is based on the principle that an Element's multiple layers of protection are intended to function collectively. This definition has been introduced in this standard and incorporated into the proposed definition of Misoperation to clarify that the overall performance of an Element's total complement of protection should be considered while evaluating an operation.

Composite Protection System – Line Example
The Composite Protection System of the Alpha-Beta line (Circuit #123) is comprised of current differential, permissive overreaching transfer trip (POTT), step distance (classic zone 1, zone 2, and zone 3), instantaneous-overcurrent, time-overcurrent, out-of-step, and overvoltage protection. The protection is housed at the Alpha and Beta substations, and includes the associated relays, communications systems, voltage and current sensing devices, DC supplies, and control circuitry.

Composite Protection System – Transformer Example
The Composite Protection System of the Alpha transformer (#2) is comprised of internal differential, overall differential, instantaneous-overcurrent, and time-overcurrent protection. The protection is housed at the Alpha substation, and includes the associated relays, voltage and current sensing devices, DC supplies, and control circuitry.

Composite Protection System – Generator Example
The Composite Protection System of the Beta generator (#3) is comprised of generator differential, overall differential, overcurrent, stator ground, reverse power, volts per hertz, loss-of-field, and undervoltage protection. The protection is housed at the Beta generating plant and at the Beta substation, and includes the associated relays, voltage and current sensing

devices, DC supplies, and control circuitry.

Composite Protection System – Breaker Failure Example

Breaker failure protection provides backup protection for the breaker, and therefore is part of the breaker's Composite Protection System. Considering breaker failure protection to be part of another Element's Composite Protection System could lead to an incorrect conclusion that a breaker failure operation automatically satisfies the "Slow Trip" criteria of the Misoperation definition.

- An example of a correct operation of the breaker's Composite Protection System is when the breaker failure relaying tripped because the line relaying operated, but the breaker failed to clear the Fault. The breaker failure relaying operated because of a failed trip coil. The failed trip coil caused a Misoperation of the line's Composite Protection System.
- An example of a correct operation of the breaker's Composite Protection System is when the breaker failure relaying tripped because the line relaying operated, but the breaker failed to clear the Fault. Only the breaker failure relaying operated because of a failed breaker mechanism. This was not a Misoperation because the breaker mechanism is not part of the breaker's Composite Protection System.
- An example of an "Unnecessary Trip – During Fault" is when the breaker failure relaying tripped at the same time as the line relaying during a Fault. The Misoperation was due to the breaker failure timer being set to zero.

Misoperation – *The failure a Composite Protection System to operate as intended for protection purposes. Any of the following is a Misoperation:*

1. **Failure to Trip – During Fault** – *A failure of a Composite Protection System to operate for a Fault condition for which it is designed. The failure of a Protection System component is not a Misoperation as long as the performance of the Composite Protection System is correct.*
2. ***Failure to Trip – Other Than Fault*** *– A failure of a Composite Protection System to operate for a non-Fault condition for which it is designed, such as a power swing, undervoltage, overexcitation, or loss of excitation. The failure of a Protection System component is not a Misoperation as long as the performance of the Composite Protection System is correct.*
3. ***Slow Trip – During Fault*** *– A Composite Protection System operation that is slower than required for a Fault condition if the duration of its operating time resulted in the operation of at least one other Element's Composite Protection System.*
4. ***Slow Trip – Other Than Fault*** *– A Composite Protection System operation that is slower than required for a non-Fault condition, such as a power swing, undervoltage, overexcitation, or loss of excitation, if the duration of its operating time resulted in the operation of at least one other Element's Composite Protection System.*
5. ***Unnecessary Trip – During Fault*** *– An unnecessary Composite Protection System operation for a Fault condition on another Element.*
6. ***Unnecessary Trip – Other Than Fault*** *– An unnecessary Composite Protection System*

operation for a non-Fault condition. A Composite Protection System operation that is caused by personnel during on-site maintenance, testing, inspection, construction, or commissioning activities is not a Misoperation.

The Misoperation definition is based on the principle that an Element's total complement of protection is intended to operate dependably and securely.

- Failure to automatically reclose after a Fault condition is not included as a Misoperation because reclosing equipment is not included within the definition of Protection System.
- A breaker failure operation does not, in itself, constitute a Misoperation.
- A remote backup operation resulting from a "Failure to Trip" or a "Slow Trip" does not, in itself, constitute a Misoperation.

This proposed definition of Misoperation provides additional clarity over the current version. A Misoperation is the failure of a Composite Protection System to operate as intended for protection purposes. The definition includes six categories which provide further differentiation of what constitutes a Misoperation. These categories are discussed in greater detail in the following sections.

Failure to Trip – During Fault

This category of Misoperation typically results in the Fault condition being cleared by remote backup Protection System operation.

Example 1a: A failure of a transformer's Composite Protection System to operate for a transformer Fault is a Misoperation.

Example 1b: A failure of a "primary" transformer relay (or any other component) to operate for a transformer Fault is not a "Failure to Trip – During Fault" Misoperation as long as another component of the transformer's Composite Protection System operated.

Example 1c: A lack of target information does not by itself constitute a Misoperation. When a high-speed pilot system does not target because a high-speed zone element trips first, it would not in and of itself be a Misoperation.

Example 1d: A failure of an overall differential relay to operate is not a "Failure to Trip – During Fault" Misoperation as long as another component such as a generator differential relay operated.

Example 1e: The Composite Protection System for a bus does not operate during a bus Fault which results in the operation of all local transformer Protection Systems connected to that bus and all remote line Protection Systems connected to that bus isolating the faulted bus from the grid. The operation of the local transformer Protection Systems and the operation of all remote line Protection Systems correctly provided backup protection. There is one "Failure to Trip – During Fault" Misoperation of the bus Composite Protection System.

In analyzing the Protection System for Misoperation, the entity must also consider whether the "Slow Trip – During Fault" category applies to the operation.

Failure to Trip – Other Than Fault

This category of Misoperation may have resulted in operator intervention. The "Failure to Trip – Other Than Fault" conditions cited in the definition are examples only, and do not constitute an all-inclusive list.

> **Example 2a:** A failure of a generator's Composite Protection System to operate for an unintentional loss of field condition is a Misoperation.
>
> **Example 2b:** A failure of an overexcitation relay (or any other component) is not a "Failure to Trip – Other Than Fault" Misoperation as long as the generator's Composite Protection System operated as intended isolating the generator from the BES.

In analyzing the Protection System for Misoperation, the entity must also consider whether the "Slow Trip – Other Than Fault" category applies to the operation.

Slow Trip – During Fault

This category of Misoperation typically results in remote backup Protection System operation before the Fault is cleared.

> **Example 3a:** A Composite Protection System that is slower than required for a Fault condition is a Misoperation if the duration of its operating time resulted in the operation of at least one other Element's Composite Protection System. The current differential element of a multiple function relay failed to operate for a line Fault. The same relay's time-overcurrent element operated after a time delay. However, an adjacent line also operated from a time-overcurrent element. The faulted line's time-overcurrent element was found to be set to trip too slowly.
>
> **Example 3b:** A failure of a breaker's Composite Protection System to operate as quickly as intended to meet the expected critical Fault clearing time for a line Fault in conjunction with a breaker failure (i.e., stuck breaker) is a Misoperation if it resulted in an unintended operation of at least one other Element's Composite Protection System. If a generating unit's Composite Protection System operates due to instability caused by the slow trip of the breaker's Composite Protection System, it is not an "Unnecessary Trip – During Fault" Misoperation of the generating unit's Composite Protection System. This event would be a "Slow Trip – During Fault" Misoperation of the breaker's Composite Protection System.
>
> **Example 3c:** A line connected to a generation interconnection station is protected with two independent high-speed pilot systems. The Composite Protection System for this line also includes step distance and time-overcurrent schemes in addition to the two pilot systems. During a Fault on this line, the two pilot systems fail to operate and the time-overcurrent scheme operates clearing the Fault with no generating units or other Elements tripping (i.e., no over-trips). This event is not a Misoperation.

The phrase “slower than required” means the duration of its operating time resulted in the operation of at least one other Element’s Composite Protection System. It would be impractical to provide a precise tolerance in the definition that would be applicable to every type of Protection System. Rather, the owner(s) reviewing each Protection System operation should understand whether the speed and outcome of its Protection System operation met their objective. The intent is not to require documentation of exact Protection System operation times, but to assure consideration of relay coordination and system stability by the owner(s) reviewing each Protection System operation.

The phrase “resulted in the operation of any other Composite Protection System” refers to the need to ensure that relaying operates in the proper or planned sequence (i.e., the primary relaying for a faulted Element operates before the remote backup relaying for the faulted Element).

In analyzing the Protection System for Misoperation, the entity must also consider the “Unnecessary Trip – During Fault” category to determine if an “unnecessary trip” applies to the Protection System operation of an Element other than the faulted Element.

If a coordination error was at the local terminal (i.e., set too slow), then it was a "Slow Trip," category of Misoperation at the local terminal.

Slow Trip – Other Than Fault

The phrase “slower than required” means the duration of its operating time resulted in the operation of at least one other Element’s Composite Protection System. It would be impractical to provide a precise tolerance in the definition that would be applicable to every type of Protection System. Rather, the owner(s) reviewing each Protection System operation should understand whether the speed and outcome of its Protection System operation met their objective. The intent is not to require documentation of exact Protection System operation times, but to assure consideration of relay coordination and system stability by the owner(s) reviewing each Protection System operation.

> **Example 4:** A phase to phase fault occurred on the terminals of a generator. The generator's Composite Protection System and a transmission line's Composite Protection System both operated in response to the fault. It was found during subsequent investigation that the generator protection contained an inappropriate time delay. This caused the transmission line's correctly set overreaching zone of protection to operate. This was a Misoperation of the generator’s Composite Protection System, but not of the transmission line’s Composite Protection System.

The “Slow Trip – Other Than Fault” conditions cited in the definition are examples only, and do not constitute an all-inclusive list.

Unnecessary Trip – During Fault

An operation of a properly coordinated remote Protection System is not in and of itself a Misoperation if the Fault has persisted for a sufficient time to allow the correct operation of the

Composite Protection System of the faulted Element to clear the Fault. A BES interrupting device failure, a “failure to trip” Misoperation, or a “slow trip” Misoperation may result in a proper remote Protection System operation.

Example 5: An operation of a transformer's Composite Protection System which trips (i.e., over-trips) for a properly cleared line Fault is a Misoperation. The Fault is cleared properly by the faulted equipment's Composite Protection System (i.e., line relaying) without the need for an external Protection System operation resulting in an unnecessary trip of the transformer protection; therefore, the transformer Protection System operation is a Misoperation.

Example 5b: An operation of a line's Composite Protection System which trips (i.e., over-trips) for a properly cleared Fault on a different line is a Misoperation. The Fault is cleared properly by the faulted line's Composite Protection System (i.e., line relaying); however, elsewhere in the system, a carrier blocking signal is not transmitted (e.g., carrier ON/OFF switch found in OFF position) resulting in the operation of a remote Protection System, single-end trip of a non-faulted line. The operation of the Protection System for the non-faulted line is an unnecessary trip during a Fault. Therefore, the non-faulted line Protection System operation is an “Unnecessary Trip – During Fault” Misoperation.

Example 5c: If a coordination error was at the remote terminal (i.e., set too fast), then it was an "Unnecessary Trip – During Fault" category of Misoperation at the remote terminal.

Unnecessary Trip – Other Than Fault

Unnecessary trips for non-Fault conditions include but are not limited to: power swings, overexcitation, loss of excitation, frequency excursions, and normal operations.

Example 6a: An operation of a line's Composite Protection System due to a relay failure during normal operation is a Misoperation.

Example 6b: Tripping a generator by the operation of the loss of field protection during an off-nominal frequency condition while the field is intact is a Misoperation assuming the Composite Protection System was not intended to operate under this condition.

Example 6c: An impedance line relay trip for a power swing that entered the relay’s characteristic is a Misoperation if the power swing was stable and the relay operated because power swing blocking was enabled and should have prevented the trip, but did not.

Example 6d: Tripping a generator operating at normal load by the operation of a reverse power protection relay due to a relay failure is a Misoperation.

Additionally, an operation that occurs during a non-Fault condition but was initiated directly by on-site (i.e., real-time) maintenance, testing, inspection, construction, or commissioning is not a Misoperation.

Example 6e: A BES interrupting device operation that occurs at the remote end of a line

during a non-Fault condition because a direct transfer trip was initiated by system maintenance and testing activities at the local end of the line is not a Misoperation because of the maintenance exclusion in category 6 of the definition of "Misoperation."

The "on-site" activities at one location that initiates a trip to another location are included in this exemption. This includes operation of a Protection System when energizing equipment to facilitate measurements, such as verification of current circuits as a part of performing commissioning; however, once the maintenance, testing, inspection, construction, or commissioning activity associated with the Protection System is complete, the "on-site" Misoperation exclusion no longer applies, regardless of the presence of on-site personnel.

Special Cases

Protection System operations for these cases would not be a Misoperation.

Example 7a: A generator Protection System operation prior to closing the unit breaker(s) is not a Misoperation provided no in-service Elements are tripped.

This type of operation is not a Misoperation because the generating unit is not synchronized and is isolated from the BES. Protection System operations that occur when the protected Element is out of service and that do not trip any in-service Elements are not Misoperations. In some cases where zones of protection overlap, the owner(s) of Elements may decide to allow a Protection System to operate faster in order to gain better overall Protection System performance for an Element.

Example 7b: The high-side of a transformer connected to a line may be within the zone of protection of the supplying line's relaying. In this case, the line relaying is planned to protect the area of the high-side of the transformer and into its primary winding. In order to provide faster protection for the line, the line relaying may be designed and set to operate without direct coordination (or coordination is waived) with local protection for Faults on the high-side of the connected transformer. Therefore, the operation of the line relaying for a high-side transformer Fault operated as intended and would not be a Misoperation.

Below are examples of conditions that would be a Misoperation.

Example7c: A 230 kV shunt capacitor bank was released for operational service. The capacitor bank trips due to a settings error in the capacitor bank differential relay upon energization.

Example 7d: A 230/115 kV BES transformer bank trips out when being re-energized due to an incorrect operation of the transformer differential relay for inrush after being released for operational service. Only the high-side breaker opens since the low-side breaker had not yet been closed.

Non-Protective Functions

BES interrupting device operations which are initiated by non-protective functions, such as those associated with generator controls, excitation controls, or turbine/boiler controls, static

voltampere-reactive compensators (SVC), flexible ac transmission systems (FACTS), high-voltage dc (HVdc) transmission systems, circuit breaker mechanisms, or other facility control systems are not operations of a Protection System. The standard is not applicable to non-protective functions such as automation (e.g., data collection) or control functions that are embedded within a Protection System.

Control Functions

The entity must make a determination as to whether the standard is applicable to each operation of its Protection System in accordance with the provided exclusions in the standard's Applicability, see Section 4.2.1. The subject matter experts (SME) developing this standard recognize that entities use Protection Systems as part of a routine practice to control BES Elements. This standard is not applicable to operation of protective functions within a Protection System when intended for controlling a BES Element as a part of an entity's process or planned switching sequence. The following are examples of conditions to which this standard is not applicable:

> **Example 8a:** The reverse power protective function that operates to remove a generating unit from service using the entity's normal or routine process.
>
> **Example 8b:** The reverse power relay enables a permissive trip and the generator operator trips the unit.

The standard is not applicable to operation of the protective relay because its operation is intended as a control function as part of a controlled shutdown sequence for the generator. However, the standard remains applicable to operation of the reverse power relay when it operates for conditions not associated with the controlled shutdown sequence, such as a motoring condition caused by a trip of the prime mover.

The following is another example of a condition to which this standard is not applicable:

> **Example 8c:** Operation of a capacitor bank interrupting device for voltage control using functions embedded within a microprocessor based relay that is part of a Protection System.

The above are examples only, and do not constitute an all-inclusive list to which the standard is not applicable.

Extenuating Circumstances

In the event of a natural disaster or other extenuating circumstances, the December 20, 2012 Sanction Guidelines of the North American Electric Reliability Corporation, Section 2.8, Extenuating Circumstances, reads: "In unique extenuating circumstances causing or contributing to the violation, such as significant natural disasters, NERC or the Regional Entity may significantly reduce or eliminate Penalties." The Regional Entities to whom NERC has delegated authority will consider extenuating circumstances when considering any sanctions in relation to the timelines outlined in this standard.

The volume of Protection System operations tend to be sporadic. If a high rate of Protection System operations is not sustained, utilities will have an opportunity to catch up within the 120 day period.

Requirement Time Periods

The time periods within all the Requirements are distinct and separate. The applicable entity in Requirement R1 has 120 calendar days to identify whether a BES interrupting device operation is a Misoperation. Once the applicable entity has identified a Misoperation, it has completed its performance under Requirement R1. Identified Misoperations with an identified cause become subject to Requirement R5 and any subsequent Requirements as necessary.

In Requirement R2, the applicable entity has 120 calendar days, based on the date of the BES interrupting device operation, to provide notification to the other Protection System owners that meet the circumstances in Parts 2.1 and 2.2. For the case of an applicable entity that was notified (R3), it has the later of 120 calendar days from the date of the BES interrupting device operation or 60 calendar days of notification to identify whether its Protection System components caused a Misoperation.

Once a Misoperation is identified in either Requirement R1 or R3, and the applicable entity did not identify the cause(s) of the Misoperation, the time period for performing at least one investigative action every two full calendar quarters begins.

The time period in Requirement R5 begins when the Misoperation cause is first identified. The applicable entity is allotted 60 calendar days to perform one of the two activities listed in Requirement R5 (e.g., CAP or declaration) to complete its performance under Requirement R5.

Requirement R6 time period is determined by the actions and the associated timetable to complete those actions identified in the CAP. The time periods contained in the CAP may change from time to time and the applicable entity is required to update the timetable when it changes.

Time periods provided in the Requirements are intended to provide a reasonable amount of time to perform each Requirement. Performing activities in the least amount of time facilitates prompt identification of Misoperations, notification to other Protection System owners, identification of the cause(s), correction of the cause(s), and that important information is retained that may be lost due to time.

Requirement R1

This Requirement initiates a review of each BES interrupting device operation to identify whether or not a Misoperation may have occurred. Since the BES interrupting device owner typically monitors and tracks device operations, the owner is the logical starting point for identifying Misoperations of Protection Systems for BES Elements. A review is required when (1) a BES interrupting device operates that is caused by a Protection System or by manual intervention in response to a Protection System failure to operate, (2) regardless of whether the owner owns all or part of the Protection System component(s), and (3) the owner identified its Protection System component(s) as causing the BES interrupting device operation or was

caused by manual intervention in response to its Protection System failure to operate.

Since most Misoperations result in the operation of one or more BES interrupting devices, these operations initiate a review to identify any Misoperation. If an Element is manually isolated in response to a failure to operate, the manual isolation of the Element triggers a review for Misoperation.

> **Example R1a:** The failure of a loss of field relay on a generating unit where an operator takes action to isolate the unit.

Manual intervention may indicate a Misoperation has occurred, thus requiring the initiation of an investigation by the BES interrupting device owner.

For the case where a BES interrupting device did not operate and remote clearing occurs due to the failure of a Composite Protection System to operate, the BES interrupting device owner would still review the operation under Requirement R1. However, if the BES interrupting device owner determines that its Protection System component operated as backup protection for a condition on another entity's BES Element, the owner would provide notification of the operation to the other Protection System owner(s) under Requirement R2, Part 2.2.

Protection Systems are made of many components. These components may be owned by different entities. For example, a Generator Owner may own a current transformer that sends information to a Transmission Owner's differential relay. All of these components and many more are part of a Protection System. It is expected that all of the owners will communicate with each other, sharing information freely, so that Protection System operations can be analyzed, Misoperations identified, and corrective actions taken.

Each entity is expected to use judgment to identify those Protection System operations that meet the definition of Misoperation regardless of the level of ownership. A combination of available information from resources such as counters, relay targets, Supervisory Control and Data Acquisition (SCADA) systems, or DME would typically be used to determine whether or not a Misoperation occurred. The intent of the standard is to classify an operation as a Misoperation if the available information leads to that conclusion. In many cases, it will not be necessary to leverage all available data to determine whether or not a Misoperation occurred. The standard also allows an entity to classify an operation as a Misoperation if entity is not sure. The entity may decide to identify the operation as a Misoperation to satisfy Requirement R1 and continue its investigation for a cause of the Misoperation . If the continued investigative actions are inconclusive, the entity may declare no cause found and end its investigation. The entity is allotted 120 calendar days from the date of its BES interrupting device operation to identify whether its Protection System component(s) caused a Misoperation.

The Protection System operation may be documented in a variety of ways such as in a report, database, spreadsheet, or list. The documentation may be organized in a variety of ways such as by BES interrupting device, protected Element, or Composite Protection System.

Repeated operations which occur during the same automatic reclosing sequence do not need a

separate identification under Requirement R1. Repeated Misoperations which occur during the same 24-hour period do not need a separate identification under Requirement R1. This is consistent with the NERC *Misoperations Report*[7] which states:

> "In order to avoid skewing the data with these repeated events, the NERC SPCS should clarify, in the next annual update of the misoperation template, that all misoperations due to the same equipment and cause within a 24 hour period be recorded as one misoperation."

The following is an example of a condition that is not a Misoperation.

> **Example R1b:** A high impedance Fault occurs within a transformer. The sudden pressure relaying detects and operates for the Fault, but the differential relaying did not operate due to the low Fault current levels. This is not a Misoperation because the Composite Protection System was not required to operate because the Fault was cleared by the sudden pressure relay.

Requirement R2

Requirement R2 ensures notification of those who have a role in identifying Misoperations, but were not accounted for within Requirement R1. In the case of multi-entity ownership, the entity that owns the BES interrupting device that operated is expected to use judgment to identify those Protection System operations that meet the definition of Misoperation under Requirement R1; however, if the entity that owns a BES interrupting device determines that its Protection System component(s) did not cause the BES interrupting device(s) operation or cannot determine whether its Protection System components caused the BES interrupting device(s) operation, it must notify the other Protection System owner(s) that share Misoperation identification responsibility when the criteria in Requirement R2 is met.

This Requirement does not preclude the Protection System owners from initially communicating and working together to determine whether a Misoperation occurred and, if so, the cause. The BES interrupting device owner is only required to officially notify the other owners when it: (1) shares the Composite Protection System ownership with other entity(ies), (2) determines that a Misoperation occurred or cannot rule out a Misoperation, and (3) determines its Protection System component(s) did not cause a Misoperation or is unsure. Officially notifying the other owners without performing a preliminary review may unnecessarily burden the other owners with compliance obligations under Requirement R3, redirect valuable resources, and add little benefit to reliability. The BES interrupting device owner should officially notify other owners when appropriate within the established time period.

The following is an example of a notification to another Protection System owner:

> **Example R2a:** Circuit breakers A and B at the Charlie station tripped from directional

[7] "Misoperations Report." Reporting Multiple Occurrences. NERC Protection System Misoperations Task Force. (http://www.nerc.com/docs/pc/psmtf/PSMTF_Report.pdf). April 1, 2013. Pg. 37 of 40.

comparison blocking (DCB) relaying on 03/03/2014 at 15:43 UTC during an external Fault. As discussed last week, the fault records indicate that a problem with your equipment (failure to transmit) caused the operation.

Example R2b: A generator unit tripped out immediately upon synchronizing to the grid due to a Misoperation of its overcurrent protection. The Transmission Owner owns the 230 kV generator breaker that operated. The Transmission Owner, as the owner of the BES interrupting device after determining that its Protection System components did not cause the Misoperation, notified the Generator Owner of the operation. The Generator Owner investigated and determined that its Protection System components caused the Misoperation. In this example, the Generator Owner's Protection System components did cause the Misoperation. As the owner of the Protection System components that caused the Misoperation, the Generator Owner is responsible for creating and implementing the CAP.

A Composite Protection System owned by different functional entities within the same registered entity does not necessarily satisfy the notification criteria in Part 2.1.1 of Requirement R2. For example, if the same personnel within a registered entity perform the Misoperation identification for both the Generator Owner and Transmission Owner functions, then the Misoperation identification would be completely covered in Requirement R1, and therefore notification would not be required. However, if the Misoperation identification is handled by different groups, then notification would be required because the Misoperation identification would not necessarily be covered in Requirement R1.

Example R2c: Line A Composite Protection System (owned by entity 1) failed to operate for an internal Fault. As a result, the zone 3 portion of Line B's Composite Protection System (owned by entity 2) and zone 3 portion of Line C's Composite Protection System (owned by entity 3) operated to clear the Fault. Entity 2 and 3 notified entity 1 of the remote zone 3 operation.

For the case where a BES interrupting device operates to provide backup protection for a non-BES Element, the entity reviewing the operation is not required to notify the other owners of Protection Systems for non-BES Elements. No notification is required because this Reliability Standard is not applicable to Protection Systems for non-BES Elements.

Requirement R3

For Requirement R3 (i.e., notification received), the entity that also owns a portion of the Composite Protection System is expected to use judgment to identify whether the Protection System operation is a Misoperation. A combination of available information from resources such as counters, relay targets, SCADA, DME, and information from the other owner(s) would typically be used to determine whether or not a Misoperation occurred. The intent of the standard is to classify an operation as a Misoperation if the available information leads to that conclusion. In many cases, it will not be necessary to leverage all available data to determine whether or not a Misoperation occurred. The standard also allows an entity to classify an operation as a Misoperation if an entity is not sure. The entity may decide to identify the operation as a Misoperation to satisfy Requirement R1 and continue its investigation for a

cause of the Misoperation. If the continued investigative actions are inconclusive, the entity may declare no cause found and end its investigation.

The entity that is notified by the BES interrupting device owner is allotted the later of 60 calendar days from receipt of notification or 120 calendar days from the BES interrupting device operation date to determine if its portion of the Composite Protection System caused the Protection System operation. It is expected that in most cases of a jointly owned Protection System, the entity making notification would have been in communication with the other owner(s) early in the process. This means that the shorter 60 calendar days only comes into play if the notification occurs in the second half of the 120 calendar days allotted to the BES interrupting device owner in Requirement R1.

The Protection System review may be organized in a variety of ways such as in a report, database, spreadsheet, or list. The documentation may be organized in a variety of ways such as by BES interrupting device, protected Element, or Composite Protection System. The BES interrupting device owner's notification received may be documented in a variety of ways such as an email or a facsimile.

Requirement R5

Resolving the causes of Protection System Misoperations benefits BES reliability by preventing recurrence. The Corrective Action Plan (CAP) is an established tool for resolving operational problems. The NERC Glossary defines a Corrective Action Plan as, *"A list of actions and an associated timetable for implementation to remedy a specific problem."* Since a CAP addresses specific problems, the determination of what went wrong needs to be completed before developing a CAP. When the Misoperation cause is identified in Requirement R1 or R3, Requirement R5 requires Protection System owner(s) to develop a CAP, or explain why corrective actions are beyond the entity's control or would not improve BES reliability. The entity must develop the CAP or make a declaration why additional actions are beyond the entity's control or would not improve BES reliability and that no further corrective actions will be taken within 60 calendar days of first determining a cause.

The SMEs developing this standard recognize there may be multiple causes for a Misoperation. In these circumstances, the CAP would include a remedy for the identified causes. The CAP may be revised if additional causes are found; therefore, the entity has the option to create a single or multiple CAP(s) to correct multiple causes of a Misoperation. The 60 calendar day period for developing a CAP (or declaration) is established on the basis of industry experience which includes operational coordination timeframes, time to consider alternative solutions, coordination of resources, and development of a schedule.

The development of a CAP is intended to document the specific corrective actions needed to be taken to prevent Misoperation recurrence, the timetable for executing such actions, and an evaluation of the CAP's applicability to the entity's other Protection Systems including other locations. The evaluation of these other Protection Systems aims to reduce the risk and likelihood of similar Misoperations in other Protection Systems. The Protection System owner is responsible for determining the extent of its evaluation concerning other Protection Systems and locations. The evaluation may result in the owner including actions to address Protection

Systems at other locations or the reasoning for not taking any action. The CAP and an evaluation of other Protection Systems including other locations must be developed to complete Requirement R5.

The following is an example of a CAP for a relay Misoperation that was applying a standing trip due to a failed capacitor within the relay and the evaluation of the cause at similar locations which determined capacitor replacement was not necessary.

For completion of each CAP in Examples R5a through R5d, please see Examples R6a through R6d.

> **Example R5a:** Actions: Remove the relay from service. Replace capacitor in the relay. Test the relay. Return to service or replace by 07/01/2014.
>
> Applicability to other Protection Systems: This type of impedance relay has not been experiencing problems and is systematically being replaced with microprocessor relays as Protection Systems are modernized. Therefore, it was assessed that a program for wholesale preemptive replacement of capacitors in this type of impedance relay does not need to be established for the system.

The following is an example of a CAP for a relay Misoperation that was applying a standing trip due to a failed capacitor within the relay and the evaluation of the cause at similar locations which determined the capacitors need preemptive correction action.

> **Example R5b:** Actions: Remove the relay from service. Replace capacitor in the relay. Test the relay. Return to service or replace by 07/01/2014.
>
> Applicability to other Protection Systems: This type of impedance relay is suspected to have previously tripped at other locations because of the same type of capacitor issue. Based on the evaluation, a program should be established by 12/01/2014 for wholesale preemptive replacement of capacitors in this type of impedance relay.

The following is an example of a CAP for a relay Misoperation that was applying a standing trip due to a failed capacitor within the relay and the evaluation of the cause at similar locations which determined the capacitors need preemptive correction action.

> **Example R5c:** Actions: Remove the relay from service. Replace capacitor in the relay. Test the relay. Return to service or replace by 07/01/2014.
>
> Applicability to other Protection Systems: This type of impedance relay is suspected to have previously tripped at other locations because of the same type of capacitor issue. Based on the evaluation, the preemptive replacement of capacitors in this type of impedance relay should be pursued for the identified stations A through I by 04/30/2015.
>
> A plan is being developed to replace the impedance relay capacitors at stations A, B, and C by 09/01/2014. A second plan is being developed to replace the impedance relay capacitors

at stations D, E, and F by 11/01/2014. The last plan will replace the impedance relay capacitors at stations G, H, and I by 02/01/2015.

The following is an example of a CAP for a relay Misoperation that was due to a version 2 firmware problem and the evaluation of the cause at similar locations which determined the firmware needs preemptive correction action.

Example R5d: Actions: Provide the manufacturer fault records. Install new firmware pending manufacturer results by 10/01/2014.

Applicability to other Protection Systems: Based on the evaluation of other locations and a risk assessment, the newer firmware version 3 should be installed at all installations that are identified to be version 2. Twelve relays were identified across the system. Proposed completion date is 12/31/2014.

The following are examples of a declaration made where corrective actions are beyond the entity's control or would not improve BES reliability and that no further corrective actions will be taken.

Example R5e: The cause of the Misoperation was due to a non-registered entity communications provider problem.

Example R5f: The cause of the Misoperation was due to a transmission transformer tapped industrial customer who initiated a direct transfer trip to a registered entity's transmission breaker.

In situations where a Misoperation cause emanates from a non-registered outside entity, there may be limited influence an entity can exert on an outside entity and is considered outside of an entity's control.

The following are examples of declarations made why corrective actions would not improve BES reliability.

Example R5g: The investigation showed that the Misoperation occurred due to transients associated with energizing transformer ABC at Station Y. Studies show that de-sensitizing the relay to the recorded transients may cause the relay to fail to operate as intended during power system oscillations.

Example R5h: As a result of an operation that left a portion of the power system in an electrical island condition, circuit XYZ within that island tripped, resulting in loss of load within the island. Subsequent investigation showed an overfrequency condition persisted after the formation of that island and the XYZ line protective relay operated. Since this relay was operating outside of its designed frequency range and would not be subject to this condition when line XYZ is operated normally connected to the BES, no corrective action will be taken because BES reliability would not be improved.

Example R5i: During a major ice storm, four of six circuits were lost at Station A. Subsequent to the loss of these circuits, a skywire (i.e., shield wire) broke near station A on line AB (between Station A and B) resulting in a phase-phase Fault. The protection scheme utilized for both protection groups is a permissive overreaching transfer trip (POTT). The Line AB protection at Station B tripped timed for this event (i.e., Slow Trip – During Fault) even though this line had been identified as requiring high speed clearing. A weak infeed condition was created at Station A due to the loss of 4 transmission circuits resulting in the absence of a permissive signal on Line AB from Station A during this Fault. No corrective action will be taken for this Misoperation as even under N-1 conditions, there is normally enough infeed at Station A to send a proper permissive signal to station B. Any changes to the protection scheme to account for this would not improve BES reliability.

A declaration why corrective actions are beyond the entity's control or would not improve BES reliability should include the Misoperation cause and the justification for taking no corrective action. Furthermore, a declaration that no further corrective actions will be taken is expected to be used sparingly.

Requirement R6

To achieve the stated purpose of this standard, which is to identify and correct the causes of Misoperations of Protection Systems for BES Elements, the responsible entity is required to implement a CAP that addresses the specific problem (i.e., cause(s) of the Misoperation) through completion. Protection System owners are required in the implementation of a CAP to update it when actions or timetable change, until completed. Accomplishing this objective is intended to reduce the occurrence of future Misoperations of a similar nature, thereby improving reliability and minimizing risk to the BES.

The following is an example of a completed CAP for a relay Misoperation that was applying a standing trip (See also, Example R5a).

Example R6a: Actions: The impedance relay was removed from service on 06/02/2014 because it was applying a standing trip. A failed capacitor was found within the impedance relay and replaced. The impedance relay functioned properly during testing after the capacitor was replaced. The impedance relay was returned to service on 06/05/2014.

CAP completed on 06/25/2014.

The following is an example of a completed CAP for a relay Misoperation that was applying a standing trip that resulted in the correction and the establishment of a program for further replacements (See also, Example R5b).

Example R6b: Actions: The impedance relay was removed from service on 06/02/2014 because it was applying a standing trip. A failed capacitor was found within the impedance relay and replaced. The impedance relay functioned properly during testing after the capacitor was replaced. The impedance relay was returned to service on 06/05/2014.

A program for wholesale preemptive replacement of capacitors in this type of impedance

relay was established on 10/28/2014.

CAP completed on 10/28/2014.

The following is an example of a completed CAP of corrective actions with a timetable that required updating for a failed relay and preemptive actions for similar installations (See also, Example R5c).

Example R6c: Actions: The impedance relay was removed from service on 06/02/2014 because it was applying a standing trip. A failed capacitor was found within the impedance relay and replaced. The impedance relay functioned properly during testing after the capacitor was replaced. The impedance relay was returned to service on 06/05/2014.

The impedance relay capacitor replacement was completed at stations A, B, and C on 08/16/2014. The impedance relay capacitor replacement was completed at stations D, E, and F on 10/24/2014. The impedance relay capacitor replacement for stations G, H, and I were postponed due to resource rescheduling from a scheduled 02/01/15 completion to 04/01/2015 completion. Capacitor replacement was completed on 03/09/2015 at stations G, H, and I. All stations identified in the evaluation have been completed.

CAP completed on 03/09/2015.

The following is an example of a completed CAP for corrective actions with updated actions for a firmware problem and preemptive actions for similar installations. (See also, Example R5d).

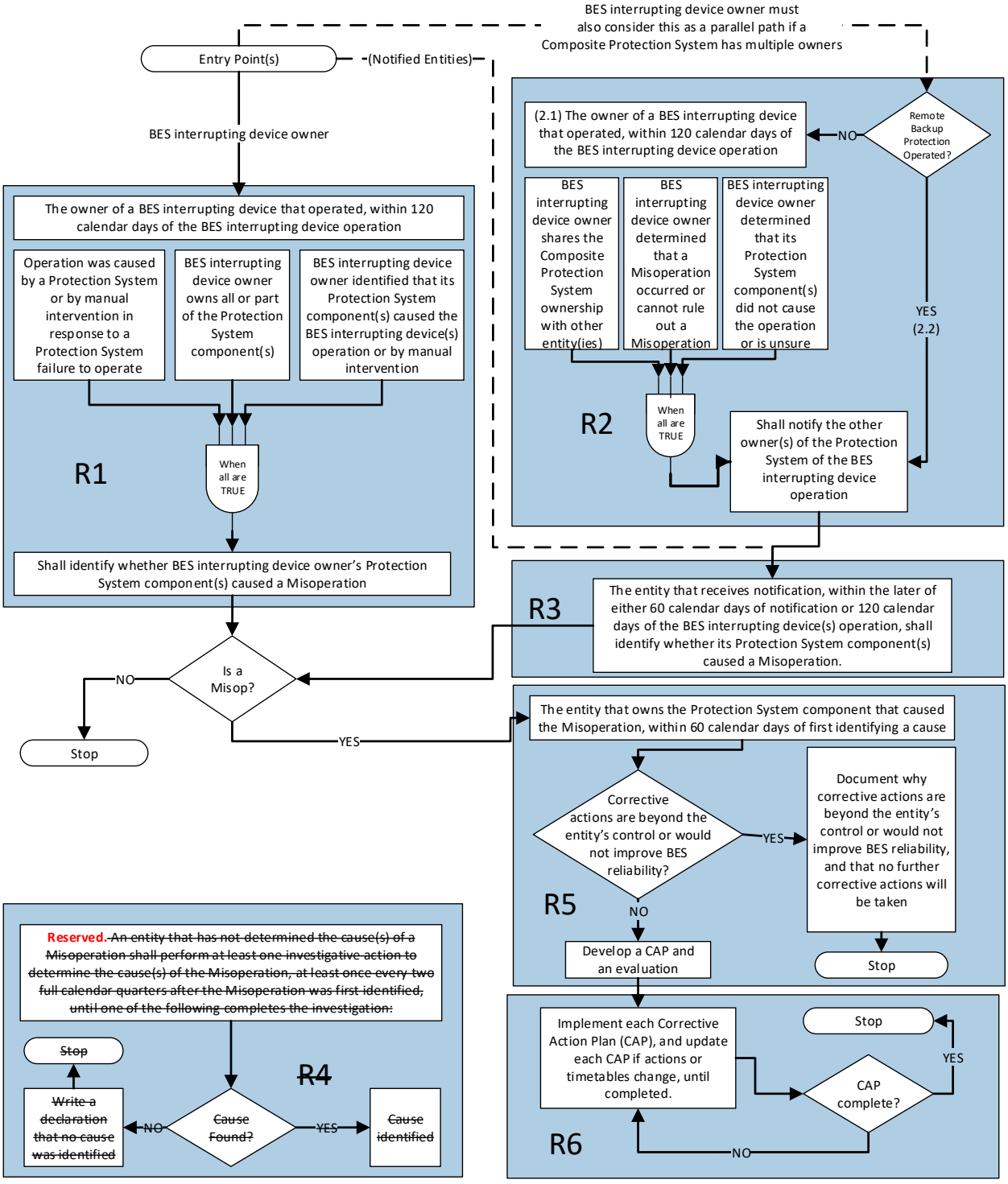
Example R6d: Actions: fault records were provided to the manufacturer on 06/04/2014. The manufacturer responded that the Misoperation was caused by a bug in version 2 firmware, and recommended installing version 3 firmware. Version 3 firmware was installed on 08/12/2014.

Nine of the twelve relays were updated to version 3 firmware on 09/23/2014. The manufacturer provided a subsequent update which was determined to be beneficial for the remaining relays. The remaining three of twelve relays identified as having the version 2 firmware were updated to version 3.01 firmware on 11/10/2014.

CAP completed on 11/10/2014.

The CAP is complete when all of the actions identified within the CAP have been completed.

Process Flow Chart: Below is a graphical representation demonstrating the relationships between Requirements:



Appendix PRC-004-6-QC-1
Specific provisions applicable in Québec for standard
PRC-004-6 – Protection System Misoperation Identification and Correction

This appendix establishes specific provisions for the application of the standard in Québec. Provisions of the standard and of this appendix must be read jointly for comprehension and interpretation purposes. Where the standard and appendix differ, the appendix shall prevail.

A. Introduction

1. Title: No specific provisions.

2. Number: No specific provisions.

3. Purpose: No specific provisions.

4. Applicability:

4.1. Functional Entities

No specific provisions.

4.2. Facilities

Replace all references to Bulk Electric System (BES) with Main Transmission System (RTP), with the exception of 4.2.1.4, which is retired, and 4.2.1.5, which is replaced as follows:

4.2.1.4. [In the French-language context] Subsection 4.2.1.4 is retired given that *plan de défense* (Remedial Action Scheme) is replaced with *automatisme de réseau* to mean the same thing and already included in 4.2.1.3.

4.2.1.5 Protection Systems for individual generating units of Dispersed Power Producing Resources if the aggregate nameplate rating of those RTP Facilities affected by Misoperation does not exceed 75 MVA.

5. Effective date:

5.1.	Adoption of the standard by the Régie de l'énergie:	May 4, 2021
5.2.	Adoption of this appendix by the Régie de l'énergie:	May 4, 2021
5.3.	Effective date of the standard and of this appendix in Québec:	October 1st, 2021
	Implementation date for non-BPS RTP Facilities:	July 1, 2022

B. Requirements and Measures

Replace all references to Bulk Electric System (BES) with Main Transmission System (RTP).

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

In Québec, "Compliance Enforcement Authority" means the Régie de l'énergie in its roles of monitoring and enforcing compliance with respect to the Reliability Standard and to this appendix.

1.2. Evidence Retention

No specific provisions.

1.3. Compliance Monitoring and Assessment Processes

The Régie de l'énergie establishes the monitoring processes used to evaluate data or information for the purpose of determining compliance or non-compliance with the Reliability Standard and with this appendix.

1.4. Additional Compliance Information

No specific provisions.

Violation Severity Levels

Replace all references to Bulk Electric System (BES) with Main Transmission System (RTP).

D. Regional Variances

No specific provisions.

E. Associated Documents

No specific provisions.

Guidelines and Technical Basis

Replace all references to Bulk Electric System (BES) with Main Transmission System (RTP).

Version history

Version	Date	Action	Change tracking
1	May 4, 2021	New appendix adoption (D-2021-058)	New
2	January 19, 2022	Addition of the implementation date for non-BPS RTP Facilities (D-2022-002)	Modification

A. Introduction

1. **Title:** **Protection System, Automatic Reclosing, and Sudden Pressure Relaying Maintenance**

2. **Number: PRC-005-6**

3. **Purpose:** To document and implement programs for the maintenance of all Protection Systems, Automatic Reclosing, and Sudden Pressure Relaying affecting the reliability of the Bulk Electric System (BES) so that they are kept in working order.

4. **Applicability:**

   4.1. Functional Entities:

   4.1.1 Transmission Owner

   4.1.2 Generator Owner

   4.1.3 Distribution Provider

   4.2. Facilities:

   4.2.1 Protection Systems and Sudden Pressure Relaying that are installed for the purpose of detecting Faults on BES Elements (lines, buses, transformers, etc.)

   4.2.2 Protection Systems used for underfrequency load-shedding systems installed per ERO underfrequency load-shedding requirements.

   4.2.3 Protection Systems used for undervoltage load-shedding systems installed to prevent system voltage collapse or voltage instability for BES reliability.

   4.2.4 Protection Systems installed as a Remedial Action Scheme (RAS) for BES reliability.

   4.2.5 Protection Systems and Sudden Pressure Relaying for generator Facilities that are part of the BES, except for generators identified through Inclusion I4 of the BES definition, including:

   4.2.5.1 Protection Systems that act to trip the generator either directly or via lockout or auxiliary tripping relays.

   4.2.5.2 Protection Systems and Sudden Pressure Relaying for generator step-up transformers for generators that are part of the BES.

   4.2.5.3 Protection Systems and Sudden Pressure Relaying for station service or excitation transformers connected to the generator bus of generators which are part of the BES, that act to trip the generator either directly or via lockout or tripping auxiliary relays.

4.2.6 Protection Systems and Sudden Pressure Relaying for the following BES generator Facilities for dispersed power producing resources identified through Inclusion I4 of the BES definition:

4.2.6.1 Protection Systems and Sudden Pressure Relaying for Facilities used in aggregating dispersed BES generation from the point where those resources aggregate to greater than 75 MVA to a common point of connection at 100kV or above.

4.2.7 Automatic Reclosing[1], including:

4.2.7.1 Automatic Reclosing applied on the terminals of Elements connected to the BES bus located at generating plant substations where the total installed gross generating plant capacity is greater than the gross capacity of the largest BES generating unit within the Balancing Authority Area or, if a member of a Reserve Sharing Group, the largest generating unit within the Reserve Sharing Group.[2]

4.2.7.2 Automatic Reclosing applied on the terminals of all BES Elements at substations one bus away from generating plants specified in Section 4.2.7.1 when the substation is less than 10 circuit-miles from the generating plant substation.

4.2.7.3 Automatic Reclosing applied as an integral part of an RAS specified in Section 4.2.4.

5. **Effective Date:** See the Implementation Plan for this standard.

6. **Definitions Used in this Standard:**

Automatic Reclosing – Includes the following Components:

- Reclosing relay
- Supervisory relay(s) or function(s) – relay(s) or function(s) that perform voltage and/or sync check functions that enable or disable operation of the reclosing relay
- Voltage sensing devices associated with the supervisory relay(s) or function(s)

[1] Automatic Reclosing addressed in Section 4.2.7.1 and 4.2.7.2 may be excluded if the equipment owner can demonstrate that a close-in three-phase fault present for twice the normal clearing time (capturing a minimum trip-close-trip time delay) does not result in a total loss of gross generation in the Interconnection exceeding the gross capacity of the largest relevant BES generating unit where the Automatic Reclosing is applied.

[2] The largest BES generating unit within the Balancing Authority Area or the largest generating unit within the Reserve Sharing Group, as applicable, is subject to change. As a result of such a change, the Automatic Reclosing Components subject to the standard could change effective on the date of such change.

- Control circuitry associated with the reclosing relay or supervisory relay(s) or function(s)

Sudden Pressure Relaying – A system that trips an interrupting device(s) to isolate the equipment it is monitoring and includes the following Components:

- Fault pressure relay – a mechanical relay or device that detects rapid changes in gas pressure, oil pressure, or oil flow that are indicative of Faults within liquid-filled, wire-wound equipment
- Control circuitry associated with a fault pressure relay

Unresolved Maintenance Issue – A deficiency identified during a maintenance activity that causes the Component to not meet the intended performance, cannot be corrected during the maintenance interval, and requires follow-up corrective action.

Segment – Components of a consistent design standard, or a particular model or type from a single manufacturer that typically share other common elements. Consistent performance is expected across the entire population of a Segment. A Segment must contain at least sixty (60) individual Components.

Component Type –

- Any one of the five specific elements of a Protection System
- Any one of the four specific elements of Automatic Reclosing
- Any one of the two specific elements of Sudden Pressure Relaying

Component – Any individual discrete piece of equipment included in a Protection System, Automatic Reclosing, or Sudden Pressure Relaying.

Countable Event – A failure of a Component requiring repair or replacement, any condition discovered during the maintenance activities in Tables 1-1 through 1-5, Table 3, Tables 4-1 through 4-3, and Table 5, which requires corrective action or a Protection System Misoperation attributed to hardware failure or calibration failure. Misoperations due to product design errors, software errors, relay settings different from specified settings, Protection System Component, Automatic Reclosing, or Sudden Pressure Relaying configuration or application errors are not included in Countable Events.

B. Requirements and Measures

R1. Each Transmission Owner, Generator Owner, and Distribution Provider shall establish a Protection System Maintenance Program (PSMP) for its Protection Systems, Automatic Reclosing, and Sudden Pressure Relaying identified in Section 4.2, Facilities. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning*]

The PSMP shall:

1.1. Identify which maintenance method (time-based, performance-based per PRC-005 Attachment A, or a combination) is used to address each Protection System, Automatic Reclosing, and Sudden Pressure Relaying Component Type. All batteries associated with the station dc supply Component Type of a Protection System shall be included in a time-based program as described in Table 1-4 and Table 3.

1.2. Include the applicable monitored Component attributes applied to each Protection System, Automatic Reclosing, and Sudden Pressure Relaying Component Type consistent with the maintenance intervals specified in Tables 1-1 through 1-5, Table 2, Table 3, Table 4-1 through 4-3, and Table 5 where monitoring is used to extend the maintenance intervals beyond those specified for unmonitored Protection System, Automatic Reclosing, and Sudden Pressure Relaying Components.

M1. Each Transmission Owner, Generator Owner and Distribution Provider shall have a documented PSMP in accordance with Requirement R1.

For each Protection System, Automatic Reclosing, and Sudden Pressure Relaying Component Type, the documentation shall include the type of maintenance method applied (time-based, performance-based, or a combination of these maintenance methods), and shall include all batteries associated with the station dc supply Component Types in a time-based program as described in Table 1-4 and Table 3. (Part 1.1)

For Component Types that use monitoring to extend the maintenance intervals, the responsible entity(s) shall have evidence for each Protection System, Automatic Reclosing, and Sudden Pressure Relaying Component Type (such as manufacturer's specifications or engineering drawings) of the appropriate monitored Component attributes as specified in Tables 1-1 through 1-5, Table 2, Table 3, Table 4-1 through 4-3, and Table 5. (Part 1.2)

R2. Each Transmission Owner, Generator Owner, and Distribution Provider that uses performance-based maintenance intervals in its PSMP shall follow the procedure established in PRC-005 Attachment A to establish and maintain its performance-based intervals. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M2. Each Transmission Owner, Generator Owner, and Distribution Provider that uses performance-based maintenance intervals shall have evidence that its current performance-based maintenance program(s) is in accordance with Requirement R2, which may include, but is not limited to, Component lists, dated maintenance records, and dated analysis records and results.

R3. Each Transmission Owner, Generator Owner, and Distribution Provider that utilizes time-based maintenance program(s) shall maintain its Protection System, Automatic Reclosing, and Sudden Pressure Relaying Components that are included within the

time-based maintenance program in accordance with the minimum maintenance activities and maximum maintenance intervals prescribed within Tables 1-1 through 1-5, Table 2, Table 3, Table 4-1 through 4-3, and Table 5. *[Violation Risk Factor: High] [Time Horizon: Operations Planning]*

M3. Each Transmission Owner, Generator Owner, and Distribution Provider that utilizes time-based maintenance program(s) shall have evidence that it has maintained its Protection System, Automatic Reclosing, and Sudden Pressure Relaying Components included within its time-based program in accordance with Requirement R3. The evidence may include, but is not limited to, dated maintenance records, dated maintenance summaries, dated check-off lists, dated inspection records, or dated work orders.

R4. Each Transmission Owner, Generator Owner, and Distribution Provider that utilizes performance-based maintenance program(s) in accordance with Requirement R2 shall implement and follow its PSMP for its Protection System, Automatic Reclosing, and Sudden Pressure Relaying Components that are included within the performance-based program(s). *[Violation Risk Factor: High] [Time Horizon: Operations Planning]*

M4. Each Transmission Owner, Generator Owner, and Distribution Provider that utilizes performance-based maintenance intervals in accordance with Requirement R2 shall have evidence that it has implemented the PSMP for the Protection System, Automatic Reclosing, and Sudden Pressure Relaying Components included in its performance-based program in accordance with Requirement R4. The evidence may include, but is not limited to, dated maintenance records, dated maintenance summaries, dated check-off lists, dated inspection records, or dated work orders.

R5. Each Transmission Owner, Generator Owner, and Distribution Provider shall demonstrate efforts to correct identified Unresolved Maintenance Issues. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M5. Each Transmission Owner, Generator Owner, and Distribution Provider shall have evidence that it has undertaken efforts to correct identified Unresolved Maintenance Issues in accordance with Requirement R5. The evidence may include, but is not limited to, work orders, replacement Component orders, invoices, project schedules with completed milestones, return material authorizations (RMAs) or purchase orders.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

As defined in the NERC Rules of Procedure, “Compliance Enforcement Authority” means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Transmission Owner, Generator Owner, and Distribution Provider shall each keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

For Requirement R1, the Transmission Owner, Generator Owner, and Distribution Provider shall each keep its current dated PSMP, as well as any superseded versions since the preceding compliance audit, including the documentation that specifies the type of maintenance program applied for each Protection System, Automatic Reclosing, or Sudden Pressure Relaying Component Type.

For Requirement R2, Requirement R3, and Requirement R4, in cases where the interval of the maintenance activity is longer than the audit cycle, the Transmission Owner, Generator Owner, and Distribution Provider shall each keep documentation of the most recent performance of that maintenance activity for the Protection System, Automatic Reclosing, or Sudden Pressure Relaying Component. In cases where the interval of the maintenance activity is shorter than the audit cycle, documentation of all performances (in accordance with the tables) of that maintenance activity for the Protection System, Automatic Reclosing, or Sudden Pressure Relaying Component since the previous scheduled audit date shall be retained.

For Requirement R5 the Transmission Owner, Generator Owner, and Distribution Provider shall each keep documentation of Unresolved Maintenance Issues identified by the entity since the last audit, including all that were resolved since the last audit.

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Investigations

Self-Reporting

Complaints

1.4. Additional Compliance Information

None

Table of Compliance Elements

Requirement Number	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	The entity's PSMP failed to specify whether one Component Type is being addressed by time-based or performance-based maintenance, or a combination of both (Part 1.1).	The entity's PSMP failed to specify whether two Component Types are being addressed by time-based or performance-based maintenance, or a combination of both (Part 1.1).	The entity's PSMP failed to specify whether three Component Types are being addressed by time-based or performance-based maintenance, or a combination of both. (Part 1.1). OR The entity's PSMP failed to include the applicable monitoring attributes applied to each Component Type consistent with the maintenance intervals specified in Tables 1-1 through 1-5, Table 2, Table 3, Tables 4-1 through 4-3, and Table 5 where monitoring is used to extend the maintenance intervals beyond those specified for unmonitored Components (Part 1.2).	The entity failed to establish a PSMP. OR The entity's PSMP failed to specify whether four or more Component Types are being addressed by time-based or performance-based maintenance, or a combination of both (Part 1.1). OR The entity's PSMP failed to include applicable station batteries in a time-based program (Part 1.1).
R2	The entity uses performance-based maintenance intervals in its PSMP but failed to reduce Countable Events to no more than 4% within three years.	NA	The entity uses performance-based maintenance intervals in its PSMP but failed to reduce Countable Events to no more than 4% within four years.	The entity uses performance-based maintenance intervals in its PSMP but: 1) Failed to establish the technical justification described within Requirement R2 for the initial use of the performance-based PSMP OR 2) Failed to reduce Countable Events to no more than 4% within five years OR

Requirement Number	Lower VSL	Moderate VSL	High VSL	Severe VSL
				3) Maintained a Segment with less than 60 Components OR 4) Failed to: • Annually update the list of Components, OR • Annually perform maintenance on the greater of 5% of the Segment population or 3 Components, OR • Annually analyze the program activities and results for each Segment.
R3	For Components included within a time-based maintenance program, the entity failed to maintain 5% or less of the total Components included within a specific Component Type in accordance with the minimum maintenance activities and maximum maintenance intervals prescribed within Tables 1-1 through 1-5, Table 2, Table 3, Tables 4-1 through 4-3, and Table 5.	For Components included within a time-based maintenance program, the entity failed to maintain more than 5% but 10% or less of the total Components included within a specific Component Type in accordance with the minimum maintenance activities and maximum maintenance intervals prescribed within Tables 1-1 through 1-5, Table 2, Table 3, Tables 4-1 through 4-3, and Table 5.	For Components included within a time-based maintenance program, the entity failed to maintain more than 10% but 15% or less of the total Components included within a specific Component Type in accordance with the minimum maintenance activities and maximum maintenance intervals prescribed within Tables 1-1 through 1-5, Table 2, Table 3, Tables 4-1 through 4-3, and Table 5.	For Components included within a time-based maintenance program, the entity failed to maintain more than 15% of the total Components included within a specific Component Type in accordance with the minimum maintenance activities and maximum maintenance intervals prescribed within Tables 1-1 through 1-5, Table 2, Table 3, Tables 4-1 through 4-3, and Table 5.

Requirement Number	Lower VSL	Moderate VSL	High VSL	Severe VSL
R4	For Components included within a performance-based maintenance program, the entity failed to maintain 5% or less of the annual scheduled maintenance for a specific Component Type in accordance with their performance-based PSMP.	For Components included within a performance-based maintenance program, the entity failed to maintain more than 5% but 10% or less of the annual scheduled maintenance for a specific Component Type in accordance with their performance-based PSMP.	For Components included within a performance-based maintenance program, the entity failed to maintain more than 10% but 15% or less of the annual scheduled maintenance for a specific Component Type in accordance with their performance-based PSMP.	For Components included within a performance-based maintenance program, the entity failed to maintain more than 15% of the annual scheduled maintenance for a specific Component Type in accordance with their performance-based PSMP.
R5	The entity failed to undertake efforts to correct 5 or fewer identified Unresolved Maintenance Issues.	The entity failed to undertake efforts to correct greater than 5 but less than or equal to 10 identified Unresolved Maintenance Issues.	The entity failed to undertake efforts to correct greater than 10 but less than or equal to 15 identified Unresolved Maintenance Issues.	The entity failed to undertake efforts to correct greater than 15 identified Unresolved Maintenance Issues.

D. Regional Variances

None.

E. Interpretations

None.

Supplemental Reference Documents

The following documents present a detailed discussion about determination of maintenance intervals and other useful information regarding establishment of a maintenance program.

1. *Supplementary Reference and FAQ - PRC-005-6 Protection System Maintenance,* Protection System Maintenance and Testing Standard Drafting Team (July 2015)
2. *Considerations for Maintenance and Testing of Auto-reclosing Schemes*, NERC System Analysis and Modeling Subcommittee, and NERC System Protection and Control Subcommittee (November 2012)
3. *Sudden Pressure Relays and Other Devices that Respond to Non-Electrical Quantities – SPCS Input for Standard Development in Response to FERC Order No. 758,* NERC System Protection and Control Subcommittee (December 2013)
4. *Sudden Pressure Relays and Other Devices that Respond to Non-Electrical Quantities* – Supplemental Information to Support Project 2007-17.3: Protection System Maintenance and Testing (October 31, 2014)

Version History

Version	Date	Action	Change Tracking
0	February 8, 2005	Adopted by NERC Board of Trustees	New
1	February 7, 2006	Adopted by NERC Board of Trustees	1. Changed incorrect use of certain hyphens (-) to "en dash" (–) and "em dash (—)." 2. Added "periods" to items where appropriate. Changed "Timeframe" to "Time Frame" in item D, 1.2.
1	March 16, 2007	PRC-005-1 Approved by FERC. Docket No. RM06-16-000	

Version	Date	Action	Change Tracking
1a	February 17, 2011	Adopted by NERC Board of Trustees	Added Appendix 1 - Interpretation regarding applicability of standard to protection of radially connected transformers developed in Project 2009-17
1a	September 26, 2011	Approved by FERC. Docket No. RD11-5-000	
1b	November 5, 2009	Adopted by NERC Board of Trustees	Interpretation of R1, R1.1, and R1.2 developed by Project 2009-10
1b	February 3, 2012	FERC Order approving revised definition of "Protection System"	Per footnote 8 of FERC's order, the definition of "Protection System" supersedes interpretation "b" of PRC-005-1b upon the effective date of the modified definition (i.e., April 1, 2013) *See N. Amer. Elec. Reliability Corp.*, 138 FERC ¶ 61,095 (February 3, 2012).
1b	February 3, 2012	PRC-005-1b Approved by FERC. Docket No. RM10-5-000	
1.1b	May 9, 2012	Adopted by NERC Board of Trustees	Errata change developed by Project 2010-07, clarified inclusion of generator interconnection Facility in Generator Owner's responsibility
1.1b	September 19, 2013	PRC-005-1.1b Approved by FERC. Docket No. RM12-16-000	
2	November 7, 2012	Adopted by NERC Board of Trustees	Project 2007-17 - Complete revision, absorbing maintenance requirements from PRC-005-1.1b, PRC-008-0, PRC-011-0, PRC-017-0

Version	Date	Action	Change Tracking
2	October 17, 2013	Approved by NERC Standards Committee	Errata Change: The Standards Committee approved an errata change to the implementation plan for PRC-005-2 to add the phrase "or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities;" to the second sentence under the "Retirement of Existing Standards" section. (no change to standard version number)
2	December 19, 2013	PRC-005-2 Approved by FERC. Docket No. RM13-7-000	
2	March 7, 2014	Adopted by NERC Board of Trustees	Modified R1 VSL in response to FERC directive (no change to standard version number)
2(i)	November 13, 2014	Adopted by NERC Board of Trustees	Applicability section revised by Project 2014-01 to clarify application of Requirements to BES dispersed power producing resources
2(i)	May 29, 2015	PRC-005-2(i) Approved by FERC. Docket No. RD15-3-000	
2(ii)	November 13, 2014	Adopted by NERC Board of Trustees	Replaced references to Special Protection System and SPS with Remedial Action Scheme and RAS
3	November 7, 2013	Adopted by the NERC Board of Trustees	Revised to address the FERC directive in Order No. 758 to include Automatic Reclosing in maintenance programs

Version	Date	Action	Change Tracking
3	February 12, 2014	Approved by NERC Standards Committee	Errata Change: The Standards Committee approved errata changes to correct capitalization of certain defined terms within the definitions of “Unresolved Maintenance Issue” and “Protection System Maintenance Program”. The changes will be reflected in the definitions section of PRC-005-3 for “Unresolved Maintenance Issue” and in the NERC Glossary of Terms for “Protection System Maintenance Program". (no change to standard version number)
3	March 7, 2014	Adopted by NERC Board of Trustees	Modified R1 VSL in response to FERC directive (no change to standard version number)
3	January 22, 2015	PRC-005-3 Approved by FERC. Docket No. RM14-8-000	
3(i)	November 13, 2014	Adopted by NERC Board of Trustees	Applicability section revised by Project 2014-01 to clarify application of Requirements to BES dispersed power producing resources
3(i)	May 29, 2015	PRC-005-3(i) Approved by FERC. Docket No. RD15-3-000	
3(ii)	November 13, 2014	Adopted by NERC Board of Trustees	Replaced references to Special Protection System and SPS with Remedial Action Scheme and RAS
4	November 13, 2014	Adopted by NERC Board of Trustees	Added Sudden Pressure Relaying in response to FERC Order No. 758
4	Sept 17, 2015	PRC-005-4 Approved by FERC. Docket No. RM15-9-000	

Version	Date	Action	Change Tracking
5	May 7, 2015	Adopted by NERC Board of Trustees	Applicability section revised by Project 2014-01 to clarify application of Requirements to BES dispersed power producing resources.
6	November 5, 2015	Adopted by NERC Board of Trustees	Revised to add supervisory relays, the voltage sensing devices, and the associated control circuitry to Automatic Reclosing in accordance with the directives in FERC Order 803.
6	December 18, 2015	FERC Letter Order approving PRC-005-6. Docket No. RD16-2-000.	

Table 1-1 Component Type - Protective Relay Excluding distributed UFLS and distributed UVLS (see Table 3)		
Component Attributes	**Maximum Maintenance Interval**[3]	**Maintenance Activities**
Any unmonitored protective relay not having all the monitoring attributes of a category below.	6 Calendar Years	For all unmonitored relays: • Verify that settings are as specified For non-microprocessor relays: • Test and, if necessary calibrate For microprocessor relays: • Verify operation of the relay inputs and outputs that are essential to proper functioning of the Protection System. • Verify acceptable measurement of power system input values.
Monitored microprocessor protective relay with the following: • Internal self-diagnosis and alarming (see Table 2). • Voltage and/or current waveform sampling three or more times per power cycle, and conversion of samples to numeric values for measurement calculations by microprocessor electronics. • Alarming for power supply failure (see Table 2).	12 Calendar Years	Verify: • Settings are as specified. • Operation of the relay inputs and outputs that are essential to proper functioning of the Protection System. • Acceptable measurement of power system input values.

[3] For the tables in this standard, a calendar year starts on the first day of a new year (January 1) after a maintenance activity has been completed. For the tables in this standard, a calendar month starts on the first day of the first month after a maintenance activity has been completed.

Table 1-1 Component Type - Protective Relay Excluding distributed UFLS and distributed UVLS (see Table 3)		
Component Attributes	**Maximum Maintenance Interval**[3]	**Maintenance Activities**
Monitored microprocessor protective relay with preceding row attributes and the following: • Ac measurements are continuously verified by comparison to an independent ac measurement source, with alarming for excessive error (See Table 2). • Some or all binary or status inputs and control outputs are monitored by a process that continuously demonstrates ability to perform as designed, with alarming for failure (See Table 2). • Alarming for change of settings (See Table 2).	12 Calendar Years	Verify only the unmonitored relay inputs and outputs that are essential to proper functioning of the Protection System.

Table 1-2 Component Type - Communications Systems Excluding distributed UFLS and distributed UVLS (see Table 3)		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Any unmonitored communications system necessary for correct operation of protective functions, and not having all the monitoring attributes of a category below.	4 Calendar Months	Verify that the communications system is functional.
	6 Calendar Years	Verify that the communications system meets performance criteria pertinent to the communications technology applied (e.g. signal level, reflected power, or data error rate). Verify operation of communications system inputs and outputs that are essential to proper functioning of the Protection System.
Any communications system with continuous monitoring or periodic automated testing for the presence of the channel function, and alarming for loss of function (See Table 2).	12 Calendar Years	Verify that the communications system meets performance criteria pertinent to the communications technology applied (e.g. signal level, reflected power, or data error rate). Verify operation of communications system inputs and outputs that are essential to proper functioning of the Protection System.
Any communications system with all of the following: • Continuous monitoring or periodic automated testing for the performance of the channel using criteria pertinent to the communications technology applied (e.g. signal level, reflected power, or data error rate, and alarming for excessive performance degradation). (See Table 2) • Some or all binary or status inputs and control outputs are monitored by a process that continuously demonstrates ability to perform as designed, with alarming for failure (See Table 2).	12 Calendar Years	Verify only the unmonitored communications system inputs and outputs that are essential to proper functioning of the Protection System

Table 1-3 Component Type - Voltage and Current Sensing Devices Providing Inputs to Protective Relays Excluding distributed UFLS and distributed UVLS (see Table 3)		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Any voltage and current sensing devices not having monitoring attributes of the category below.	12 Calendar Years	Verify that current and voltage signal values are provided to the protective relays.
Voltage and Current Sensing devices connected to microprocessor relays with ac measurements that are continuously verified by comparison of sensing input value, as measured by the microprocessor relay, to an independent ac measurement source, with alarming for unacceptable error or failure (see Table 2).	No periodic maintenance specified	None.

Table 1-4(a) Component Type – Protection System Station dc Supply Using Vented Lead-Acid (VLA) Batteries Excluding distributed UFLS and distributed UVLS (see Table 3) Protection System Station dc supply used only for non-BES interrupting devices for RAS, non-distributed UFLS systems, or non-distributed UVLS systems is excluded (see Table 1-4(e)).		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Protection System Station dc supply using Vented Lead-Acid (VLA) batteries not having monitoring attributes of Table 1-4(f).	4 Calendar Months	Verify: • Station dc supply voltage Inspect: • Electrolyte level • For unintentional grounds
	18 Calendar Months	Verify: • Float voltage of battery charger • Battery continuity • Battery terminal connection resistance • Battery intercell or unit-to-unit connection resistance Inspect: • Cell condition of all individual battery cells where cells are visible – or measure battery cell/unit internal ohmic values where the cells are not visible • Physical condition of battery rack

Table 1-4(a) Component Type – Protection System Station dc Supply Using Vented Lead-Acid (VLA) Batteries Excluding distributed UFLS and distributed UVLS (see Table 3) Protection System Station dc supply used only for non-BES interrupting devices for RAS, non-distributed UFLS systems, or non-distributed UVLS systems is excluded (see Table 1-4(e)).		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
	18 Calendar Months -or- 6 Calendar Years	Verify that the station battery can perform as manufactured by evaluating cell/unit measurements indicative of battery performance (e.g. internal ohmic values or float current) against the station battery baseline. -or- Verify that the station battery can perform as manufactured by conducting a performance or modified performance capacity test of the entire battery bank.

Table 1-4(b) Component Type – Protection System Station dc Supply Using Valve-Regulated Lead-Acid (VRLA) Batteries Excluding distributed UFLS and distributed UVLS (see Table 3) Protection System Station dc supply used only for non-BES interrupting devices for RAS, non-distributed UFLS systems, or non-distributed UVLS systems is excluded (see Table 1-4(e)).		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Protection System Station dc supply with Valve Regulated Lead-Acid (VRLA) batteries not having monitoring attributes of Table 1-4(f).	4 Calendar Months	Verify: • Station dc supply voltage Inspect: • For unintentional grounds
	6 Calendar Months	Inspect: • Condition of all individual units by measuring battery cell/unit internal ohmic values.
	18 Calendar Months	Verify: • Float voltage of battery charger • Battery continuity • Battery terminal connection resistance • Battery intercell or unit-to-unit connection resistance Inspect: • Physical condition of battery rack

Table 1-4(b) Component Type – Protection System Station dc Supply Using Valve-Regulated Lead-Acid (VRLA) Batteries Excluding distributed UFLS and distributed UVLS (see Table 3) Protection System Station dc supply used only for non-BES interrupting devices for RAS, non-distributed UFLS systems, or non-distributed UVLS systems is excluded (see Table 1-4(e)).		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
	6 Calendar Months -or- 3 Calendar Years	Verify that the station battery can perform as manufactured by evaluating cell/unit measurements indicative of battery performance (e.g. internal ohmic values or float current) against the station battery baseline. -or- Verify that the station battery can perform as manufactured by conducting a performance or modified performance capacity test of the entire battery bank.

Table 1-4(c) Component Type – Protection System Station dc Supply Using Nickel-Cadmium (NiCad) Batteries Excluding distributed UFLS and distributed UVLS (see Table 3) Protection System Station dc supply used only for non-BES interrupting devices for RAS, non-distributed UFLS system, or non-distributed UVLS systems is excluded (see Table 1-4(e)).		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Protection System Station dc supply **Nickel-Cadmium (NiCad) batteries** not having monitoring attributes of Table 1-4(f).	4 Calendar Months	Verify: • Station dc supply voltage Inspect: • Electrolyte level • For unintentional grounds
	18 Calendar Months	Verify: • Float voltage of battery charger • Battery continuity • Battery terminal connection resistance • Battery intercell or unit-to-unit connection resistance Inspect: • Cell condition of all individual battery cells. • Physical condition of battery rack

Table 1-4(c) Component Type – Protection System Station dc Supply Using Nickel-Cadmium (NiCad) Batteries Excluding distributed UFLS and distributed UVLS (see Table 3) Protection System Station dc supply used only for non-BES interrupting devices for RAS, non-distributed UFLS system, or non-distributed UVLS systems is excluded (see Table 1-4(e)).		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
	6 Calendar Years	Verify that the station battery can perform as manufactured by conducting a performance or modified performance capacity test of the entire battery bank.

Table 1-4(d) Component Type – Protection System Station dc Supply Using Non Battery Based Energy Storage Excluding distributed UFLS and distributed UVLS (see Table 3) Protection System Station dc supply used only for non-BES interrupting devices for RAS, non-distributed UFLS system, or non-distributed UVLS systems is excluded (see Table 1-4(e)).		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Any Protection System station dc supply not using a battery and not having monitoring attributes of Table 1-4(f).	4 Calendar Months	Verify: • Station dc supply voltage Inspect: • For unintentional grounds
	18 Calendar Months	Inspect: Condition of non-battery based dc supply
	6 Calendar Years	Verify that the dc supply can perform as manufactured when ac power is not present.

Table 1-4(e) Component Type – Protection System Station dc Supply for non-BES Interrupting Devices for RAS, non-distributed UFLS, and non-distributed UVLS systems		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Any Protection System dc supply used for tripping only non-BES interrupting devices as part of a RAS, non-distributed UFLS, or non-distributed UVLS system and not having monitoring attributes of Table 1-4(f).	When control circuits are verified (See Table 1-5)	Verify Station dc supply voltage.

Table 1-4(f) Exclusions for Protection System Station dc Supply Monitoring Devices and Systems		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Any station dc supply with high and low voltage monitoring and alarming of the battery charger voltage to detect charger overvoltage and charger failure (See Table 2).	No periodic maintenance specified	No periodic verification of station dc supply voltage is required.
Any battery based station dc supply with electrolyte level monitoring and alarming in every cell (See Table 2).		No periodic inspection of the electrolyte level for each cell is required.
Any station dc supply with unintentional dc ground monitoring and alarming (See Table 2).		No periodic inspection of unintentional dc grounds is required.
Any station dc supply with charger float voltage monitoring and alarming to ensure correct float voltage is being applied on the station dc supply (See Table 2).		No periodic verification of float voltage of battery charger is required.
Any battery based station dc supply with monitoring and alarming of battery string continuity (See Table 2).		No periodic verification of the battery continuity is required.
Any battery based station dc supply with monitoring and alarming of the intercell and/or terminal connection detail resistance of the entire battery (See Table 2).		No periodic verification of the intercell and terminal connection resistance is required.
Any Valve Regulated Lead-Acid (VRLA) or Vented Lead-Acid (VLA) station battery with internal ohmic value or float current monitoring and alarming, and evaluating present values relative to baseline internal ohmic values for every cell/unit (See Table 2).		No periodic evaluation relative to baseline of battery cell/unit measurements indicative of battery performance is required to verify the station battery can perform as manufactured.
Any Valve Regulated Lead-Acid (VRLA) or Vented Lead-Acid (VLA) station battery with monitoring and alarming of each cell/unit internal ohmic value (See Table 2).		No periodic inspection of the condition of all individual units by measuring battery cell/unit internal ohmic values of a station VRLA or Vented Lead-Acid (VLA) battery is required.

Table 1-5 Component Type - Control Circuitry Associated With Protective Functions Excluding distributed UFLS and distributed UVLS (see Table 3), Automatic Reclosing (see Table 4), and Sudden Pressure Relaying (see Table 5) Note: Table requirements apply to all Control Circuitry Components of Protection Systems, and RAS except as noted.		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Trip coils or actuators of circuit breakers, interrupting devices, or mitigating devices (regardless of any monitoring of the control circuitry).	6 Calendar Years	Verify that each trip coil is able to operate the circuit breaker, interrupting device, or mitigating device.
Electromechanical lockout devices which are directly in a trip path from the protective relay to the interrupting device trip coil (regardless of any monitoring of the control circuitry).	6 Calendar Years	Verify electrical operation of electromechanical lockout devices.
Unmonitored control circuitry associated with RAS. (See Table 4-2(b) for RAS which include Automatic Reclosing.)	12 Calendar Years	Verify all paths of the control circuits essential for proper operation of the RAS.
Unmonitored control circuitry associated with protective functions inclusive of all auxiliary relays.	12 Calendar Years	Verify all paths of the trip circuits inclusive of all auxiliary relays through the trip coil(s) of the circuit breakers or other interrupting devices.
Control circuitry associated with protective functions and/or RAS whose integrity is monitored and alarmed (See Table 2).	No periodic maintenance specified	None.

Table 2 – Alarming Paths and Monitoring In Tables 1-1 through 1-5, Table 3, Tables 4-1 through 4-3, and Table 5 alarm attributes used to justify extended maximum maintenance intervals and/or reduced maintenance activities are subject to the following maintenance requirements		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Any alarm path through which alarms in Tables 1-1 through 1-5, Table 3, Tables 4-1 through 4-3, and Table 5 are conveyed from the alarm origin to the location where corrective action can be initiated, and not having all the attributes of the "Alarm Path with monitoring" category below. Alarms are reported within 24 hours of detection to a location where corrective action can be initiated.	12 Calendar Years	Verify that the alarm path conveys alarm signals to a location where corrective action can be initiated.
Alarm Path with monitoring: The location where corrective action is taken receives an alarm within 24 hours for failure of any portion of the alarming path from the alarm origin to the location where corrective action can be initiated.	No periodic maintenance specified	None.

Table 3 Maintenance Activities and Intervals for distributed UFLS and distributed UVLS Systems		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Any unmonitored protective relay not having all the monitoring attributes of a category below.	6 Calendar Years	Verify that settings are as specified. For non-microprocessor relays: • Test and, if necessary calibrate. For microprocessor relays: • Verify operation of the relay inputs and outputs that are essential to proper functioning of the Protection System. • Verify acceptable measurement of power system input values.
Monitored microprocessor protective relay with the following: • Internal self-diagnosis and alarming (See Table 2). • Voltage and/or current waveform sampling three or more times per power cycle, and conversion of samples to numeric values for measurement calculations by microprocessor electronics. Alarming for power supply failure (See Table 2).	12 Calendar Years	Verify: • Settings are as specified. • Operation of the relay inputs and outputs that are essential to proper functioning of the Protection System. • Acceptable measurement of power system input values.
Monitored microprocessor protective relay with preceding row attributes and the following: • AC measurements are continuously verified by comparison to an independent ac measurement source, with alarming for excessive error (See Table 2).	12 Calendar Years	Verify only the unmonitored relay inputs and outputs that are essential to proper functioning of the Protection System.

Table 3 Maintenance Activities and Intervals for distributed UFLS and distributed UVLS Systems		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
• Some or all binary or status inputs and control outputs are monitored by a process that continuously demonstrates ability to perform as designed, with alarming for failure (See Table 2). Alarming for change of settings (See Table 2).		
Voltage and/or current sensing devices associated with UFLS or UVLS systems.	12 Calendar Years	Verify that current and/or voltage signal values are provided to the protective relays.
Protection System dc supply for tripping non-BES interrupting devices used only for a UFLS or UVLS system.	12 Calendar Years	Verify Protection System dc supply voltage.
Control circuitry between the UFLS or UVLS relays and electromechanical lockout and/or tripping auxiliary devices (excludes non-BES interrupting device trip coils).	12 Calendar Years	Verify the path from the relay to the lockout and/or tripping auxiliary relay (including essential supervisory logic).
Electromechanical lockout and/or tripping auxiliary devices associated only with UFLS or UVLS systems (excludes non-BES interrupting device trip coils).	12 Calendar Years	Verify electrical operation of electromechanical lockout and/or tripping auxiliary devices.
Control circuitry between the electromechanical lockout and/or tripping auxiliary devices and the non-BES interrupting devices in UFLS or UVLS systems, or between UFLS or UVLS relays (with no interposing electromechanical lockout or auxiliary device) and the non-BES interrupting devices (excludes non-BES interrupting device trip coils).	No periodic maintenance specified	None.
Trip coils of non-BES interrupting devices in UFLS or UVLS systems.	No periodic maintenance specified	None.

Table 4-1

Maintenance Activities and Intervals for Automatic Reclosing Components

Component Type – Reclosing and Supervisory Relay

Note: In cases where Components of Automatic Reclosing are common to Components listed in Table 1-1 through 1-5, the Components only need to be tested once during a distinct maintenance interval.

Component Attributes	Maximum Maintenance Interval	Maintenance Activities
Any unmonitored reclosing relay or supervisory relay not having all the monitoring attributes of a category below.	6 Calendar Years	Verify that settings are as specified. For non-microprocessor reclosing or supervisory relays: • Test and, if necessary calibrate For microprocessor reclosing or supervisory relays: • Verify operation of the relay inputs and outputs that are essential to proper functioning of the Automatic Reclosing. For microprocessor supervisory relays: • Verify acceptable measurement of power system input values.
• Monitored microprocessor reclosing relay or supervisory relay with the following: Internal self-diagnosis and alarming (See Table 2). • Alarming for power supply failure (See Table 2). For supervisory relay: • Voltage waveform sampling three or more times per power cycle, and conversion of samples to numeric values for measurement calculations by microprocessor electronics.	12 Calendar Years	Verify: • Settings are as specified. • Operation of the relay inputs and outputs that are essential to proper functioning of the Automatic Reclosing. For supervisory relays: • Verify acceptable measurement of power system input values.

Table 4-1 Maintenance Activities and Intervals for Automatic Reclosing Components Component Type – Reclosing and Supervisory Relay Note: In cases where Components of Automatic Reclosing are common to Components listed in Table 1-1 through 1-5, the Components only need to be tested once during a distinct maintenance interval.		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Monitored microprocessor reclosing relay or supervisory relay with preceding row attributes and the following: • Some or all binary or status inputs and control outputs are monitored by a process that continuously demonstrates ability to perform as designed, with alarming for failure (See Table 2). • Alarming for change of settings (See Table 2). For supervisory relay: • Ac measurements are continuously verified by comparison to an independent ac measurement source, with alarming for excessive error (See Table 2).	12 Calendar Years	Verify only the unmonitored relay inputs and outputs that are essential to proper functioning of the Automatic Reclosing.

Table 4-2(a) Maintenance Activities and Intervals for Automatic Reclosing Components Component Type – Control Circuitry Associated with Reclosing and Supervisory Relays that are NOT an Integral Part of an RAS Note: In cases where Components of Automatic Reclosing are common to Components listed in Table 1-5, the Components only need to be tested once during a distinct maintenance interval.		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Unmonitored Control circuitry associated with Automatic Reclosing that is not an integral part of an RAS.	12 Calendar Years	Verify that Automatic Reclosing, upon initiation, does not issue a premature closing command to the close circuitry.
Control circuitry associated with Automatic Reclosing that is not part of an RAS and is monitored and alarmed for conditions that would result in a premature closing command. (See Table 2)	No periodic maintenance specified	None.

Table 4-2(b) Maintenance Activities and Intervals for Automatic Reclosing Components Component Type – Control Circuitry Associated with Reclosing and Supervisory Relays that ARE an Integral Part of an RAS Note: In cases where Components of Automatic Reclosing are common to Components listed in Table 1-5, the Components only need to be tested once during a distinct maintenance interval.		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Close coils or actuators of circuit breakers or similar devices that are used in conjunction with Automatic Reclosing as part of an RAS (regardless of any monitoring of the control circuitry).	6 Calendar Years	Verify that each close coil or actuator is able to operate the circuit breaker or mitigating device.
Unmonitored close control circuitry associated with Automatic Reclosing used as an integral part of an RAS.	12 Calendar Years	Verify all paths of the control circuits associated with Automatic Reclosing that are essential for proper operation of the RAS.
Control circuitry associated with Automatic Reclosing that is an integral part of an RAS whose integrity is monitored and alarmed. (See Table 2)	No periodic maintenance specified	None.

Table 4-3 Maintenance Activities and Intervals for Automatic Reclosing Components Component Type – Voltage Sensing Devices Associated with Supervisory Relays Note: In cases where Components of Automatic Reclosing are common to Components listed in Table 1-3, the Components only need to be tested once during a distinct maintenance interval.		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Any voltage sensing devices not having monitoring attributes of the category below.	12 Calendar Years	Verify that voltage signal values are provided to the supervisory relays.
Voltage sensing devices that are connected to microprocessor supervisory relays with ac measurements that are continuously verified by comparison of sensing input value, as measured by the microprocessor relay, to an independent ac measurement source, with alarming for unacceptable error or failure. (See Table 2)	No periodic maintenance specified	None.

Table 5 Maintenance Activities and Intervals for Sudden Pressure Relaying Note: In cases where Components of Sudden Pressure Relaying are common to Components listed in Table 1-5, the Components only need to be tested once during a distinct maintenance interval.		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Any fault pressure relay.	6 Calendar Years	Verify the pressure or flow sensing mechanism is operable.
Electromechanical lockout devices which are directly in a trip path from the fault pressure relay to the interrupting device trip coil (regardless of any monitoring of the control circuitry).	6 Calendar Years	Verify electrical operation of electromechanical lockout devices.
Unmonitored control circuitry associated with Sudden Pressure Relaying.	12 Calendar Years	Verify all paths of the trip circuits inclusive of all auxiliary relays through the trip coil(s) of the circuit breakers or other interrupting devices.
Control circuitry associated with Sudden Pressure Relaying whose integrity is monitored and alarmed (See Table 2).	No periodic maintenance specified	None.

PRC-005 — Attachment A

Criteria for a Performance-Based Protection System Maintenance Program

Purpose: To establish a technical basis for initial and continued use of a performance-based Protection System Maintenance Program (PSMP).

To establish the technical justification for the initial use of a performance-based PSMP:

1. Develop a list with a description of Components included in each designated Segment, with a minimum Segment population of 60 Components.
2. Maintain the Components in each Segment according to the time-based maximum allowable intervals established in Tables 1-1 through 1-5, Table 3, Tables 4-1 through 4-3, and Table 5 until results of maintenance activities for the Segment are available for a minimum of 30 individual Components of the Segment.
3. Document the maintenance program activities and results for each Segment, including maintenance dates and Countable Events for each included Component.
4. Analyze the maintenance program activities and results for each Segment to determine the overall performance of the Segment and develop maintenance intervals.
5. Determine the maximum allowable maintenance interval for each Segment such that the Segment experiences Countable Events on no more than 4% of the Components within the Segment, for the greater of either the last 30 Components maintained or all Components maintained in the previous year.

To maintain the technical justification for the ongoing use of a performance-based PSMP:

1. At least annually, update the list of Components and Segments and/or description if any changes occur within the Segment.
2. Perform maintenance on the greater of 5% of the Components (addressed in the performance based PSMP) in each Segment or 3 individual Components within the Segment in each year.
3. For the prior year, analyze the maintenance program activities and results for each Segment to determine the overall performance of the Segment.
4. Using the prior year's data, determine the maximum allowable maintenance interval for each Segment such that the Segment experiences Countable Events on no more than 4% of the Components within the Segment, for the greater of either the last 30 Components maintained or all Components maintained in the previous year.

If the Components in a Segment maintained through a performance-based PSMP experience 4% or more Countable Events, develop, document, and implement an action plan to reduce the Countable Events to less than 4% of the Segment population within 3 years.

Rationale:

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for revisions to Automatic Reclosing:
To address directives from FERC Order No. 803 addressing Automatic Reclosing, the definition for Automatic Reclosing was revised to add supervisory relays, the associated voltage sensing devices, and the associated control circuitry.

Rationale for revisions to Component Type:
With the revision of the definition of Automatic Reclosing, there are four specific elements of this definition, rather than two as stated in the prior version.

Appendix PRC-005-6-QC-1

Specific provisions applicable in Québec for standard PRC-005-6 – Protection System, Automatic Reclosing, and Sudden Pressure Relaying Maintenance

This appendix establishes specific provisions for the application of the standard in Québec. Provisions of the standard and of this appendix must be read jointly for comprehension and interpretation purposes. Where the standard and appendix differ, the appendix shall prevail.

A. Introduction

1. Title: No specific provisions.

2. Number: No specific provisions.

3. Purpose: No specific provisions.

4. Applicability:

4.1. Functional Entities

No specific provisions.

4.2. Facilities

Replace all references to "Bulk Electric System (BES)" with "Main Transmission System (RTP)", including the footnotes 1 and 2.

The subsections of Section 4.2 apply, with the exception of the following subsections, which take precedence:

4.2.2. Protection Systems for underfrequency load shedding (UFLS) systems.

4.2.5. Protection Systems and Sudden Pressure Relaying for generator Facilities that are part of the RTP, except for Dispersed Power Producing Resources, including the following:

4.2.6. Protection Systems and Sudden Pressure Relaying for the following RTP generation Facilities in the case of Dispersed Power Producing Resources:

4.2.6.1 Protection Systems and Sudden Pressure Relaying for Facilities mentioned in point b) of the Dispersed Power Producing Resources definition in the Glossary of Terms Used in NERC Reliability Standards (the "Glossary").

5. Effective date:

5.1.	Adoption of the standard by the Régie de l'énergie:	December 11, 2020
5.2.	Adoption of this appendix by the Régie de l'énergie:	December 11, 2020
5.3.	Effective date of the standard and of this appendix in Québec:	April 1, 2021

BPS Protection Systems that were already covered by PRC-005-2: the implementations dates for the Requirements are those of PRC-005-2 (see tables 1a and 1b of this Appendix).

RTP Protection Systems that were not included in PRC-005-2: the implementation dates for the Requirements are specified in tables 2a and 2b of this Appendix. These tables consider not only the equipment that is now covered because it is part of the RTP (including the BPS), but also all Elements newly covered by PRC-005-6, i.e., Automatic Reclosing, Sudden Pressure Relaying, Protection Systems installed as Remedial Action Schemes (RAS) and not

corresponding to the definition of SPS, and the Protection Systems of Dispersed Power Producing Resources.

Table 1a – Implementation dates of PRC-005-2, applicable only to BPS

Requirements	Implementation dates in Québec
R1, R2, R5	January 1, 2017
R3, R4	See table below

Table 1b – Implementation dates of PRC-005-2 for requirements R3 and R4

Maximum Maintenance Interval (tables 1 to 3)	Applicability	Implementation dates in Québec
≤1 year	100% maintenance required	January 1, 2017
1 year to 2 years	100% maintenance required	April 1, 2017
Up to 3 years	30% maintenance required	April 1, 2017
	60% maintenance required	April 1, 2017
	100% maintenance required	April 1, 2018
Up to 6 years	30% maintenance required	April 1, 2017
	60% maintenance required	April 1, 2019
	100% maintenance required	April 1, 2021
Up to 12 years	30% maintenance required	April 1, 2019
	60% maintenance required	April 1, 2023
	100% maintenance required	April 1, 2027

Table 2a – Implementation dates for PRC-005-6, applicable to the RTP and now covering Automatic Reclosing, Sudden Pressure Relaying, Protection Systems installed as Remedial Action Schemes (RAS), but not included in the definition of SPS, and Protection Systems for Dispersed Power Producing Resources

Requirements	Implementation dates in Québec
R1, R2 and R5	October 1, 2022
R3 and R4	see table below

Table 2b – Implementation dates of PRC-005-6 for requirements R3 and R4

Maximum Maintenance Interval (tables 1 to 5)	Applicability	Implementation dates in Québec
≤1 year	100% maintenance required	April 1, 2023
1 year to 2 years	100% maintenance required	July 1, 2023
Up to 3 years	30% maintenance required	July 1, 2023
	60% maintenance required	July 1, 2024
	100% maintenance required	August 1, 2025
Up to 6 years	30% maintenance required	April 1, 2024
	60% maintenance required	April 1, 2025
	100% maintenance required	April 1, 2027
Up to 12 years	30% maintenance required	April 1, 2026
	60% maintenance required	October 1, 2028
	100% maintenance required	April 1, 2033

6. Definitions Used in this Standard

No specific provisions.

B. Requirements and Measures

No specific provisions.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

In Québec, "Compliance Enforcement Authority" means the Régie de l'énergie in its roles of monitoring and enforcing compliance with respect to the Reliability Standard and to this appendix.

1.2. Evidence Retention

No specific provisions.

1.3. Compliance Monitoring and Assessment Processes

The Régie de l'énergie establishes the monitoring processes used to evaluate data or information for the purpose of determining compliance or non-compliance with the Reliability Standard and with this appendix.

1.4. Additional Compliance Information

No specific provisions.

Appendix PRC-005-6-QC-1

Specific provisions applicable in Québec for standard PRC-005-6 – Protection System, Automatic Reclosing, and Sudden Pressure Relaying Maintenance

Table of Compliance Elements

No specific provisions.

D. Regional Variances

No specific provisions.

E. Interpretations

No specific provisions.

Supplemental Reference Documents

No specific provisions.

Tables 1-1 to 1-5

Replace all references to the term “non-BES” with the term “non-RTP.”

Table 2

No specific provisions.

Table 3

Replace all references to the term “non-BES” with the term “non-RTP.”

Tables 4-1 to 5

No specific provisions.

Attachment A

No specific provisions.

Version history

Version	Date	Action	Change tracking
1	December 11, 2020	New appendix	New

A. Introduction

1. **Title:** **Automatic Underfrequency Load Shedding**

2. **Number:** PRC-006-5

3. **Purpose:** To establish design and documentation requirements for automatic underfrequency load shedding (UFLS) programs to arrest declining frequency, assist recovery of frequency following underfrequency events and provide last resort system preservation measures.

4. **Applicability:**

   4.1. Planning Coordinators

   4.2. UFLS entities shall mean all entities that are responsible for the ownership, operation, or control of UFLS equipment as required by the UFLS program established by the Planning Coordinators. Such entities may include one or more of the following:

   4.2.1 Transmission Owners

   4.2.2 Distribution Providers

   4.2.3 UFLS-Only Distribution Providers

   4.3. Transmission Owners that own Elements identified in the UFLS program established by the Planning Coordinators.

5. **Effective Date:**

   See Implementation Plan

B. Requirements and Measures

R1. Each Planning Coordinator shall develop and document criteria, including consideration of historical events and system studies, to select portions of the Bulk Electric System (BES), including interconnected portions of the BES in adjacent Planning Coordinator areas and Regional Entity areas that may form islands. *[VRF: Medium][Time Horizon: Long-term Planning]*

M1. Each Planning Coordinator shall have evidence such as reports, or other documentation of its criteria to select portions of the Bulk Electric System that may form islands including how system studies and historical events were considered to develop the criteria per Requirement R1.

R2. Each Planning Coordinator shall identify one or more islands to serve as a basis for designing its UFLS program including: *[VRF: Medium][Time Horizon: Long-term Planning]*

2.1. Those islands selected by applying the criteria in Requirement R1, and

2.2. Any portions of the BES designed to detach from the Interconnection (planned islands) as a result of the operation of a relay scheme or Special Protection System, and

2.3. A single island that includes all portions of the BES in either the Regional Entity area or the Interconnection in which the Planning Coordinator's area resides. If a Planning Coordinator's area resides in multiple Regional Entity areas, each of those Regional Entity areas shall be identified as an island. Planning Coordinators may adjust island boundaries to differ from Regional Entity area boundaries by mutual consent where necessary for the sole purpose of producing contiguous regional islands more suitable for simulation.

M2. Each Planning Coordinator shall have evidence such as reports, memorandums, e-mails, or other documentation supporting its identification of an island(s) as a basis for designing a UFLS program that meet the criteria in Requirement R2, Parts 2.1 through 2.3.

R3. Each Planning Coordinator shall develop a UFLS program, including notification of and a schedule for implementation by UFLS entities within its area, that meets the following performance characteristics in simulations of underfrequency conditions resulting from an imbalance scenario, where an imbalance = [(load — actual generation output) / (load)], of up to 25 percent within the identified island(s). *[VRF: High][Time Horizon: Long-term Planning]*

3.1. Frequency shall remain above the Underfrequency Performance Characteristic curve in PRC-006-5 - Attachment 1, either for 60 seconds or until a steady-state condition between 59.3 Hz and 60.7 Hz is reached, and

3.2. Frequency shall remain below the Overfrequency Performance Characteristic curve in PRC-006-5 - Attachment 1, either for 60 seconds or until a steady-state condition between 59.3 Hz and 60.7 Hz is reached, and

3.3. Volts per Hz (V/Hz) shall not exceed 1.18 per unit for longer than two seconds cumulatively per simulated event, and shall not exceed 1.10 per unit for longer than 45 seconds cumulatively per simulated event at each generator bus and generator step-up transformer high-side bus associated with each of the following:

- Individual generating units greater than 20 MVA (gross nameplate rating) directly connected to the BES
- Generating plants/facilities greater than 75 MVA (gross aggregate nameplate rating) directly connected to the BES
- Facilities consisting of one or more units connected to the BES at a common bus with total generation above 75 MVA gross nameplate rating.

M3. Each Planning Coordinator shall have evidence such as reports, memorandums, e-mails, program plans, or other documentation of its UFLS program, including the

notification of the UFLS entities of implementation schedule, that meet the criteria in Requirement R3, Parts 3.1 through 3.3.

R4. Each Planning Coordinator shall conduct and document a UFLS design assessment at least once every five years that determines through dynamic simulation whether the UFLS program design meets the performance characteristics in Requirement R3 for each island identified in Requirement R2. The simulation shall model each of the following: *[VRF: High][Time Horizon: Long-term Planning]*

4.1. Underfrequency trip settings of individual generating units greater than 20 MVA (gross nameplate rating) directly connected to the BES that trip above the Generator Underfrequency Trip Modeling curve in PRC-006-5 - Attachment 1.

4.2. Underfrequency trip settings of generating plants/facilities greater than 75 MVA (gross aggregate nameplate rating) directly connected to the BES that trip above the Generator Underfrequency Trip Modeling curve in PRC-006-5 - Attachment 1.

4.3. Underfrequency trip settings of any facility consisting of one or more units connected to the BES at a common bus with total generation above 75 MVA (gross nameplate rating) that trip above the Generator Underfrequency Trip Modeling curve in PRC-006-5 - Attachment 1.

4.4. Overfrequency trip settings of individual generating units greater than 20 MVA (gross nameplate rating) directly connected to the BES that trip below the Generator Overfrequency Trip Modeling curve in PRC-006-5 — Attachment 1.

4.5. Overfrequency trip settings of generating plants/facilities greater than 75 MVA (gross aggregate nameplate rating) directly connected to the BES that trip below the Generator Overfrequency Trip Modeling curve in PRC-006-5 — Attachment 1.

4.6. Overfrequency trip settings of any facility consisting of one or more units connected to the BES at a common bus with total generation above 75 MVA (gross nameplate rating) that trip below the Generator Overfrequency Trip Modeling curve in PRC-006-5 — Attachment 1.

4.7. Any automatic Load restoration that impacts frequency stabilization and operates within the duration of the simulations run for the assessment.

M4. Each Planning Coordinator shall have dated evidence such as reports, dynamic simulation models and results, or other dated documentation of its UFLS design assessment that demonstrates it meets Requirement R4, Parts 4.1 through 4.7.

R5. Each Planning Coordinator, whose area or portions of whose area is part of an island identified by it or another Planning Coordinator which includes multiple Planning Coordinator areas or portions of those areas, shall coordinate its UFLS program design with all other Planning Coordinators whose areas or portions of whose areas are also part of the same identified island through one of the following: *[VRF: High][Time Horizon: Long-term Planning]*

- Develop a common UFLS program design and schedule for implementation per Requirement R3 among the Planning Coordinators whose areas or portions of whose areas are part of the same identified island, or
- Conduct a joint UFLS design assessment per Requirement R4 among the Planning Coordinators whose areas or portions of whose areas are part of the same identified island, or
- Conduct an independent UFLS design assessment per Requirement R4 for the identified island, and in the event the UFLS design assessment fails to meet Requirement R3, identify modifications to the UFLS program(s) to meet Requirement R3 and report these modifications as recommendations to the other Planning Coordinators whose areas or portions of whose areas are also part of the same identified island and the ERO.

M5. Each Planning Coordinator, whose area or portions of whose area is part of an island identified by it or another Planning Coordinator which includes multiple Planning Coordinator areas or portions of those areas, shall have dated evidence such as joint UFLS program design documents, reports describing a joint UFLS design assessment, letters that include recommendations, or other dated documentation demonstrating that it coordinated its UFLS program design with all other Planning Coordinators whose areas or portions of whose areas are also part of the same identified island per Requirement R5.

R6. Each Planning Coordinator shall maintain a UFLS database containing data necessary to model its UFLS program for use in event analyses and assessments of the UFLS program at least once each calendar year, with no more than 15 months between maintenance activities. *[VRF: Lower][Time Horizon: Long-term Planning]*

M6. Each Planning Coordinator shall have dated evidence such as a UFLS database, data requests, data input forms, or other dated documentation to show that it maintained a UFLS database for use in event analyses and assessments of the UFLS program per Requirement R6 at least once each calendar year, with no more than 15 months between maintenance activities.

R7. Each Planning Coordinator shall provide its UFLS database containing data necessary to model its UFLS program to other Planning Coordinators within its Interconnection within 30 calendar days of a request. *[VRF: Lower][Time Horizon: Long-term Planning]*

M7. Each Planning Coordinator shall have dated evidence such as letters, memorandums, e-mails or other dated documentation that it provided their UFLS database to other Planning Coordinators within their Interconnection within 30 calendar days of a request per Requirement R7.

R8. Each UFLS entity shall provide data to its Planning Coordinator(s) according to the format and schedule specified by the Planning Coordinator(s) to support maintenance of each Planning Coordinator's UFLS database. *[VRF: Lower][Time Horizon: Long-term Planning]*

M8. Each UFLS Entity shall have dated evidence such as responses to data requests, spreadsheets, letters or other dated documentation that it provided data to its Planning Coordinator according to the format and schedule specified by the Planning Coordinator to support maintenance of the UFLS database per Requirement R8.

R9. Each UFLS entity shall provide automatic tripping of Load in accordance with the UFLS program design and schedule for implementation, including any Corrective Action Plan, as determined by its Planning Coordinator(s) in each Planning Coordinator area in which it owns assets. *[VRF: High][Time Horizon: Long-term Planning]*

M9. Each UFLS Entity shall have dated evidence such as spreadsheets summarizing feeder load armed with UFLS relays, spreadsheets with UFLS relay settings, or other dated documentation that it provided automatic tripping of load in accordance with the UFLS program design and schedule for implementation, including any Corrective Action Plan, per Requirement R9.

R10. Each Transmission Owner shall provide automatic switching of its existing capacitor banks, Transmission Lines, and reactors to control over-voltage as a result of underfrequency load shedding if required by the UFLS program and schedule for implementation, including any Corrective Action Plan, as determined by the Planning Coordinator(s) in each Planning Coordinator area in which the Transmission Owner owns transmission. *[VRF: High][Time Horizon: Long-term Planning]*

M10. Each Transmission Owner shall have dated evidence such as relay settings, tripping logic or other dated documentation that it provided automatic switching of its existing capacitor banks, Transmission Lines, and reactors in order to control over-voltage as a result of underfrequency load shedding if required by the UFLS program and schedule for implementation, including any Corrective Action Plan, per Requirement R10.

R11. Each Planning Coordinator, in whose area a BES islanding event results in system frequency excursions below the initializing set points of the UFLS program, shall conduct and document an assessment of the event within one year of event actuation to evaluate: *[VRF: Medium][Time Horizon: Operations Assessment]*

11.1. The performance of the UFLS equipment,

11.2. The effectiveness of the UFLS program.

M11. Each Planning Coordinator shall have dated evidence such as reports, data gathered from an historical event, or other dated documentation to show that it conducted an event assessment of the performance of the UFLS equipment and the effectiveness of the UFLS program per Requirement R11.

R12. Each Planning Coordinator, in whose islanding event assessment (per R11) UFLS program deficiencies are identified, shall conduct and document a UFLS design assessment to consider the identified deficiencies within two years of event actuation. *[VRF: Medium][Time Horizon: Operations Assessment]*

M12. Each Planning Coordinator shall have dated evidence such as reports, data gathered from an historical event, or other dated documentation to show that it conducted a UFLS design assessment per Requirements R12 and R4 if UFLS program deficiencies are identified in R11.

R13. Each Planning Coordinator, in whose area a BES islanding event occurred that also included the area(s) or portions of area(s) of other Planning Coordinator(s) in the same islanding event and that resulted in system frequency excursions below the initializing set points of the UFLS program, shall coordinate its event assessment (in accordance with Requirement R11) with all other Planning Coordinators whose areas or portions of whose areas were also included in the same islanding event through one of the following: *[VRF: Medium][Time Horizon: Operations Assessment]*

- Conduct a joint event assessment per Requirement R11 among the Planning Coordinators whose areas or portions of whose areas were included in the same islanding event, or
- Conduct an independent event assessment per Requirement R11 that reaches conclusions and recommendations consistent with those of the event assessments of the other Planning Coordinators whose areas or portions of whose areas were included in the same islanding event, or
- Conduct an independent event assessment per Requirement R11 and where the assessment fails to reach conclusions and recommendations consistent with those of the event assessments of the other Planning Coordinators whose areas or portions of whose areas were included in the same islanding event, identify differences in the assessments that likely resulted in the differences in the conclusions and recommendations and report these differences to the other Planning Coordinators whose areas or portions of whose areas were included in the same islanding event and the ERO.

M13. Each Planning Coordinator, in whose area a BES islanding event occurred that also included the area(s) or portions of area(s) of other Planning Coordinator(s) in the same islanding event and that resulted in system frequency excursions below the initializing set points of the UFLS program, shall have dated evidence such as a joint assessment report, independent assessment reports and letters describing likely reasons for differences in conclusions and recommendations, or other dated documentation demonstrating it coordinated its event assessment (per Requirement R11) with all other Planning Coordinator(s) whose areas or portions of whose areas were also included in the same islanding event per Requirement R13.

R14. Each Planning Coordinator shall respond to written comments submitted by UFLS entities and Transmission Owners within its Planning Coordinator area following a comment period and before finalizing its UFLS program, indicating in the written response to comments whether changes will be made or reasons why changes will not be made to the following *[VRF: Lower][Time Horizon: Long-term Planning]*:

14.1. UFLS program, including a schedule for implementation

14.2. UFLS design assessment

14.3. Format and schedule of UFLS data submittal

M14. Each Planning Coordinator shall have dated evidence of responses, such as e-mails and letters, to written comments submitted by UFLS entities and Transmission Owners within its Planning Coordinator area following a comment period and before finalizing its UFLS program per Requirement R14.

R15. Each Planning Coordinator that conducts a UFLS design assessment under Requirement R4, R5, or R12 and determines that the UFLS program does not meet the performance characteristics in Requirement R3, shall develop a Corrective Action Plan and a schedule for implementation by the UFLS entities within its area. *[VRF: High][Time Horizon: Long-term Planning]*

15.1. For UFLS design assessments performed under Requirement R4 or R5, the Corrective Action Plan shall be developed within the five-year time frame identified in Requirement R4.

15.2. For UFLS design assessments performed under Requirement R12, the Corrective Action Plan shall be developed within the two-year time frame identified in Requirement R12.

M15. Each Planning Coordinator that conducts a UFLS design assessment under Requirement R4, R5, or R12 and determines that the UFLS program does not meet the performance characteristics in Requirement R3, shall have a dated Corrective Action Plan and a schedule for implementation by the UFLS entities within its area, that was developed within the time frame identified in Part 15.1 or 15.2.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention

Each Planning Coordinator and UFLS entity shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation:

- Each Planning Coordinator shall retain the current evidence of Requirements R1, R2, R3, R4, R5, R12, R14, and R15, Measures M1, M2, M3, M4, M5, M12, M14, and M15 as well as any evidence necessary to show compliance since the last compliance audit.
- Each Planning Coordinator shall retain the current evidence of UFLS database update in accordance with Requirement R6, Measure M6, and evidence of the prior year's UFLS database update.
- Each Planning Coordinator shall retain evidence of any UFLS database transmittal to another Planning Coordinator since the last compliance audit in accordance with Requirement R7, Measure M7.
- Each UFLS entity shall retain evidence of UFLS data transmittal to the Planning Coordinator(s) since the last compliance audit in accordance with Requirement R8, Measure M8.
- Each UFLS entity shall retain the current evidence of adherence with the UFLS program in accordance with Requirement R9, Measure M9, and evidence of adherence since the last compliance audit.
- Transmission Owner shall retain the current evidence of adherence with the UFLS program in accordance with Requirement R10, Measure M10, and evidence of adherence since the last compliance audit.
- Each Planning Coordinator shall retain evidence of Requirements R11, and R13, and Measures M11, and M13 for 6 calendar years.

If a Planning Coordinator or UFLS entity is found non-compliant, it shall keep information related to the non-compliance until found compliant or for the retention period specified above, whichever is longer.

The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audit

Self-Certification

Spot Checking

Compliance Violation Investigation

Self-Reporting

Complaints

1.4. Additional Compliance Information

None

Violation Severity Levels

R #	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	N/A	The Planning Coordinator developed and documented criteria but failed to include the consideration of historical events, to select portions of the BES, including interconnected portions of the BES in adjacent Planning Coordinator areas and Regional Entity areas that may form islands. OR The Planning Coordinator developed and documented criteria but failed to include the consideration of system studies, to select portions of the BES, including interconnected portions of the BES in adjacent Planning Coordinator areas and Regional Entity areas, that may form islands.	The Planning Coordinator developed and documented criteria but failed to include the consideration of historical events and system studies, to select portions of the BES, including interconnected portions of the BES in adjacent Planning Coordinator areas and Regional Entity areas, that may form islands.	The Planning Coordinator failed to develop and document criteria to select portions of the BES, including interconnected portions of the BES in adjacent Planning Coordinator areas and Regional Entity areas, that may form islands.
R2	N/A	The Planning Coordinator identified an island(s) to	The Planning Coordinator identified an island(s) to serve	The Planning Coordinator identified an island(s) to serve

R #	Lower VSL	Moderate VSL	High VSL	Severe VSL
		serve as a basis for designing its UFLS program but failed to include one (1) of the Parts as specified in Requirement R2, Parts 2.1, 2.2, or 2.3.	as a basis for designing its UFLS program but failed to include two (2) of the Parts as specified in Requirement R2, Parts 2.1, 2.2, or 2.3.	as a basis for designing its UFLS program but failed to include all of the Parts as specified in Requirement R2, Parts 2.1, 2.2, or 2.3. OR The Planning Coordinator failed to identify any island(s) to serve as a basis for designing its UFLS program.
R3	N/A	The Planning Coordinator developed a UFLS program, including notification of and a schedule for implementation by UFLS entities within its area where imbalance = [(load — actual generation output) / (load)], of up to 25 percent within the identified island(s)., but failed to meet one (1) of the performance characteristic in Requirement R3, Parts 3.1, 3.2, or 3.3 in simulations of underfrequency conditions.	The Planning Coordinator developed a UFLS program including notification of and a schedule for implementation by UFLS entities within its area where imbalance = [(load — actual generation output) / (load)], of up to 25 percent within the identified island(s)., but failed to meet two (2) of the performance characteristic in Requirement R3, Parts 3.1, 3.2, or 3.3 in simulations of underfrequency conditions.	The Planning Coordinator developed a UFLS program including notification of and a schedule for implementation by UFLS entities within its area where imbalance = [(load — actual generation output) / (load)], of up to 25 percent within the identified island(s).,but failed to meet all the performance characteristic in Requirement R3, Parts 3.1, 3.2, and 3.3 in simulations of underfrequency conditions. OR The Planning Coordinator failed to develop a UFLS program

R #	Lower VSL	Moderate VSL	High VSL	Severe VSL
				including notification of and a schedule for implementation by UFLS entities within its area
R4	The Planning Coordinator conducted and documented a UFLS assessment at least once every five years that determined through dynamic simulation whether the UFLS program design met the performance characteristics in Requirement R3 for each island identified in Requirement R2 but the simulation failed to include one (1) of the items as specified in Requirement R4, Parts 4.1 through 4.7.	The Planning Coordinator conducted and documented a UFLS assessment at least once every five years that determined through dynamic simulation whether the UFLS program design met the performance characteristics in Requirement R3 for each island identified in Requirement R2 but the simulation failed to include two (2) of the items as specified in Requirement R4, Parts 4.1 through 4.7.	The Planning Coordinator conducted and documented a UFLS assessment at least once every five years that determined through dynamic simulation whether the UFLS program design met the performance characteristics in Requirement R3 for each island identified in Requirement R2 but the simulation failed to include three (3) of the items as specified in Requirement R4, Parts 4.1 through 4.7.	The Planning Coordinator conducted and documented a UFLS assessment at least once every five years that determined through dynamic simulation whether the UFLS program design met the performance characteristics in Requirement R3 but simulation failed to include four (4) or more of the items as specified in Requirement R4, Parts 4.1 through 4.7. OR The Planning Coordinator failed to conduct and document a UFLS assessment at least once every five years that determines through dynamic simulation whether the UFLS program design meets the performance characteristics in Requirement R3 for each island identified in Requirement R2

R #	Lower VSL	Moderate VSL	High VSL	Severe VSL
R5	N/A	N/A	N/A	The Planning Coordinator, whose area or portions of whose area is part of an island identified by it or another Planning Coordinator which includes multiple Planning Coordinator areas or portions of those areas, failed to coordinate its UFLS program design through one of the manners described in Requirement R5.
R6	N/A	N/A	N/A	The Planning Coordinator failed to maintain a UFLS database for use in event analyses and assessments of the UFLS program at least once each calendar year, with no more than 15 months between maintenance activities.
R7	The Planning Coordinator provided its UFLS database to other Planning Coordinators more than 30 calendar days and up to and including 40 calendar days following the request.	The Planning Coordinator provided its UFLS database to other Planning Coordinators more than 40 calendar days but less than and including 50 calendar days following the request.	The Planning Coordinator provided its UFLS database to other Planning Coordinators more than 50 calendar days but less than and including 60 calendar days following the request.	The Planning Coordinator provided its UFLS database to other Planning Coordinators more than 60 calendar days following the request. OR

R #	Lower VSL	Moderate VSL	High VSL	Severe VSL
				The Planning Coordinator failed to provide its UFLS database to other Planning Coordinators.
R8	The UFLS entity provided data to its Planning Coordinator(s) less than or equal to 10 calendar days following the schedule specified by the Planning Coordinator(s) to support maintenance of each Planning Coordinator's UFLS database.	The UFLS entity provided data to its Planning Coordinator(s) more than 10 calendar days but less than or equal to 15 calendar days following the schedule specified by the Planning Coordinator(s) to support maintenance of each Planning Coordinator's UFLS database. OR The UFLS entity provided data to its Planning Coordinator(s) but the data was not according to the format specified by the Planning Coordinator(s) to support maintenance of each Planning Coordinator's UFLS database.	The UFLS entity provided data to its Planning Coordinator(s) more than 15 calendar days but less than or equal to 20 calendar days following the schedule specified by the Planning Coordinator(s) to support maintenance of each Planning Coordinator's UFLS database.	The UFLS entity provided data to its Planning Coordinator(s) more than 20 calendar days following the schedule specified by the Planning Coordinator(s) to support maintenance of each Planning Coordinator's UFLS database. OR The UFLS entity failed to provide data to its Planning Coordinator(s) to support maintenance of each Planning Coordinator's UFLS database.
R9	The UFLS entity provided less than 100% but more than (and including) 95% of automatic tripping of Load in accordance with the UFLS	The UFLS entity provided less than 95% but more than (and including) 90% of automatic tripping of Load in accordance with the UFLS program design	The UFLS entity provided less than 90% but more than (and including) 85% of automatic tripping of Load in accordance with the UFLS program design	The UFLS entity provided less than 85% of automatic tripping of Load in accordance with the UFLS program design and schedule for implementation,

R #	Lower VSL	Moderate VSL	High VSL	Severe VSL
	program design and schedule for implementation, including any Corrective Action Plan, as determined by the Planning Coordinator(s) area in which it owns assets.	and schedule for implementation, including any Corrective Action Plan, as determined by the Planning Coordinator(s) area in which it owns assets.	and schedule for implementation, including any Corrective Action Plan, as determined by the Planning Coordinator(s) area in which it owns assets.	including any Corrective Action Plan, as determined by the Planning Coordinator(s) area in which it owns assets.
R10	The Transmission Owner provided less than 100% but more than (and including) 95% automatic switching of its existing capacitor banks, Transmission Lines, and reactors to control over-voltage if required by the UFLS program and schedule for implementation, including any Corrective Action Plan, as determined by the Planning Coordinator(s) in each Planning Coordinator area in which the Transmission Owner owns transmission.	The Transmission Owner provided less than 95% but more than (and including) 90% automatic switching of its existing capacitor banks, Transmission Lines, and reactors to control over-voltage if required by the UFLS program and schedule for implementation, including any Corrective Action Plan, as determined by the Planning Coordinator(s) in each Planning Coordinator area in which the Transmission Owner owns transmission.	The Transmission Owner provided less than 90% but more than (and including) 85% automatic switching of its existing capacitor banks, Transmission Lines, and reactors to control over-voltage if required by the UFLS program and schedule for implementation, including any Corrective Action Plan, as determined by the Planning Coordinator(s) in each Planning Coordinator area in which the Transmission Owner owns transmission.	The Transmission Owner provided less than 85% automatic switching of its existing capacitor banks, Transmission Lines, and reactors to control over-voltage if required by the UFLS program and schedule for implementation, including any Corrective Action Plan, as determined by the Planning Coordinator(s) in each Planning Coordinator area in which the Transmission Owner owns transmission.
R11	The Planning Coordinator, in whose area a BES islanding event resulting in system frequency excursions below the initializing set points of	The Planning Coordinator, in whose area a BES islanding event resulting in system frequency excursions below the initializing set points of	The Planning Coordinator, in whose area a BES islanding event resulting in system frequency excursions below the initializing set points of the	The Planning Coordinator, in whose area a BES islanding event resulting in system frequency excursions below the initializing set points of the UFLS program,

R #	Lower VSL	Moderate VSL	High VSL	Severe VSL
	the UFLS program, conducted and documented an assessment of the event and evaluated the parts as specified in Requirement R11, Parts 11.1 and 11.2 within a time greater than one year but less than or equal to 13 months of actuation.	the UFLS program, conducted and documented an assessment of the event and evaluated the parts as specified in Requirement R11, Parts 11.1 and 11.2 within a time greater than 13 months but less than or equal to 14 months of actuation.	UFLS program, conducted and documented an assessment of the event and evaluated the parts as specified in Requirement R11, Parts 11.1 and 11.2 within a time greater than 14 months but less than or equal to 15 months of actuation. OR The Planning Coordinator, in whose area an islanding event resulting in system frequency excursions below the initializing set points of the UFLS program, conducted and documented an assessment of the event within one year of event actuation but failed to evaluate one (1) of the Parts as specified in Requirement R11, Parts11.1 or 11.2.	conducted and documented an assessment of the event and evaluated the parts as specified in Requirement R11, Parts 11.1 and 11.2 within a time greater than 15 months of actuation. OR The Planning Coordinator, in whose area an islanding event resulting in system frequency excursions below the initializing set points of the UFLS program, failed to conduct and document an assessment of the event and evaluate the Parts as specified in Requirement R11, Parts 11.1 and 11.2. OR The Planning Coordinator, in whose area an islanding event resulting in system frequency excursions below the initializing set points of the UFLS program, conducted and documented an assessment of the event within one year of event actuation but failed to evaluate all of the Parts

R #	Lower VSL	Moderate VSL	High VSL	Severe VSL
				as specified in Requirement R11, Parts 11.1 and 11.2.
R12	N/A	The Planning Coordinator, in which UFLS program deficiencies were identified per Requirement R11, conducted and documented a UFLS design assessment to consider the identified deficiencies greater than two years but less than or equal to 25 months of event actuation.	The Planning Coordinator, in which UFLS program deficiencies were identified per Requirement R11, conducted and documented a UFLS design assessment to consider the identified deficiencies greater than 25 months but less than or equal to 26 months of event actuation.	The Planning Coordinator, in which UFLS program deficiencies were identified per Requirement R11, conducted and documented a UFLS design assessment to consider the identified deficiencies greater than 26 months of event actuation. OR The Planning Coordinator, in which UFLS program deficiencies were identified per Requirement R11, failed to conduct and document a UFLS design assessment to consider the identified deficiencies.
R13	N/A	N/A	N/A	The Planning Coordinator, in whose area a BES islanding event occurred that also included the area(s) or portions of area(s) of other Planning Coordinator(s) in the same islanding event and that resulted in system frequency excursions below the initializing set points of the UFLS

R #	Lower VSL	Moderate VSL	High VSL	Severe VSL
				program, failed to coordinate its UFLS event assessment with all other Planning Coordinators whose areas or portions of whose areas were also included in the same islanding event in one of the manners described in Requirement R13
R14	N/A	N/A	N/A	The Planning Coordinator failed to respond to written comments submitted by UFLS entities and Transmission Owners within its Planning Coordinator area following a comment period and before finalizing its UFLS program, indicating in the written response to comments whether changes were made or reasons why changes were not made to the items in Parts 14.1 through 14.3.
R15	N/A	The Planning Coordinator determined, through a UFLS design assessment performed under Requirement R4, R5, or R12, that the UFLS program did not meet the performance characteristics in Requirement	The Planning Coordinator determined, through a UFLS design assessment performed under Requirement R4, R5, or R12, that the UFLS program did not meet the performance characteristics in Requirement	The Planning Coordinator determined, through a UFLS design assessment performed under Requirement R4, R5, or R12, that the UFLS program did not meet the performance characteristics in Requirement

R #	Lower VSL	Moderate VSL	High VSL	Severe VSL
		R3, and developed a Corrective Action Plan and a schedule for implementation by the UFLS entities within its area, but exceeded the permissible time frame for development by a period of up to 1 month.	R3, and developed a Corrective Action Plan and a schedule for implementation by the UFLS entities within its area, but exceeded the permissible time frame for development by a period greater than 1 month but not more than 2 months.	R3, but failed to develop a Corrective Action Plan and a schedule for implementation by the UFLS entities within its area. OR The Planning Coordinator determined, through a UFLS design assessment performed under Requirement R4, R5, or R12, that the UFLS program did not meet the performance characteristics in Requirement R3, and developed a Corrective Action Plan and a schedule for implementation by the UFLS entities within its area, but exceeded the permissible time frame for development by a period greater than 2 months.

D. Regional Variances

D.A. Regional Variance for the Quebec Interconnection

The following Interconnection-wide variance shall be applicable in the Quebec Interconnection and replaces, in their entirety, Requirements R3 and R4 and the violation severity levels associated with Requirements R3 and R4.

Rationale for Requirement D.A.3:

There are two modifications for requirement D.A.3 :

1. 25% Generation Deficiency : Since the Quebec Interconnection has no potential viable BES Island in underfrequency conditions, the largest generation deficiency scenarios are limited to extreme contingencies not already covered by RAS.

Based on Hydro-Québec TransÉnergie Transmission Planning requirements, the stability of the network shall be maintained for extreme contingencies using a case representing internal transfers not expected to be exceeded 25% of the time.

The Hydro-Québec TransÉnergie defense plan to cover these extreme contingencies includes two RAS (RPTC- generation rejection and remote load shedding and TDST - a centralized UVLS) and the UFLS.

2. Frequency performance curve (attachment 1A) : Specific cases where a small generation deficiency using a peak case scenario with the minimum requirement of spinning reserve can lead to an acceptable frequency deviation in the Quebec Interconnection while stabilizing between the PRC-006-2 requirement (59.3 Hz) and the UFLS anti-stall threshold (59.0 Hz).

An increase of the anti-stall threshold to 59.3 Hz would correct this situation but would cause frequent load shedding of customers without any gain of system reliability. Therefore, it is preferable to lower the steady state frequency minimum value to 59.0 Hz.

The delay in the performance characteristics curve is harmonized between D.A.3 and R.3 to 60 seconds.

Rationale for Requirements D.A.3.3. and D.A.4:

The **Q**uebec Interconnection has its own definition of BES. In Quebec, the vast majority of BES generating plants/facilities are not directly connected to the BES. For simulations to take into account sufficient generating resources D.A.3.3 and D.A.4 need simply refer to BES generators, plants or facilities since these are listed in a Registry approved by Québec's Regulatory Body (Régie de l'Énergie).

D.A.3. Each Planning Coordinator shall develop a UFLS program, including notification of and a schedule for implementation by UFLS entities within its area, that meets the following performance characteristics in simulations of underfrequency conditions resulting from each of these extreme events:

- Loss of the entire capability of a generating station.
- Loss of all transmission circuits emanating from a generating station, switching station, substation or dc terminal.
- Loss of all transmission circuits on a common right-of-way.
- Three-phase fault with failure of a circuit breaker to operate and correct operation of a breaker failure protection system and its associated breakers.
- Three-phase fault on a circuit breaker, with normal fault clearing.
- The operation or partial operation of a RAS for an event or condition for which it was not intended to operate.

[VRF: High][Time Horizon: Long-term Planning]

D.A.3.1. Frequency shall remain above the Underfrequency Performance Characteristic curve in PRC-006 - Attachment 1A, either for 60 seconds or until a steady-state condition between 59.0 Hz and 60.7 Hz is reached, and

D.A.3.2. Frequency shall remain below the Overfrequency Performance Characteristic curve in PRC-006 - Attachment 1A, either for 60 seconds or until a steady-state condition between 59.0 Hz and 60.7 Hz is reached, and

D.A.3.3. Volts per Hz (V/Hz) shall not exceed 1.18 per unit for longer than two seconds cumulatively per simulated event, and shall not exceed 1.10 per unit for longer than 45 seconds cumulatively per simulated event at each Quebec BES generator bus and associated generator step-up transformer high-side bus

M.D.A.3. Each Planning Coordinator shall have evidence such as reports, memorandums, e-mails, program plans, or other documentation of its UFLS program, including the notification of the UFLS entities of implementation schedule, that meet the criteria in Requirement D.A.3 Parts D.A.3.1 through D.A.3.3.

D.A.4. Each Planning Coordinator shall conduct and document a UFLS design assessment at least once every five years that determines through dynamic simulation whether the UFLS program design meets the performance characteristics in Requirement D.A.3 for each island identified in Requirement R2. The simulation shall model each of the following; *[VRF: High][Time Horizon: Long-term Planning]*

D.A.4.1 Underfrequency trip settings of individual generating units that are part of Quebec BES plants/facilities that trip above the Generator

Underfrequency Trip Modeling curve in PRC-006 - Attachment 1A, and

D.A.4.2 Overfrequency trip settings of individual generating units that are part of Quebec BES plants/facilities that trip below the Generator Overfrequency Trip Modeling curve in PRC-006 - Attachment 1A, and

D.A.4.3 Any automatic Load restoration that impacts frequency stabilization and operates within the duration of the simulations run for the assessment.

M.D.A.4. Each Planning Coordinator shall have dated evidence such as reports, dynamic simulation models and results, or other dated documentation of its UFLS design assessment that demonstrates it meets Requirement D.A.4 Parts D.A.4.1 through D.A.4.3.

D#	Lower VSL	Moderate VSL	High VSL	Severe VSL
DA3	N/A	The Planning Coordinator developed a UFLS program, including notification of and a schedule for implementation by UFLS entities within its area, but failed to meet one (1) of the performance characteristic in Parts D.A.3.1, D.A.3.2, or D.A.3.3 in simulations of underfrequency conditions	The Planning Coordinator developed a UFLS program including notification of and a schedule for implementation by UFLS entities within its area, but failed to meet two (2) of the performance characteristic in Parts D.A.3.1, D.A.3.2, or D.A.3.3 in simulations of underfrequency conditions	The Planning Coordinator developed a UFLS program including notification of and a schedule for implementation by UFLS entities within its area, but failed to meet all the performance characteristic in Parts D.A.3.1, D.A.3.2, and D.A.3.3 in simulations of underfrequency conditions OR The Planning Coordinator failed to develop a UFLS program including notification of and a schedule for implementation by UFLS entities within its area.
DA4	N/A	The Planning Coordinator conducted and documented a UFLS assessment at least once every five years that determined through dynamic simulation whether the UFLS program design met the performance characteristics in Requirement D.A.3 but the simulation failed to include one (1) of the items as	The Planning Coordinator conducted and documented a UFLS assessment at least once every five years that determined through dynamic simulation whether the UFLS program design met the performance characteristics in Requirement D.A.3 but the simulation failed to include two (2) of the items as	The Planning Coordinator conducted and documented a UFLS assessment at least once every five years that determined through dynamic simulation whether the UFLS program design met the performance characteristics in Requirement D.A.3 but the simulation failed to include all of the items as

D#	Lower VSL	Moderate VSL	High VSL	Severe VSL
		specified in Parts D.A.4.1, D.A.4.2 or D.A.4.3.	specified in Parts D.A.4.1, D.A.4.2 or D.A.4.3.	specified in Parts D.A.4.1, D.A.4.2 and D.A.4.3. OR The Planning Coordinator failed to conduct and document a UFLS assessment at least once every five years that determines through dynamic simulation whether the UFLS program design meets the performance characteristics in Requirement D.A.3

D.B. Regional Variance for the Western Electricity Coordinating Council

The following Interconnection-wide variance shall be applicable in the Western Interconnection and replaces, in their entirety, Requirements R1 through R5, and R11 through R15.

As used in the RV, Planning Coordinator is specific to those Planning Coordinators providing Planning Coordinator service(s) to entities within the Western Interconnection, regardless of where the Planning Coordinator is located.

D.B.1. Each Planning Coordinator shall participate in a joint regional review with the other Planning Coordinators that develops and documents criteria, including consideration of historical events and system studies, to select portions of the Bulk Electric System (BES) that may form islands. *[VRF: Medium][Time Horizon: Long-term Planning]*

M.D.B.1. Each Planning Coordinator will have evidence such as reports, or other documentation of its criteria, developed as part of the joint regional review with other Planning Coordinators to select portions of the Bulk Electric System that may form islands including how system studies and historical events were considered to develop the criteria per Requirement D.B.1.

D.B.2. Each Planning Coordinator shall identify one or more islands from the regional review (per D.B.1) to serve as a basis for designing a Western Interconnection-wide coordinated UFLS program including: *[VRF: Medium][Time Horizon: Long-term Planning]*

D.B.2.1. Those islands selected by applying the criteria in Requirement D.B.1, and

D.B.2.2. Any portions of the BES designed to detach from the Western Interconnection (planned islands) as a result of the operation of a relay scheme or Remedial Action Scheme.

M.D.B.2. Each Planning Coordinator will have evidence such as reports, memorandums, e-mails, or other documentation supporting its identification of an island(s), from the regional review (per D.B.1), as a basis for designing a Western Interconnection-wide coordinated UFLS program meeting the criteria in Requirement D.B.2 Parts D.B.2.1 and D.B.2.2.

D.B.3. Each Planning Coordinator shall adopt a UFLS program, coordinated across the Western Interconnection, including notification of and a schedule for implementation by UFLS entities within its area, that meets the following performance characteristics in simulations of underfrequency conditions resulting from an imbalance scenario, where an imbalance = [(load — actual generation output) / (load)], of up to 25 percent within the identified island(s). *[VRF: High][Time Horizon: Long-term Planning]*

D.B.3.1. Frequency shall remain above the Underfrequency Performance Characteristic curve in PRC-006-5 - Attachment 1, either for 60

seconds or until a steady-state condition between 59.3 Hz and 60.7 Hz is reached, and

D.B.3.2. Frequency shall remain below the Overfrequency Performance Characteristic curve in PRC-006-5 - Attachment 1, either for 60 seconds or until a steady-state condition between 59.3 Hz and 60.7 Hz is reached, and

D.B.3.3. Volts per Hz (V/Hz) shall not exceed 1.18 per unit for longer than two seconds cumulatively per simulated event, and shall not exceed 1.10 per unit for longer than 45 seconds cumulatively per simulated event at each generator bus and generator step-up transformer high-side bus associated with each of the following:

D.B.3.3.1. Individual generating units greater than 20 MVA (gross nameplate rating) directly connected to the BES

D.B.3.3.2. Generating plants/facilities greater than 75 MVA (gross aggregate nameplate rating) directly connected to the BES

D.B.3.3.3. Facilities consisting of one or more units connected to the BES at a common bus with total generation above 75 MVA gross nameplate rating.

M.D.B.3. Each Planning Coordinator will have evidence such as reports, memorandums, e-mails, program plans, or other documentation of its adoption of a UFLS program, coordinated across the Western Interconnection, including the notification of the UFLS entities of implementation schedule meeting the criteria in Requirement D.B.3 Parts D.B.3.1 through D.B.3.3.

D.B.4. Each Planning Coordinator shall participate in and document a coordinated UFLS design assessment with the other Planning Coordinators in the Western Interconnection at least once every five years that determines through dynamic simulation whether the UFLS program design meets the performance characteristics in Requirement D.B.3 for each island identified in Requirement D.B.2. The simulation shall model each of the following: *[VRF: High][Time Horizon: Long-term Planning]*

D.B.4.1. Underfrequency trip settings of individual generating units greater than 20 MVA (gross nameplate rating) directly connected to the BES that trip above the Generator Underfrequency Trip Modeling curve in PRC-006-5 - Attachment 1.

D.B.4.2. Underfrequency trip settings of generating plants/facilities greater than 75 MVA (gross aggregate nameplate rating) directly connected to the BES that trip above the Generator Underfrequency Trip Modeling curve in PRC-006-5 - Attachment 1.

D.B.4.3. Underfrequency trip settings of any facility consisting of one or more units connected to the BES at a common bus with total generation above 75 MVA (gross nameplate rating) that trip above the Generator Underfrequency Trip Modeling curve in PRC-006-5 - Attachment 1.

D.B.4.4. Overfrequency trip settings of individual generating units greater than 20 MVA (gross nameplate rating) directly connected to the BES that trip below the Generator Overfrequency Trip Modeling curve in PRC-006-5 — Attachment 1.

D.B.4.5. Overfrequency trip settings of generating plants/facilities greater than 75 MVA (gross aggregate nameplate rating) directly connected to the BES that trip below the Generator Overfrequency Trip Modeling curve in PRC-006-5 — Attachment 1.

D.B.4.6. Overfrequency trip settings of any facility consisting of one or more units connected to the BES at a common bus with total generation above 75 MVA (gross nameplate rating) that trip below the Generator Overfrequency Trip Modeling curve in PRC-006-5 — Attachment 1.

D.B.4.7. Any automatic Load restoration that impacts frequency stabilization and operates within the duration of the simulations run for the assessment.

M.D.B.4. Each Planning Coordinator will have dated evidence such as reports, dynamic simulation models and results, or other dated documentation of its participation in a coordinated UFLS design assessment with the other Planning Coordinators demonstrating that it meets Requirement D.B.4 Parts D.B.4.1 through D.B.4.7.

D.B.5. through D.B.10. Reserved

D.B.11. Each Planning Coordinator, in whose area a BES islanding event results in system frequency excursions below the initializing set points of the UFLS program, shall participate in and document a coordinated event assessment with all affected Planning Coordinators to conduct and document an assessment of the event within one year of event actuation to evaluate: *[VRF: Medium][Time Horizon: Operations Assessment]*

D.B.11.1. The performance of the UFLS equipment,

D.B.11.2 The effectiveness of the UFLS program

M.D.B.11. Each Planning Coordinator will have dated evidence such as reports, data gathered from an historical event, or other dated documentation to show that it participated in a coordinated event assessment of the performance of the UFLS equipment and the effectiveness of the UFLS program per Requirement D.B.11.

D.B.12. Each Planning Coordinator, in whose islanding event assessment (per D.B.11) UFLS program deficiencies are identified, shall participate in and document a coordinated UFLS design assessment of the UFLS program with all other Planning Coordinators in the Western Interconnection to consider the identified deficiencies within two years of event actuation. *[VRF: Medium][Time Horizon: Operations Assessment]*

M.D.B.12. Each Planning Coordinator will have dated evidence such as reports, data gathered from an historical event, or other dated documentation to show that it participated in a UFLS design assessment per Requirements D.B.12 and D.B.4 if UFLS program deficiencies are identified in D.B.11.

D #	Lower VSL	Moderate VSL	High VSL	Severe VSL
D.B.1	N/A	The Planning Coordinator participated in a joint regional review with the other Planning Coordinators that developed and documented criteria but failed to include the consideration of historical events, to select portions of the BES, including interconnected portions of the BES in adjacent Planning Coordinator areas, that may form islands OR The Planning Coordinator participated in a joint regional review with the other Planning Coordinators that developed and documented criteria but failed to include the consideration of system studies, to select portions of the BES, including interconnected portions of the BES in adjacent Planning Coordinator areas, that may form islands	The Planning Coordinator participated in a joint regional review with the other Planning Coordinators that developed and documented criteria but failed to include the consideration of historical events and system studies, to select portions of the BES, including interconnected portions of the BES in adjacent Planning Coordinator areas, that may form islands	The Planning Coordinator failed to participate in a joint regional review with the other Planning Coordinators that developed and documented criteria to select portions of the BES, including interconnected portions of the BES in adjacent Planning Coordinator areas that may form islands
D.B.2	N/A	N/A	The Planning Coordinator identified an island(s) from the	The Planning Coordinator identified an island(s) from the

D #	Lower VSL	Moderate VSL	High VSL	Severe VSL
			regional review to serve as a basis for designing its UFLS program but failed to include one (1) of the parts as specified in Requirement D.B.2, Parts D.B.2.1 or D.B.2.2	regional review to serve as a basis for designing its UFLS program but failed to include all of the parts as specified in Requirement D.B.2, Parts D.B.2.1 or D.B.2.2 OR The Planning Coordinator failed to identify any island(s) from the regional review to serve as a basis for designing its UFLS program.
D.B.3	N/A	The Planning Coordinator adopted a UFLS program, coordinated across the Western Interconnection that included notification of and a schedule for implementation by UFLS entities within its area, but failed to meet one (1) of the performance characteristic in Requirement D.B.3, Parts D.B.3.1, D.B.3.2, or D.B.3.3 in simulations of underfrequency conditions	The Planning Coordinator adopted a UFLS program, coordinated across the Western Interconnection that included notification of and a schedule for implementation by UFLS entities within its area, but failed to meet two (2) of the performance characteristic in Requirement D.B.3, Parts D.B.3.1, D.B.3.2, or D.B.3.3 in simulations of underfrequency conditions	The Planning Coordinator adopted a UFLS program, coordinated across the Western Interconnection that included notification of and a schedule for implementation by UFLS entities within its area, but failed to meet all the performance characteristic in Requirement D.B.3, Parts D.B.3.1, D.B.3.2, and D.B.3.3 in simulations of underfrequency conditions OR The Planning Coordinator failed to adopt a UFLS program,

D #	Lower VSL	Moderate VSL	High VSL	Severe VSL
				coordinated across the Western Interconnection , including notification of and a schedule for implementation by UFLS entities within its area.
D.B.4	The Planning Coordinator participated in and documented a coordinated UFLS assessment with the other Planning Coordinators across the Western Interconnection at least once every five years that determines through dynamic simulation whether the UFLS program design meets the performance characteristics in Requirement D.B.3 for each island identified in Requirement D.B.2 but the simulation failed to include one (1) of the items as specified in Requirement D.B.4, Parts D.B.4.1 through D.B.4.7.	The Planning Coordinator participated in and documented a coordinated UFLS assessment with the other Planning Coordinators across the Western Interconnection at least once every five years that determines through dynamic simulation whether the UFLS program design meets the performance characteristics in Requirement D.B.3 for each island identified in Requirement D.B.2 but the simulation failed to include two (2) of the items as specified in Requirement D.B.4, Parts D.B.4.1 through D.B.4.7.	The Planning Coordinator participated in and documented a coordinated UFLS assessment with the other Planning Coordinators across the Western Interconnection at least once every five years that determines through dynamic simulation whether the UFLS program design meets the performance characteristics in Requirement D.B.3 for each island identified in Requirement D.B.2 but the simulation failed to include three (3) of the items as specified in Requirement D.B.4, Parts D.B.4.1 through D.B.4.7.	The Planning Coordinator participated in and documented a coordinated UFLS assessment with the other Planning Coordinators across the Western Interconnection at least once every five years that determines through dynamic simulation whether the UFLS program design meets the performance characteristics in Requirement D.B.3 for each island identified in Requirement D.B.2 but the simulation failed to include four (4) or more of the items as specified in Requirement D.B.4, Parts D.B.4.1 through D.B.4.7. OR The Planning Coordinator failed to participate in and document a coordinated UFLS assessment with the other Planning Coordinators across the Western

D #	Lower VSL	Moderate VSL	High VSL	Severe VSL
				Interconnection at least once every five years that determines through dynamic simulation whether the UFLS program design meets the performance characteristics in Requirement D.B.3 for each island identified in Requirement D.B.2
D.B.11	The Planning Coordinator, in whose area a BES islanding event resulting in system frequency excursions below the initializing set points of the UFLS program, participated in and documented a coordinated event assessment with all Planning Coordinators whose areas or portions of whose areas were also included in the same islanding event and evaluated the parts as specified in Requirement D.B.11, Parts D.B.11.1 and D.B.11.2 within a time greater than one year but less than or equal to 13 months of actuation.	The Planning Coordinator, in whose area a BES islanding event resulting in system frequency excursions below the initializing set points of the UFLS program, participated in and documented a coordinated event assessment with all Planning Coordinators whose areas or portions of whose areas were also included in the same islanding event and evaluated the parts as specified in Requirement D.B.11, Parts D.B.11.1 and D.B.11.2 within a time greater than 13 months but less than or equal to 14 months of actuation.	The Planning Coordinator, in whose area a BES islanding event resulting in system frequency excursions below the initializing set points of the UFLS program, participated in and documented a coordinated event assessment with all Planning Coordinators whose areas or portions of whose areas were also included in the same islanding event and evaluated the parts as specified in Requirement D.B.11, Parts D.B.11.1 and D.B.11.2 within a time greater than 14 months but less than or equal to 15 months of actuation. OR The Planning Coordinator, in whose area an islanding event	The Planning Coordinator, in whose area a BES islanding event resulting in system frequency excursions below the initializing set points of the UFLS program, participated in and documented a coordinated event assessment with all Planning Coordinators whose areas or portions of whose areas were also included in the same islanding event and evaluated the parts as specified in Requirement D.B.11, Parts D.B.11.1 and D.B.11.2 within a time greater than 15 months of actuation. OR The Planning Coordinator, in whose area an islanding event resulting in system frequency

D #	Lower VSL	Moderate VSL	High VSL	Severe VSL
			resulting in system frequency excursions below the initializing set points of the UFLS program, participated in and documented a coordinated event assessment with all Planning Coordinators whose areas or portions of whose areas were also included in the same islanding event within one year of event actuation but failed to evaluate one (1) of the parts as specified in Requirement D.B.11, Parts D.B.11.1 or D.B.11.2.	excursions below the initializing set points of the UFLS program, failed to participate in and document a coordinated event assessment with all Planning Coordinators whose areas or portion of whose areas were also included in the same island event and evaluate the parts as specified in Requirement D.B.11, Parts D.B.11.1 and D.B.11.2. OR The Planning Coordinator, in whose area an islanding event resulting in system frequency excursions below the initializing set points of the UFLS program, participated in and documented a coordinated event assessment with all Planning Coordinators whose areas or portions of whose areas were also included in the same islanding event within one year of event actuation but failed to evaluate all of the parts as specified in Requirement D.B.11, Parts D.B.11.1 and D.B.11.2.

D #	Lower VSL	Moderate VSL	High VSL	Severe VSL
D.B.12	N/A	The Planning Coordinator, in which UFLS program deficiencies were identified per Requirement D.B.11, participated in and documented a coordinated UFLS design assessment of the coordinated UFLS program with the other Planning Coordinators across the Western Interconnection to consider the identified deficiencies in greater than two years but less than or equal to 25 months of event actuation.	The Planning Coordinator, in which UFLS program deficiencies were identified per Requirement D.B.11, participated in and documented a coordinated UFLS design assessment of the coordinated UFLS program with the other Planning Coordinators across the Western Interconnection to consider the identified deficiencies in greater than 25 months but less than or equal to 26 months of event actuation.	The Planning Coordinator, in which UFLS program deficiencies were identified per Requirement D.B.11, participated in and documented a coordinated UFLS design assessment of the coordinated UFLS program with the other Planning Coordinators across the Western Interconnection to consider the identified deficiencies in greater than 26 months of event actuation. OR The Planning Coordinator, in which UFLS program deficiencies were identified per Requirement D.B.11, failed to participate in and document a coordinated UFLS design assessment of the coordinated UFLS program with the other Planning Coordinators across the Western Interconnection to consider the identified deficiencies

E. Associated Documents

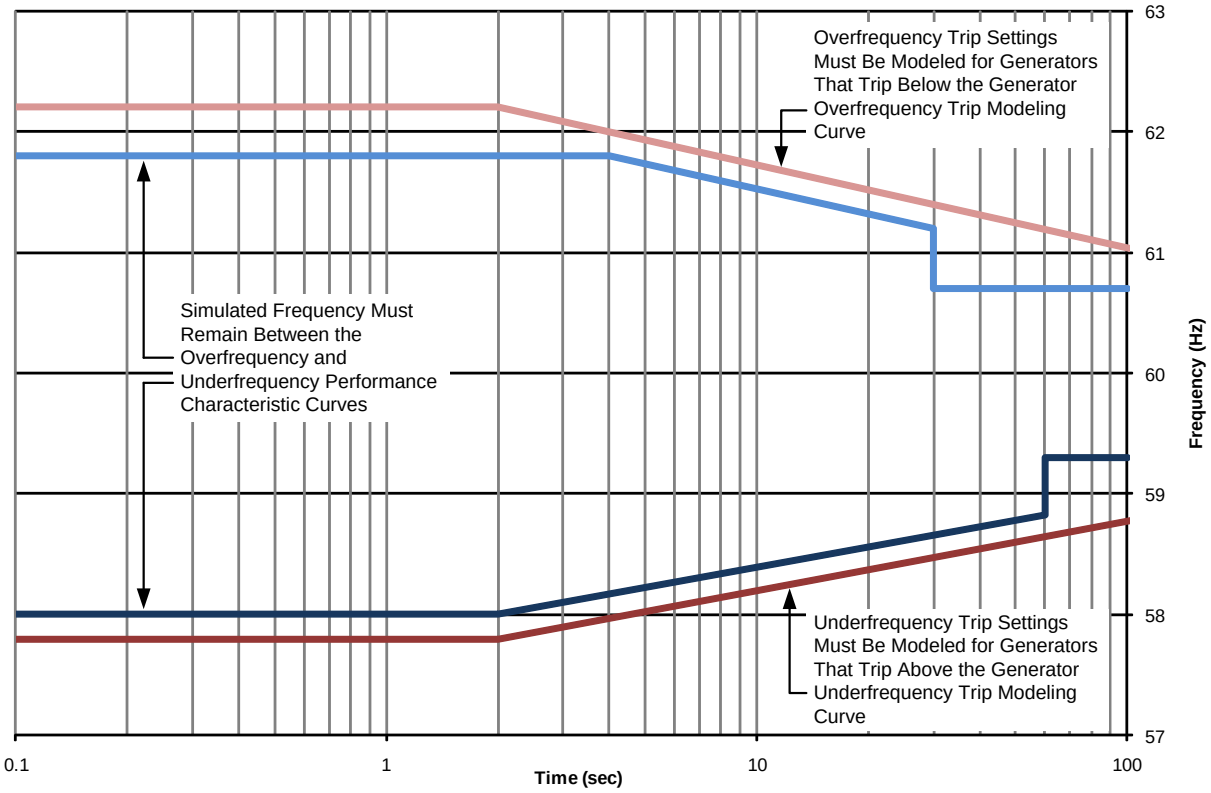
Version History

Version	Date	Action	Change Tracking
0	April 1, 2005	Effective Date	New
1	May 25, 2010	Completed revision, merging and updating PRC-006-0, PRC-007-0 and PRC-009-0.	
1	November 4, 2010	Adopted by the Board of Trustees	
1	May 7, 2012	FERC Order issued approving PRC-006-1 (approval becomes effective July 10, 2012)	
1	November 9, 2012	FERC Letter Order issued accepting the modification of the VRF in R5 from (Medium to High) and the modification of the VSL language in R8.	
2	November 13, 2014	Adopted by the Board of Trustees	Revisions made under Project 2008-02: Undervoltage Load Shedding (UVLS) & Underfrequency Load Shedding (UFLS) to address directive issued in FERC Order No. 763. Revisions to existing Requirement R9 and R10 and addition of new Requirement R15.
2	March 4, 2015	FERC Order issued approving PRC-006-2. Docket No. RD15-2-000	
3	August 10, 2017	Adopted by the NERC Board of Trustees	Revisions to the Regional Variance for the Quebec Interconnection.
3	September 5, 2017	FERC Order issued approving PRC-006-3.	

4	February 6, 2020	Adopted by NERC Board of Trustees	Revisions under Project 2017-07
5	August 20, 2020	Adopted by NERC Board of Trustees	In Version 5: 1) Requirements R14 and R15 were added to the list of Requirements not applicable to the Western Interconnection (WI), 2) use of "Planning Coordinator" (PC) was made specific to PCs providing services within the WI, regardless of where the PC is located, 3) non-substantive changes were made conforming the document and styles to the newest NERC conventions and templates, and 4) references to Version 3 were updated to Version 5.
5	December 23,2020	FERC Oder approving PRC-006-5 Docket No. RD21-1-000	
5	April 1, 2021	Effective Date	

PRC-006-5 – Attachment 1

Underfrequency Load Shedding Program
Design Performance and Modeling Curves for
Requirements R3 Parts 3.1-3.2 and R4 Parts 4.1-4.6



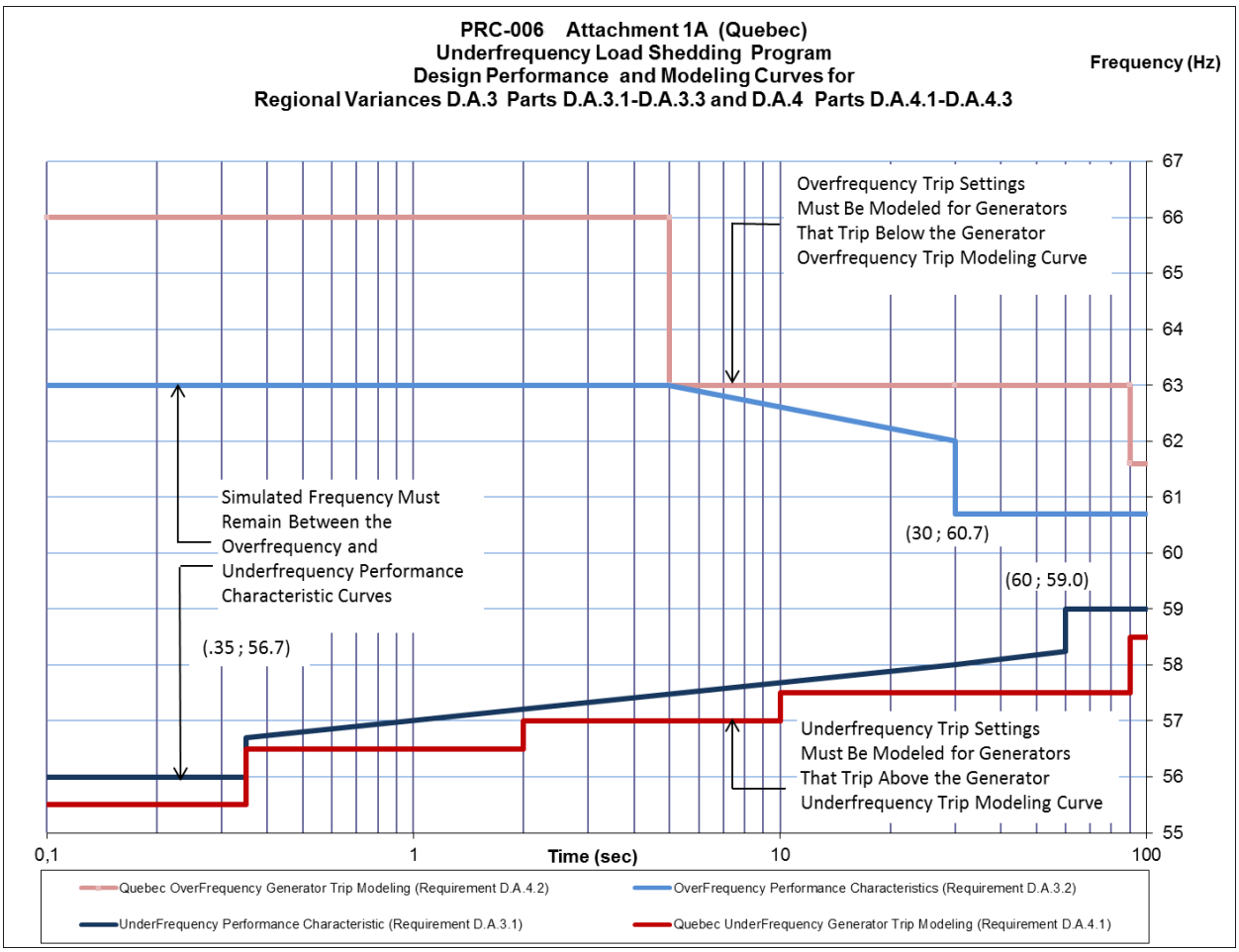
- Generator Overfrequency Trip Modeling (Requirement R4 Parts 4.4-4.6)
- Overfrequency Performance Characteristic (Requirement R3 Part 3.2)
- Underfrequency Performance Characteristic (Requirement R3 Part 3.1)
- Generator Underfrequency Trip Modeling (Requirement R4 Parts 4.1-4.3)

Curve Definitions

Generator Overfrequency Trip Modeling		Overfrequency Performance Characteristic		
t ≤ 2 s	t > 2 s	t ≤ 4 s	4 s < t ≤ 30 s	t > 30 s
f = 62.2 Hz	f = -0.686log(t) + 62.41 Hz	f = 61.8 Hz	f = -0.686log(t) + 62.21 Hz	f = 60.7 Hz

Generator Underfrequency Trip Modeling	Underfrequency Performance Characteristic

t ≤ 2 s	t > 2 s	t ≤ 2 s	2 s < t ≤ 60 s	t > 60 s
f = 57.8 Hz	f = 0.575log(t) + 57.63 Hz	f = 58.0 Hz	f = 0.575log(t) + 57.83 Hz	f = 59.3 Hz


PRC-006 Attachment 1A (Quebec)
Underfrequency Load Shedding Program
Design Performance and Modeling Curves for
Regional Variances D.A.3 Parts D.A.3.1-D.A.3.3 and D.A.4 Parts D.A.4.1-D.A.4.3
Frequency (Hz)
Overfrequency Trip Settings
Must Be Modeled for Generators
That Trip Below the Generator
Overfrequency Trip Modeling Curve
Simulated Frequency Must
Remain Between the
Overfrequency and
Underfrequency Performance
Characteristic Curves
(.35 ; 56.7)
(30 ; 60.7)
(60 ; 59.0)
Underfrequency Trip Settings
Must Be Modeled for Generators
That Trip Above the Generator
Underfrequency Trip Modeling Curve
67
66
65
64
63
62
61
60
59
58
57
56
55
0,1
1
10
100
Time (sec)
Quebec OverFrequency Generator Trip Modeling (Requirement D.A.4.2)
OverFrequency Performance Characteristics (Requirement D.A.3.2)
UnderFrequency Performance Characteristic (Requirement D.A.3.1)
Quebec UnderFrequency Generator Trip Modeling (Requirement D.A.4.1)

Rationale:

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for R9:

The "Corrective Action Plan" language was added in response to the FERC directive from Order No. 763, which raised concern that the standard failed to specify how soon an entity would need to implement corrections after a deficiency is identified by a Planning Coordinator (PC) assessment. The revised language adds clarity by requiring that each UFLS entity follow the UFLS program, including any Corrective Action Plan, developed by the PC.

Also, to achieve consistency of terminology throughout this standard, the word "application" was replaced with "implementation." (See Requirements R3, R14 and R15)

Rationale for R10:

The "Corrective Action Plan" language was added in response to the FERC directive from Order No. 763, which raised concern that the standard failed to specify how soon an entity would need to implement corrections after a deficiency is identified by a PC assessment. The revised language adds clarity by requiring that each UFLS entity follow the UFLS program, including any Corrective Action Plan, developed by the PC.

Also, to achieve consistency of terminology throughout this standard, the word "application" was replaced with "implementation." (See Requirements R3, R14 and R15)

Rationale for R15:

Requirement R15 was added in response to the directive from FERC Order No. 763, which raised concern that the standard failed to specify how soon an entity would need to implement corrections after a deficiency is identified by a PC assessment. Requirement R15 addresses the FERC directive by making explicit that if deficiencies are identified as a result of an assessment, the PC shall develop a Corrective Action Plan and schedule for implementation by the UFLS entities.

A "Corrective Action Plan" is defined in the NERC Glossary of Terms as, "a list of actions and an associated timetable for implementation to remedy a specific problem." Thus, the Corrective Action Plan developed by the PC will identify the specific timeframe for an entity to implement corrections to remedy any deficiencies identified by the PC as a result of an assessment.

Appendix PRC-006-5-QC-1
Specific provisions applicable to Standard
PRC-006-5 — Automatic Underfrequency Load Shedding

This appendix establishes specific provisions for the application of the standard in Québec. Provisions of the standard and of this appendix must be read jointly for comprehension and interpretation purposes. Where the standard and appendix differ, the appendix shall prevail.

A. Introduction

1. Title: No specific provision

2. Number: No specific provision

3. Purpose: No specific provision

4. Applicability:

This standard only applies to the facilities of the Main Transmission System (RTP).

5. Effective Date:

5.1. Adoption of the standard by the Régie de l'énergie: June 28, 2022

5.2. Adoption of this appendix by the Régie de l'énergie: June 28, 2022

5.3. Effective date of the standard and of this appendix in Québec: October 1, 2022

B. Requirements and Measures

No specific provision

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

In Québec, "Compliance Enforcement Authority" means the Régie de l'énergie in its roles of monitoring and enforcing compliance with respect to the Reliability Standard and to this appendix.

1.2. Evidence Retention

No specific provision

1.3. Compliance Monitoring and Assessment Processes

The Régie de l'énergie establishes the monitoring processes used to evaluate data or information for the purpose of determining compliance or non-compliance with the Reliability Standard and with this appendix.

1.4. Additional Compliance Information

No specific provision

2. Violation Severity Levels

No specific provision

D. Regional Variances

No specific provision

D.A. Regional Variance for the Québec Interconnection

No specific provision

D.B. Regional Variance for the Western Electricity Coordinating Council

No specific provision

E. Associated Documents

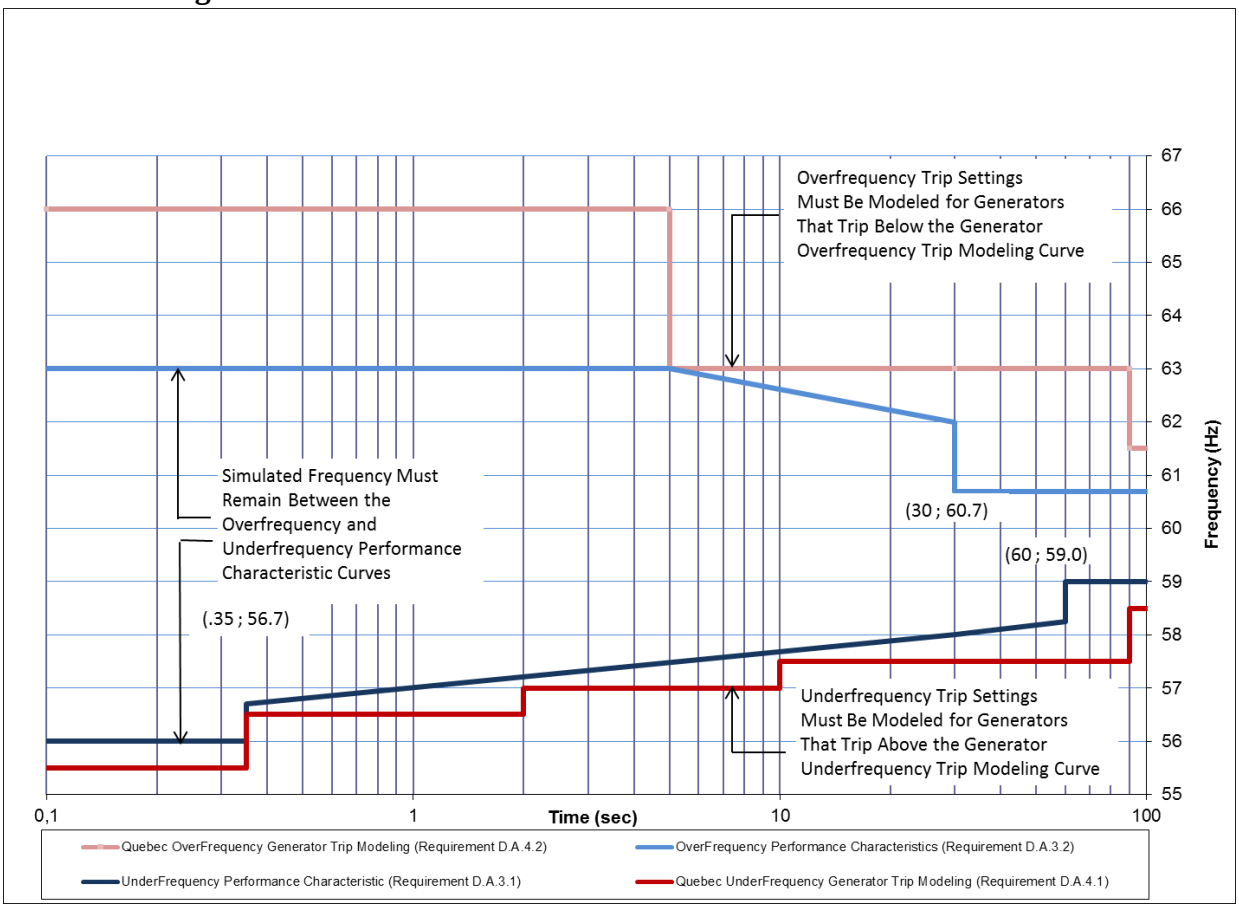
No specific provision

PRC-006-5 – Attachment 1

No specific provision

PRC-006-5 – Attachment 1A (Québec)

PRC-006-5 Attachment 1A (Québec)
UnderFrequency Load Shedding Program
Design Performance and Modeling Curves for
Regional Variances D.A.3.1-D.A.3.3 and D.A.4 Parts D.A.4.1-D.A.4.3



Curve Definitions

Generator Overfrequency Trip Modeling			Overfrequency Performance Characteristic		
t ≤ 5 s	t ≤ 90 s	t > 90 s	t ≤ 5 s	5 s < t ≤ 30 s	t > 30 s
f = 66 Hz	f = 63 Hz	f = 61.5 Hz	f = 63 Hz	f = −1.29log(t) + 63.90 Hz	f = 60.7 Hz

Generator Underfrequency Trip Modeling					Underfrequency Performance Characteristic		
t ≤ 0.35 s	t ≤ 2 s	t ≤ 10 s	t ≤ 90 s	t > 90 s	t ≤ 0.35 s	0.35 s < t ≤ 60 s	t > 60 s
f = 55.5 Hz	f = 56.5 Hz	f = 57.0 Hz	f = 57.5 Hz	f = 58.5 Hz	f = 56.0 Hz	f = 0.72 log(t) + 57.03 Hz	f = 59 Hz

Rationale

No specific provision

Version history

Version	Date	Action	Change Tracking
1	June 28, 2022	New appendix as per decision D-2022-085	New

A. Introduction

1. **Title:** Automatic Underfrequency Load Shedding

2. **Number:** PRC-006-NPCC-2

3. **Purpose:** The NPCC Automatic Underfrequency Load Shedding (UFLS) regional Reliability Standard establishes more stringent and specific NPCC UFLS program requirements than the NERC continent-wide PRC-006 standard. The program is designed such that declining frequency is arrested and recovered in accordance with established NPCC performance requirements stipulated in this document.

4. **Applicability:**

   4.1. Functional Entities:

   4.1.1. Generator Owner

   4.1.2. Planning Coordinator

   4.1.3. Distribution Providers that are responsible for the ownership, operation, or control of UFLS equipment as required by the UFLS program established by the Planning Coordinators

   4.1.4. Transmission Owners that are responsible for the ownership, operation, or control of UFLS equipment as required by the UFLS program established by the Planning Coordinators

5. **Effective Date:** See Implementation Plan.

B. Requirements and Measures

R1. Each Planning Coordinator in the Eastern Interconnection portion of NPCC shall design an UFLS program, pertaining to islands wholly within the NPCC Region, having performance characteristics that prevents the frequency from remaining below 59.5 Hz for more than 30 seconds in accordance with Figure 1 *[Violation Risk Factor: High] [Time Horizon: Long Term Planning]*

M1. Each Planning Coordinator shall have evidence such as reports, system studies and/or real-time power flow data captured from actual system events and other dated documentation that demonstrates it meets Requirement R1.

R2. Each Planning Coordinator shall provide UFLS island boundaries, as identified per the NERC continent-wide PRC-006 Standard on UFLS, to Distribution Providers, Generator Owners, and Transmission Owners within 30 calendar days of receipt of a request. *[Violation Risk Factor: Lower] [Time Horizon: Long Term Planning]*

M2. Each Planning Coordinator shall have evidence such as dated documentation that demonstrates that it meets requirement R2.

R3. Each Distribution Provider and Transmission Owner in the Eastern Interconnection portion of NPCC shall implement an automatic UFLS program, reflecting normal operating conditions, excluding outages. The automatic UFLS program shall be implemented on an island basis for each identified island per the NERC continent-wide PRC-006 Standard on UFLS as follows: *[Violation Risk Factor: High] [Time Horizon: Long Term Planning]*

- The UFLS program shall be implemented by each Distribution Provider and Transmission Owner according to the frequency thresholds, nominal operating times, and load shedding amounts specified in Attachment C, Tables 1-3; or
- The UFLS program shall be implemented collectively by multiple Distribution Providers or Transmission Owners, as long as they reside in the same UFLS island identified by the Planning Coordinator per Requirement R2. These multiple Distribution Providers or Transmission Owners, via mutual agreement, shall act as a single entity to provide an aggregated automatic UFLS program that sheds their coincident peak aggregated net Load according to the frequency thresholds, total nominal operating time, and load shedding amounts specified in Attachment C, Tables 1-3.

M3. Each Distribution Provider and Transmission Owner in the Eastern Interconnection portion of NPCC shall have evidence such as documentation or reports containing the location and amount of load to be tripped in their respective areas, and the corresponding frequency thresholds, on those circuits included in its UFLS program identified in Requirement R3. (Attachment C, Tables 1-3).

R4. Each Distribution Provider or Transmission Owner in the Eastern Interconnection portion of NPCC that does not meet the UFLS program parameters specified in Attachment C, Table 1-3, and each Distribution Provider or Transmission Owner in the Quebec Interconnection that does not meet the UFLS program parameters specified by its Planning Coordinator shall: *[Violation Risk Factor: High] [Time Horizon: Long Term Planning]*

- Within 30 calendar days of determining that it does not meet the specified parameters, notify its Planning Coordinator that it does not meet the UFLS program parameters; and
- Within the following 180 calendar days from notification of the Planning Coordinator,

(1) develop a Corrective Action Plan and a schedule for implementation that is mutually agreed upon with its Planning Coordinator or
(2) provide its Planning Coordinator with a technical study that demonstrates that the deviations from the program parameters will not result in failure of UFLS performance criteria being met for any island. The technical study must be acceptable to the Planning Coordinator prior to implementing deviations from program parameters and shall demonstrate coordination with UFLS programs of all entities residing within the same island(s) identified by the Planning

Coordinator in Requirement R2. The technical study shall also demonstrate coordination with other UFLS programs of adjoining Planning Coordinators, or (3) provide its Planning Coordinator with an analysis demonstrating that no alternative load shedding solution is available that would allow the Distribution Provider or Transmission Owner to comply with UFLS Attachment C Table 2 or Attachment C Table 3.

M4. Each Distribution Provider or Transmission Owner shall have evidence such as reports analysis, system studies and dated documentation that demonstrates that it meets Requirement R4.

R5. Each Planning Coordinator shall develop and review settings for inhibit thresholds at least once per five calendar years (such as, but not limited to, voltage, current and time) to be utilized within its region's UFLS program. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning]*

M5. Each Planning Coordinator shall have evidence such as reports, system studies or analysis that demonstrates that it meets Requirement R5.

R6. Each Planning Coordinator shall provide each Transmission Owner and Distribution Provider within its Planning Coordinator area the applicable inhibit thresholds within 30 calendar days of any changes. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M6. Each Planning Coordinator shall provide evidence such as letters, emails or other dated documentation that demonstrates that it meets Requirement R6.

R7. Each Distribution Provider and Transmission Owner that receives a notification pursuant to Requirement R6 shall develop and submit an implementation plan with respect to inhibit thresholds for approval by the Planning Coordinator within 90 calendar days of the request from the Planning Coordinator. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M7. Each Distribution Provider and Transmission Owner shall provide evidence such as letters, emails, or other dated documentation that demonstrates that it meets Requirement R7.

R8. Each Distribution Provider and Transmission Owner shall implement the inhibit thresholds provided by the Planning Coordinator in accordance with Requirement R6 and based on the Planning Coordinator approved implementation plan in accordance with R7. *[Violation Risk Factor: High] [Time Horizon: Operation Planning]*

M8. Each Distribution Provider and Transmission Owner shall provide evidence such as test reports, data sheets, completed work orders, or other documentation that demonstrates that it meets Requirement R8.

R9. Each Transmission Owner and Distribution Provider shall annually provide documentation, with no more than 15 calendar months between updates, to its Planning Coordinator of the actual net Load that would have been shed by the UFLS relays at each UFLS stage. The actual net Load shall be coincident with the entity's integrated hourly peak net Load during the previous year, as determined by measuring or calculating Load through the switches that would disconnect load if triggered by the UFLS relays. If measured data is unavailable then calculated data may be used. *[Violation Risk Factor: Lower] [Time Horizon: Long Term Planning]*

M9. Each Distribution Provider and Transmission Owner shall provide evidence such as reports, spreadsheets or other dated documentation submitted to its Planning Coordinator that indicates the net amount of load shed and the percentage of its peak load at each stage of its UFLS program to demonstrate that it meets Requirement R9.

R10. Each Generator Owner shall set each generator underfrequency trip relay, if so equipped, on or below the appropriate generator underfrequency trip protection setting threshold curve in Figure 2, except as otherwise exempted in Requirements R13 and R16. *[Violation Risk Factor: High] [Time Horizon: Long Term Planning]*

M10. Each Generator Owner shall provide evidence such as reports, data sheets, spreadsheets or other documentation that demonstrates that it meets Requirement R10.

R11. Each Generator Owner shall transmit the generator underfrequency trip setting and time delay within 45 calendar days of the Planning Coordinator's request. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M11. Each Generator Owner shall provide evidence such as emails, letters or other dated documentation that demonstrates that it meets Requirement R11.

R12. Each Generator Owner with a new generating unit, or an existing generator increasing its net capability by greater than 10% shall: *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning]*

- **12.1** Design measures to prevent the generating unit from tripping directly or indirectly for underfrequency conditions above the appropriate generator tripping threshold curve in Figure 2.
- **12.2** Design auxiliary system(s) or devices used for the control and protection of auxiliary system(s), necessary for the generating unit operation such that they will not trip the generating unit during underfrequency conditions above the appropriate generator underfrequency trip protection setting threshold curve in Figure 2.

M12. Each Generator Owner shall provide evidence such as reports, data sheets, specifications, memorandum or other documentation that demonstrates that it meets Requirement R12.

R13. For existing non-nuclear units in service prior to July 1, 2015, that have underfrequency protections set to trip above the appropriate curve in Figure 2: *[Violation Risk Factor: High] [Time Horizon: Long Term Planning]*

13.1 Each Generator Owner shall set the underfrequency protection to operate at the lowest frequency allowed by the plant design and licensing limitations.

13.2 Each Generator Owner shall transmit the existing underfrequency settings and any changes to the underfrequency settings along with the technical basis for the settings to the Planning Coordinator.

13.3 Each Planning Coordinator in Ontario, Québec and the Maritime Provinces shall arrange for compensatory load shedding, in accordance with Attachment A and as provided by a Distribution Provider or Transmission Owner, that is adequate to compensate for the loss of generator(s) due to early tripping that is within the UFLS island identified by the Planning Coordinator in Requirement R2.

13.4 Each Generator Owner in the ISO-NE Planning Coordinator area and in NYISO Planning Coordinator area shall arrange for compensatory load shedding, in accordance with Attachment B and as provided by a Distribution Provider or Transmission Owner, that is adequate to compensate for the loss of generator(s) due to early tripping that is within the UFLS island identified by the Planning Coordinator in Requirement R2.

M13. Each Generator Owner with existing non-nuclear units in service prior to July 1, 2015 which have underfrequency tripping that is not compliant with Requirement R10 shall provide evidence such as reports, spreadsheets, memorandum or dated documentation demonstrating that it meets Requirement R13.

R14. Each Planning Coordinator in Ontario, Quebec and the Maritime provinces shall apply the criteria described in Attachment A to determine the compensatory load shedding that is required in Requirement R13.3 for generating units in its respective NPCC area. *[Violation Risk Factor: High] [Time Horizon: Long Term Planning]*

M14. Each Planning Coordinator in Ontario, Quebec and Maritime provinces shall provide evidence such as reports, memorandum or other documentation that demonstrates that it followed the methodology described in Attachment A and meets Requirement R14.

R15. Each Generator Owner, Distribution Provider or Transmission Owner within the ISO-NE Planning Coordinator area and in NYISO Planning Coordinator Area shall apply the criteria described in Attachment B to determine the compensatory load shedding that

is required in Requirement R13.4 for generating units in its respective NPCC area. *[Violation Risk Factor: High] [Time Horizon: Long Term Planning]*

M15. Each Generator Owner, Distribution Provider or Transmission Owner within the Planning Coordinator area of ISO-NE or the NYISO shall provide evidence such as reports, memorandum, or other documentation that demonstrates that it followed the methodology described in Attachment B and meets Requirement R15.

R16. Each Generator Owner of existing nuclear generating plants with units that have underfrequency relay threshold settings above the Eastern Interconnection generator tripping curve in Figure 2 based on their licensing design shall: *[Violation Risk Factor: High] [Time Horizon: Long Term Planning]*

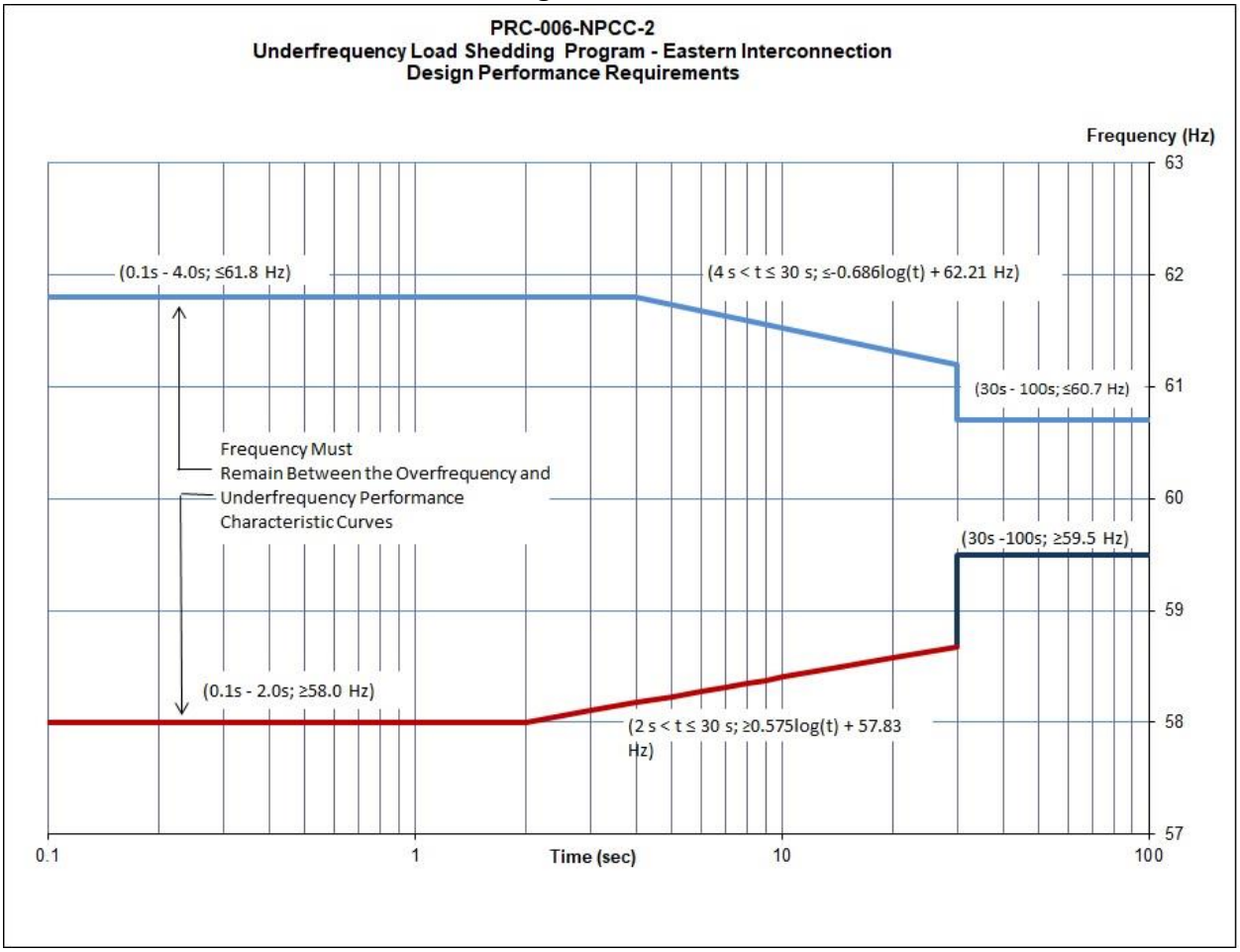
16.1 Set the underfrequency protection to operate at a frequency setting that is as low as possible in accordance with the plant design and licensing limitations but not greater than 57.8 Hz.

16.2 Set the frequency trip setting upper tolerance to no greater than + 0.1 Hz.

16.3 Transmit the initial frequency trip setting and any changes to the setting and the technical basis for the settings to the Planning Coordinator.

M16. Each Generator Owner of nuclear units that have generator trip settings above the generator trip curve in Figure 2 shall provide evidence such as letters, reports and dated documentation that demonstrates that it meets Requirement R16.

Figure 1



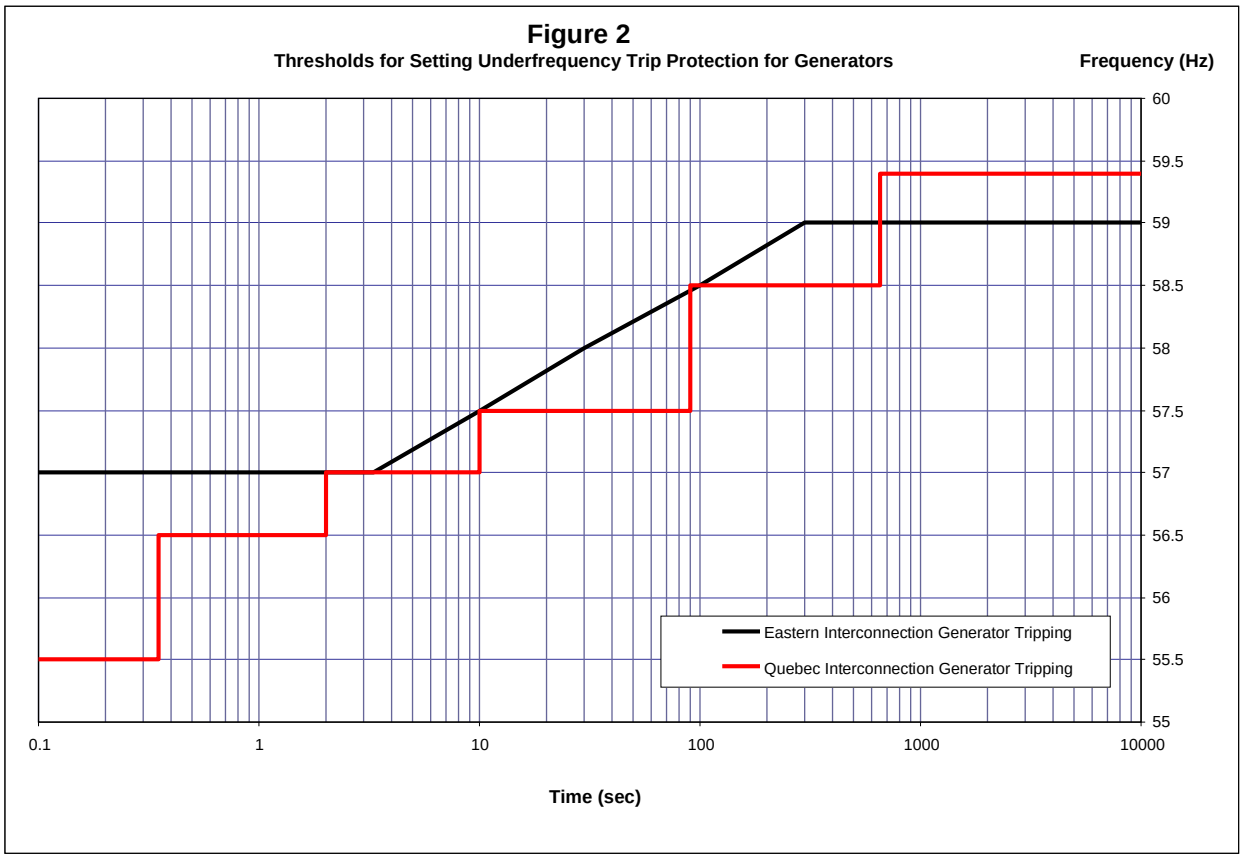
NERC PRC-006 Overfrequency Requirements (Continent-Wide Standard on UFLS)
NERC PRC-006 Underfrequency Requirements (Continent-Wide Standard on UFLS) - out to 30 seconds only
NERC PRC-006-NPCC Underfrequency Requirements (Regional Standard on UFLS)- more stringent than Content-Wide Standard from 30 - 100 seconds

Curve Data:

Overfrequency Requirements		**Source**
t ≤ 4 s	f = 61.8 Hz	NERC PRC-006 (Continent-Wide Standard on UFLS)
4 s < t ≤ 30 s	f = -0.686log(t) + 62.21 Hz	
t > 30 s	f = 60.7 Hz	

Underfrequency Requirements		**Source**
t ≤ 2 s	f = 58.0 Hz	NERC PRC-006 (Continent-Wide Standard on UFLS)
2 s < t ≤ 30 s	f = 0.575log(t) + 57.83 Hz	
t > 30 s	f = 59.5 Hz	NERC PRC-006-NPCC (Regional Standard on UFLS)

Figure 2
PRC-006-NPCC-2
Underfrequency Load Shedding Program – Thresholds for Setting Underfrequency Trip Protection for Generators



C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority:

Northeast Power Coordinating Council

1.2. Evidence Retention:

The Distribution Provider and Transmission Owner shall keep evidences for three calendar years for Measures 2, 3, 4, 5, 8, and 9.

The Planning Coordinator shall keep evidence for three calendar years for Measures 1, 2, 5, 6, and 7.

The Distribution Provider, Transmission Owner, and Generator Owner shall keep evidences for three calendar years for Measures 15.

The Generator Owner shall keep evidence for three calendar years for Measures 10, 11, 12, 13, and 16.

1.3. Compliance Monitoring and Enforcement Program:

Compliance Audit

Self-Certification

Spot Checking

Compliance Violation Investigation

Self-Reporting

Complaints

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	N/A	N/A	N/A	The Planning Coordinator failed to design an UFLS program having performance characteristics that prevent frequency from remaining below 59.5 Hz in accordance with Figure 1.
R2.	The Planning Coordinator provided its UFLS island boundaries, as identified per the NERC continent-wide PRC-006 Standard on UFLS but did so more than 30 calendar days and up to and including 40 days following a request.	The Planning Coordinator provided its UFLS island boundaries, as identified per the NERC continent-wide PRC-006 Standard on UFLS but did so more than 40 calendar days but less than and including 50 days following a request.	The Planning Coordinator provided its UFLS island boundaries, as identified per the NERC continent-wide PRC-006 Standard on UFLS but did so more than 50 calendar days but less than and including 60 days following a request.	The Planning Coordinator failed to provide its UFLS island boundaries, as identified per the NERC continent-wide PRC-006 Standard on UFLS. within 60 calendar days following a request.
R3.	The Distribution Provider or Transmission Owner failed to apply appropriate settings on 20% or less of the relays identified as included in the UFLS program, or amount of load tripped is within 10% deviation from the required amount of Load required to be shed at each stage	The Distribution Provider or Transmission Owner failed to apply appropriate settings on 20%-40% of the relays identified as included in the UFLS program, or amount of load tripped is within 20% deviation from the required amount of Load required to be shed at each stage m	The Distribution Provider or Transmission Owner failed to apply appropriate settings on 40%-60% of the relays identified as included in the UFLS program, or amount of load tripped is within 30% deviation from the required amount of Load required to be shed at each stage.	The Distribution Provider or Transmission Owner failed to apply appropriate settings on > 60% of the relays identified as included in the UFLS program, or amount of load tripped has a > 30% deviation from the required amount of Load required to be shed at each stage
R4.	The Distribution Provider or Transmission Owner that cannot meet the tolerances and/or number of stages and frequency set points specified in the UFLS Program fulfilled its obligations for	The Distribution Provider or Transmission Owner that cannot meet the tolerances and/or number of stages and frequency set points specified in the UFLS Program fulfilled its obligations for	The Distribution Provider or Transmission Owner that cannot meet the tolerances and/or number of stages and frequency set points specified in the UFLS Program fulfilled its obligations but exceeded the permissible	The Distribution Provider or Transmission Owner that cannot meet the tolerances and/or number of stages and frequency set points specified in the UFLS Program failed to meet all of items in Requirement 5 within 60

	Requirement R5, Parts %.1 through Part 5.4 but exceeded the permissible time frame for one or more of the 4 items by a period of up to 10 calendar days but less than or equal to 20 calendar days.	Requirement R5, Parts %.1 through Part 5.4 but exceeded the permissible time frame for one or more of the 4 items within a time greater than 20 calendar days but less than or equal to 30 calendar days.	time frame for one or more of the 4 items within a time greater than 30 calendar days but less than or equal to 60 calendar days.	calendar days of permissible time for each item.
R5.	The Planning Coordinator developed or reviewed settings for inhibit thresholds at least once per five calendar years, for less than 100% but more than (and including) 95% of relays within its region's UFLS program.	The Planning Coordinator developed or reviewed settings for inhibit thresholds at least once per five calendar years, for less than 95% but more than (and including) 90% of relays within its region's UFLS program.	The Planning Coordinator developed or reviewed settings for inhibit thresholds at least once per five calendar years, for less than 90% but more than (and including) 85% of relays within its region's UFLS program.	The Planning Coordinator developed or reviewed settings for inhibit thresholds at least once per five calendar years, for less than 85% of relays within its region's UFLS program.
R6.	The Planning Coordinator provided to a Transmission Owner or Distribution Provider within its Planning Coordinator area the applicable inhibit thresholds more than 30 calendar days and up to and including 40 calendar days of any changes.	The Planning Coordinator provided to a Transmission Owner or Distribution Provider within its Planning Coordinator area the applicable inhibit thresholds more than 40 calendar days but less than and including 50 calendar days of any changes.	The Planning Coordinator provided to a Transmission Owner or Distribution Provider within its Planning Coordinator area the applicable inhibit thresholds more than 50 calendar days but less than and including 60 calendar days of any changes.	The Planning Coordinator failed to provide to a Transmission Owner or Distribution Provider within its Planning Coordinator area the applicable inhibit thresholds within 60 calendar days after any changes
R7.	The Distribution Provider or Transmission Owner developed and submitted its implementation plan more than 90 calendar days and up to and including 100 calendar days following the request.	The Distribution Provider or Transmission Owner developed and submitted its implementation plan more than 100 calendar days and up to and including 110 calendar days following the request.	The Distribution Provider or Transmission Owner developed and submitted its implementation plan more than 110 calendar days and up to and including 120 calendar days following the request.	The Distribution Provider or Transmission Owner failed to develop and submit its implementation plan within 120 days following the request.
R8.	Implemented the inhibit threshold settings provided by the Planning Coordinator in accordance with the Planning Coordinator approved implementation plan for	The Distribution Provider or Transmission Owner implemented the inhibit threshold settings provided by the Planning Coordinator in accordance with	The Distribution Provider or Transmission Owner implemented the inhibit threshold settings provided by the Planning Coordinator in accordance with	The Distribution Provider or Transmission Owner implemented the inhibit threshold settings provided by the Planning Coordinator in accordance with

	less than 100% but more than (and including) 95% of UFLS relays.	the Planning Coordinator approved implementation plan for less than 95% but more than (and including) 90% of UFLS relays.	the Planning Coordinator approved implementation plan for less than 90% but more than (and including) 85% of UFLS relays.	the Planning Coordinator approved implementation plan for less than 85% of UFLS relays.
R9.	The Distribution Provider or Transmission Owner provided to its Planning Coordinator documentation of the actual net Load that would have been shed by the UFLS relays at each UFLS stage as described in Requirement R11 more than 15 calendar months but less than (and including) 16 calendar months since last update.	The Distribution Provider or Transmission Owner provided to its Planning Coordinator documentation of the actual net Load that would have been shed by the UFLS relays at each UFLS stage as described in Requirement R11 more than 16 calendar months but less than (and including)17 calendar months since last update.	The Distribution Provider or Transmission Owner provided to its Planning Coordinator documentation of the actual net Load that would have been shed by the UFLS relays at each UFLS stage as described in Requirement R11 more than 17 calendar months but less than (and including)18 calendar months since last update.	The Distribution Provider or Transmission Owner failed to provide to its Planning Coordinator documentation of the actual net Load that would have been shed by the UFLS relays at each UFLS stage as described in Requirement R11 within 18 calendar months since last update.
R10.	N/A	N/A	N/A	The Generator Owner did not set each generator underfrequency trip relay, if so equipped, on or below the appropriate generator underfrequency trip protection settings threshold curve in Figure 2, except as otherwise exempted.
R11.	The Generator Owner transmitted the generator underfrequency trip setting and time delay more than 45calendar days and less than (and including) 55 calendar days of the Planning Coordinator's request.	The Generator Owner transmitted the generator underfrequency trip setting and time delay more than 55 calendar days and less than (and including) 65 calendar days of the Planning Coordinator's request.	The Generator Owner transmitted the generator underfrequency trip setting and time delay more than 65 calendar days and less than (and including) 75 calendar days of the Planning Coordinator's request.	The Generator Owner failed to transmit the generator underfrequency trip setting and time delay within 75 calendar days of the Planning Coordinator's request.
R12.	N/A	N/A	The Generator Owner with a new generating unit, or an existing	The Generator Owner with a new generating unit, or an existing generator increasing its net

			generator increasing its net capability by greater than 10%: Did not fulfill the obligation of Requirement R12; Part 12.1 OR Did not fulfill the obligation of Requirement R12, Part 12.2.	capability by greater than 10%, did not fulfill the obligations of Requirement R12, Part 12.1 and Part 12.2.
R13.	N/A	The Generator Owner failed to transmit the existing underfrequency settings and any changes to the underfrequency settings along with the technical basis for the settings to the Planning Coordinatoras specified in Requirement R13, Part 13.2.	The Generator Owner failed to set the underfrequency protection to operate at the lowest frequency allowed by the plant design and licensing limitations a specified in Requirement 13, Part 13.1	The Planning Coordinator in Ontario, Québec and the Maritime Provinces or the Generator Owner within the ISO-NE and in NYISO Planning Coordinator areas failed to arrange for compensatory load shedding as specified in Requirement R13, Part 13.3.
R14.	N/A	N/A	N/A	The Planning Coordinator did not apply the criteria described in Attachment A to determine the compensatory load shedding that is required.
R15.	N/A	N/A	N/A	The Generator Owner, Distribution Provider, or Transmission Owner did not apply the criteria described in Attachment B to determine the compensatory load shedding that is required.
R16.	N/A	The Generator Owner failed to transmit the initial frequency trip setting and any changes to the setting and the technical basis for the settings to the Planning	The Generator Owner: Failed to set the underfrequency protection as specified in Requirement R16; Part 16.1 OR	The Generator Owner did not fulfill the obligations of Requirement R16, Part 16.1 and Part 16.2.

		Coordinator as specified in Requirement R16, Part 16.3.	Failed to set the frequency trip setting upper tolerance as specified in Requirement R16, Part 16.2.	

D. Regional Variances

None.

E. Associated Documents

Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	2-9-2012	Adopted by Board of Trustees	
2	6-23-2015	RSAR Submitted	
2	11-5-2019	Adopted by the NERC Board of Trustees	
2	2-18-2020	FERC issued letter order approving PRC-006-NPCC-2. Docket No. RD20-1-000	

Standard Attachments

PRC-006-NPCC-2 Attachment A

Compensatory Load Shedding Criteria for Ontario, Quebec, and the Maritime Provinces:

The Planning Coordinator in Ontario, Quebec and the Maritime provinces is responsible for establishing the compensatory load shedding requirements for all existing non-nuclear units in its NPCC area with underfrequency protections set to trip above the appropriate curve in Figure 2. In addition, it is the Planning Coordinator's responsibility to communicate these requirements to the appropriate Distribution Provider or Transmission Owner and to ensure that adequate compensatory load shedding is provided in all UFLS islands in which the unit may operate.

The methodology below provides a set of criteria for the Planning Coordinator to follow for determining compensatory load shedding requirements as part of its UFLS Assessment based on the NERC PRC Standard on UFLS:

1. The Planning Coordinator shall identify, compile and maintain a list of all existing non-nuclear generating units in their Planning Coordinator area that were in service prior to the effective date of the regional Standard (July 1, 2015 PRC-006-NPCC-1). The list must indicate generating units, if any, that have their underfrequency protections set to trip above the appropriate curve in Figure 2. Generating Units not appearing on the list as of the effective date of Version 1 of the regional standard, as shown above, must have their Underfrequency protections set to trip on or below the appropriate curve in Figure 2. The list shall include the following information for each unit:

    1.1 Generator name and generating capacity
    1.2 Underfrequency protection trip settings, including frequency trip set points and time delays
    1.3 Physical and electrical location of the unit
    1.4 All islands within which the unit may operate

2. For each generating unit identified in (1) above, the Planning Coordinator shall establish the requirements for compensatory load shedding based on criteria outlined below:

    2.1 Arrange for a Distribution Provider or Transmission Owner that owns UFLS relays within the island(s) identified by the Planning Coordinator within which the generator may operate to provide compensatory load shedding.

    2.2 In Ontario and in the Maritime provinces, the compensatory load shedding that is provided by the Distribution Provider or Transmission Owner shall be in

addition to the amount that the Distribution Provider or Transmission Owner is required to shed as specified in Requirement R4.

2.3 The compensatory load shedding shall be provided at the UFLS program stage (or threshold stage for Quebec) with a frequency threshold setting that corresponds to the highest frequency at which the subject generator will trip above the appropriate curve in Figure 2 during an underfrequency event. If the highest frequency at which the subject generator will trip above the appropriate curve in Figure 2 does not correspond to a specific UFLS program stage threshold setting, the compensatory load shedding shall be provided at the UFLS program stage with a frequency threshold setting that is higher than the highest frequency at which the subject generator will trip above the appropriate curve in Figure 2.

2.4 The amount of compensatory load shedding shall be equivalent (±5%) to the average net generator megawatt output for the prior two calendar years, as specified by the Planning Coordinator, plus expected station loads to be transferred to the system upon loss of the facility. The net generation output should only include those hours when the unit was a net generator to the electric system.

In the specific instance of a generating unit that has been interconnected to the electric system for less than two calendar years, the amount of compensatory load shedding shall be equivalent (±5%) to the maximum claimed seasonal capability of the generator over two calendar years, plus expected station loads to be transferred to the system upon loss of the facility.

PRC-006-NPCC-2 Attachment B

Compensatory Load Shedding Criteria for ISO-NE and NYISO:

The Generator Owner in the New England states or New York State are responsible for establishing a compensatory load shedding program for all existing non-nuclear units with underfrequency protection set to trip above the appropriate curve in Figure 2 of this standard. The Generator Owner shall follow the methodology below to determine compensatory load shedding requirements:

1. The Generator Owner shall identify, compile, and maintain a list of all of its existing non-nuclear generating units that were in service prior to the effective date of the regional Standard (July 1, 2015 PRC-006-NPCC-1). The list must indicate the Generator Owner's generating units, if any, which have their underfrequency protections set to trip above the appropriate curve in Figure 2. Generating Units not appearing on the list as of the effective date of Version 1 of the regional standard, as shown above, must have their Underfrequency protections set to trip on or below the appropriate curve in Figure 2. The list shall include the following information associated with each unit:

    1.1 Generator name and generating capacity
    1.2 Underfrequency protection trip settings, including frequency trip set points and time delays
    1.3 Physical and electrical location of the unit
    1.4 Smallest island within which the unit may operate as identified by the Planning Coordinator in Requirement R1 of this Standard.

2. For each generating unit identified in (1) above, the Generator Owner shall establish the requirements for compensatory load shedding based on criteria outlined below:

    2.1 In cases where a Distribution Provider or Transmission Owner has coordinated protection settings with the Generator Owner to cause the generator to trip above the appropriate curve in Figure 2, the Distribution Provider or Transmission Owner is responsible to provide the appropriate amount of compensatory load to be shed within the same and smallest island identified by the Planning Coordinator in Requirement R1 of this standard.

    2.2 In cases where a Generator Owner has a generator that cannot physically meet the set points defined by the appropriate curve in Figure 2, the Generator Owner shall arrange for a Distribution Provider or Transmission Owner to provide the appropriate amount of compensatory load to be shed within the same and smallest island identified by the Planning Coordinator in Requirement R1 of this standard.

2.3 The compensatory load shedding that is provided by the Distribution Provider or Transmission Owner shall be in addition to the amount that the Distribution Provider or Transmission Owner is required to shed as specified in Requirement R4.

2.4 The compensatory load shedding shall be provided at the UFLS program stage with the frequency threshold setting at or closest to but above the frequency at which the subject generator will trip.

2.5 The amount of compensatory load shedding shall be equivalent (±5%) to the average net generator megawatt output for the prior two calendar years, as specified by the Planning Coordinator, plus expected station loads to be transferred to the system upon loss of the facility. The net generation output should only include those hours when the unit was a net generator to the electric system.

In the specific instance of a generating unit that has been interconnected to the electric system for less than two calendar years, the amount of compensatory load shedding shall be equivalent (±5%) to the maximum claimed seasonal capability of the generator over two calendar years, plus expected station loads to be transferred to the system upon loss of the facility.

PRC-006-NPCC-2 Attachment C

UFLS Table 1: Eastern Interconnection Distribution Providers and Transmission Owners with 100 MW[2] or more of peak net Load shall implement a UFLS program with the following attributes:					
UFLS Stage	Frequency Threshold (Hz)	Minimum Relay Time Delay (s)	Total Nominal Operating Time (s)[1]	Load Shed at Stage as % of TO or DP Load	Cumulative Load Shed as % of TO or DP Load
1	59.5	0.10	0.30	6.5 – 7.5	6.5 – 7.5
2	59.3	0.10	0.30	6.5 – 7.5	13.5 – 14.5
3	59.1	0.10	0.30	6.5 – 7.5	20.5 – 21.5
4	58.9	0.10	0.30	6.5 – 7.5	27.5 – 28.5
5	59.5	0.10	10.0	2 - 3	29.5 – 31.5

UFLS Table 2: Eastern Interconnection Distribution Providers and Transmission Owners with 50 MW[2] or more and less than 100 MW[2] of peak net Load shall implement a UFLS program with the following attributes:					
UFLS Stage	Frequency Threshold (Hz)	Minimum Relay Time Delay (s)	Total Nominal Operating Time (s)[1]	Load Shed at Stage as % of TO or DP Load	Cumulative Load Shed as % of TO or DP Load
1	59.5	0.10	0.30	14 – 25	14 – 25
2	59.1	0.10	0.30	14 – 25	28 – 50

1. The total nominal operating time includes the underfrequency relay operating time plus any interposing auxiliary relay operating times, communication times, and the rated breaker interrupting time. The underfrequency relay operating time is measured from the time when frequency passes through the frequency threshold setpoint, using a test rate of frequency decay of 0.2 Hz per second. If the relay operating time is dependent on the rate of frequency decay, the underfrequency relay operating time and any subsequent testing of the UFLS relays shall utilize a test rate of linear frequency decay of 0.2 Hz per second.

2. Peak net load shall be calculated as an average of the peak net load from the previous 3 years, excluding the current year.

UFLS Table 3: Eastern Interconnection Distribution Providers and Transmission Owners with 25 MW[2] or more and less than 50 MW[2] of peak net Load shall implement a UFLS program with the following attributes:					
UFLS Stage	Frequency Threshold (Hz)	Minimum Relay Time Delay (s)	Total Nominal Operating Time (s)[1]	Load Shed at Stage as % of TO or DP Load	Cumulative Load Shed as % of TO or DP Load
1	59.5	0.10	0.30	28 – 50	28 – 50

1. The total nominal operating time includes the underfrequency relay operating time plus any interposing auxiliary relay operating times, communication times, and the rated breaker interrupting time. The underfrequency relay operating time is measured from the time when frequency passes through the frequency threshold setpoint, using a test rate of frequency decay of 0.2 Hz per second. If the relay operating time is dependent on the rate of frequency decay, the underfrequency relay operating time and any subsequent testing of the UFLS relays shall utilize a test rate of linear frequency decay of 0.2 Hz per second.
2. Peak net load shall be calculated as an average of the peak net load from the previous 3 years, excluding the current year.

Rationale Box:

Standard PRC-006-3, R4 requires the Planning Coordinator to conduct a UFLS assessment at least once every five years. However, aside from a UFLS islanding event, it does not prescribe other factors or events which could warrant a new UFLS assessment in less than the five years time-frame.

PRC-006-NPCC-01 contained requirements if changes to load distribution impacted UFLS program performance (R21) but did not consider many other factors. The drafting team recommends retiring these requirements (R21, R22, R23) and replacing them with the following guidance.

Significant variations in the following factors could require a Planning Coordinator to conduct a new assessment:

- Changes to the BES that could modify the creation of islands or the severity of events such as new transmission topologies, revised protection schemes or new or revised RAS.
- Unforeseen islanding event
- Real and reactive load distribution (including changes to location of compensatory load shedding)
- Transmission Owner or Distribution Provider's inability to implement the UFLS program within the stated tolerances
- Load characteristics in particular frequency responsive load
- Automatic load restoration
- Generation geographical distribution
- Generator trip settings
- Generation mix in particular non-BES generation that may not be subject to frequency ride-through criteria
- Generator dynamic modeling
- Dynamic VAR device modeling
- HVDC dynamic modeling

Rationale for Requirement R1: Figure 1 of this document shows the NPCC underfrequency criteria for the Eastern Interconnection portion of NPCC. Figure 1 also shows the NERC criteria as defined in the NERC PRC Standard on UFLS.

Rationale for Requirement R5: An inhibit function provides supervisory control over a UFLS relay. For example, an undervoltage inhibit feature prevents UFLS relay operation if the sensed voltage decreases below an adjustable setting. An undervoltage inhibit function is intended to prevent operation of a UFLS relay when the transmission supply is lost to distribution station feeding many induction motors. Following loss of the transmission supply, motors may support the voltage while the motors coast down in speed. The motors coasting down (ringing down) will look like an underfrequency event to the relay. The inhibit setting is set to a voltage above which the motor load is expected to sustain. This prevents the underfrequency relay from

tripping and locking out distribution feeder breakers supplying the motor load, between the time the transmission supply line trips and the time when the line recloses to restore the load. Voltages sustained by motors that are coasting down (e.g. 0.70 pu) are typically much lower than voltages at which the UFLS relays are required to operate to meet UFLS performance criteria. However, motor loads supplied by cable networks typically have higher ring down voltages because of cable charging. Therefore, care must be taken so that the voltage inhibit setting is not higher than the voltage at which UFLS relays are required to operate to meet UFLS performance criteria.

Rationale for Requirement R9: Ideally, the amount of load to be shed in each stage of the UFLS program for every entity should perfectly match that prescribed in this Standard, for all phases of the load cycle, i.e., seasonal (summer vs. winter), weekly (weekday vs. weekend vs. holidays), daily (morning, noon, and night), etc. for all of the identified islands. Practically, however, this is obviously not possible because the load cycles of the various areas and sub-areas within any given island do not perfectly track the load cycle of the overall island. The UFLS program, on the other hand, is designed based on peak conditions for the overall island. The percentages of actual load shedding that would occur for any conditions other than peak, therefore, can only approximate that prescribed in the Standard. To that end, Requirement R11 requires entities to document measured loads in the UFLS program coincident with their own annual peak, whether or not that peak occurs at the same time or in the same season as the peak of the identified island in which their load resides. Using individual entity peaks vs. overall island peaks provides a consistent approach for accounting purposes among the very entities that are responsible for designing and maintaining their UFLS programs.

Appendix PRC-006-NPCC-2-QC-1

Specific provisions applicable in Québec for standard
PRC-006-NPCC-2 – Automatic Underfrequency Load Shedding

This appendix establishes specific provisions for the application of the standard in Québec. Provisions of the standard and of this appendix must be read jointly for comprehension and interpretation purposes. Where the standard and appendix differ, the appendix shall prevail.

A. Introduction

1. Title: No specific provisions.

2. Number: No specific provisions.

3. Purpose: No specific provisions.

4. Applicability:

4.1. Functional Entities

No specific provisions.

4.2. Facilities

For Planning Coordinators and Generator Owners, the applicable generation facilities for this standard are the generation Facilities of the Main Transmission System (RTP).

5. Effective date:

5.1.	Adoption of the standard by the Régie de l'énergie:	February 23, 2021
5.2.	Adoption of this appendix by the Régie de l'énergie:	February 23, 2021
5.3.	Effective date of the standard and of this appendix in Québec:	April 1st, 2021

B. Requirements and Measures

No specific provisions.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

In Québec, "Compliance Enforcement Authority" means the Régie de l'énergie in its roles of monitoring and enforcing compliance with respect to the Reliability Standard and to this appendix.

1.2. Evidence Retention

No specific provisions.

1.3. Compliance Monitoring and Enforcement Program

The Régie de l'énergie establishes the monitoring processes used to evaluate data or information for the purpose of determining compliance or non-compliance with the Reliability Standard and with this appendix.

Violation Severity Levels

No specific provisions.

D. Regional Variances

No specific provisions.

E. Associated Documents

No specific provisions.

Standard Attachments

No specific provisions.

Version history

Version	Date	Action	Change tracking
1	February 23, 2021	New appendix	New

A. Introduction

1. **Title:** Undervoltage Load Shedding

2. **Number:** PRC-010-2

3. **Purpose:** To establish an integrated and coordinated approach to the design, evaluation, and reliable operation of Undervoltage Load Shedding Programs (UVLS Programs).

4. **Applicability:**

   4.1. Functional Entities:

   4.1.1 Planning Coordinator.

   4.1.2 Transmission Planner.

   4.1.3 Undervoltage load shedding (UVLS) entities – Distribution Providers and Transmission Owners responsible for the ownership, operation, or control of UVLS equipment as required by the UVLS Program established by the Transmission Planner or Planning Coordinator.

5. **Effective Date:** See Project 2008-02.2 Implementation Plan.

B. Requirements and Measures

R1. Each Planning Coordinator or Transmission Planner that is developing a UVLS Program shall evaluate its effectiveness and subsequently provide the UVLS Program's specifications and implementation schedule to the UVLS entities responsible for implementing the UVLS Program. The evaluation shall include, but is not limited to, studies and analyses that show: *[Violation Risk Factor: High] [Time Horizon: Long-term Planning]*

1.1. The implementation of the UVLS Program resolves the identified undervoltage issues that led to its development and design.

1.2. The UVLS Program is integrated through coordination with generator voltage ride-through capabilities and other protection and control systems, including, but not limited to, transmission line protection, autoreclosing, Remedial Action Schemes, and other undervoltage-based load shedding programs.

M1. Acceptable evidence may include, but is not limited to, date-stamped studies and analyses, reports, or other documentation detailing the effectiveness of the UVLS Program, and date-stamped communications showing that the UVLS Program specifications and implementation schedule were provided to UVLS entities.

R2. Each UVLS entity shall adhere to the UVLS Program specifications and implementation schedule determined by its Planning Coordinator or Transmission Planner associated with UVLS Program development per Requirement R1 or with any Corrective Action Plans per Requirement R5. *[Violation Risk Factor: High] [Time Horizon: Long-term Planning]*

M2. Acceptable evidence must include date-stamped documentation on the completion of actions and may include, but is not limited to, identifying the equipment armed with UVLS relays, the UVLS relay settings, associated Load summaries, work management program records, work orders, and maintenance records.

R3. Each Planning Coordinator or Transmission Planner shall perform a comprehensive assessment to evaluate the effectiveness of each of its UVLS Programs at least once every 60 calendar months. Each assessment shall include, but is not limited to, studies and analyses that evaluate whether: *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

3.1. The UVLS Program resolves the identified undervoltage issues for which the UVLS Program is designed.

3.2. The UVLS Program is integrated through coordination with generator voltage ride-through capabilities and other protection and control systems, including, but not limited to, transmission line protection, autoreclosing, Remedial Action Schemes, and other undervoltage-based load shedding programs.

M3. Acceptable evidence may include, but is not limited to, date-stamped reports or other documentation detailing the assessment of the UVLS Program.

R4. Each Planning Coordinator or Transmission Planner shall, within 12 calendar months of an event that resulted in a voltage excursion for which its UVLS Program was designed to operate, perform an assessment to evaluate: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

4.1. Whether its UVLS Program resolved the undervoltage issues associated with the event, and

4.2. The performance (i.e., operation and non-operation) of the UVLS Program equipment.

M4. Acceptable evidence may include, but is not limited to, date-stamped event data, event analysis reports, or other documentation detailing the assessment of the UVLS Program and associated equipment.

R5. Each Planning Coordinator or Transmission Planner that identifies deficiencies during an assessment performed in either Requirement R3 or R4 shall develop a Corrective Action Plan to address the deficiencies and subsequently provide the Corrective Action Plan, including an implementation schedule, to UVLS entities within three calendar months of completing the assessment. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M5. Acceptable evidence must include a date-stamped Corrective Action Plan that addresses identified deficiencies and may also include date-stamped reports or other documentation supporting the Corrective Action Plan. Evidence should also include date-stamped communications showing that the Corrective Action Plan and an associated implementation schedule were provided to UVLS entities.

R6. Each Planning Coordinator that has a UVLS Program in its area shall update a database containing data necessary to model the UVLS Program(s) in its area for use in event analyses and assessments of the UVLS Program at least once each calendar year. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M6. Acceptable evidence may include, but is not limited to, date-stamped spreadsheets, database reports, or other documentation demonstrating a UVLS Program database was updated.

R7. Each UVLS entity shall provide data to its Planning Coordinator according to the format and schedule specified by the Planning Coordinator to support maintenance of a UVLS Program database. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M7. Acceptable evidence may include, but is not limited to, date-stamped emails, letters, or other documentation demonstrating data was provided to the Planning Coordinator as specified.

R8. Each Planning Coordinator that has a UVLS Program in its area shall provide its UVLS Program database to other Planning Coordinators and Transmission Planners within its Interconnection, and other functional entities with a reliability need, within 30 calendar days of a written request. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M8. Acceptable evidence may include, but is not limited to, date-stamped emails, letters, or other documentation demonstrating that the UVLS Program database was provided within 30 calendar days of receipt of a written request.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The Planning Coordinator, Transmission Planner, Distribution Provider, and Transmission Owner shall keep data or evidence to show compliance as identified

below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

The applicable entity shall retain documentation as evidence for six calendar years.

If an applicable entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved, or for the time specified above, whichever is longer.

The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes

"Compliance Monitoring and Assessment Processes" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated reliability standard.

1.4. Additional Compliance Information

None.

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	Long-term Planning	High	N/A	N/A	N/A	The applicable entity that developed the UVLS Program failed to evaluate the program's effectiveness and subsequently provide the UVLS Program's specifications and implementation schedule to UVLS entities in accordance with Requirement R1, including the items specified in Parts 1.1 and 1.2.

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R2	Long-term Planning	High	N/A	N/A	The applicable entity failed to adhere to the UVLS Program specifications in accordance with Requirement R2. OR The applicable entity failed to adhere to the implementation schedule in accordance with Requirement R2.	The applicable entity failed to adhere to the UVLS Program specifications and implementation schedule in accordance with Requirement R2.
R3	Long-term Planning	Medium	N/A	N/A	N/A	The applicable entity failed to perform an assessment at least once during the 60 calendar months in accordance with Requirement R3, including the items specified in Parts 3.1 and 3.2.

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R4	Operations Planning	Medium	The applicable entity performed an assessment in accordance with Requirement R4 within a time period greater than 12 calendar months but less than or equal to 13 calendar months after an applicable event.	The applicable entity performed an assessment in accordance with Requirement R4 within a time period greater than 13 calendar months but less than or equal to 14 calendar months after an applicable event.	The applicable entity performed an assessment in accordance with Requirement R4 within a time period greater than 14 calendar months but less than or equal to 15 calendar months after an applicable event.	The applicable entity performed an assessment in accordance with Requirement R4 within a time period greater than 15 calendar months after an applicable event. OR The applicable entity failed to perform an assessment in accordance with Requirement R4.

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R5	Operations Planning	Medium	The applicable entity developed a Corrective Action Plan and provided it to UVLS entities in accordance with Requirement R5 but was late by less than or equal to 15 calendar days.	The applicable entity developed a Corrective Action Plan and provided it to UVLS entities in accordance with Requirement R5 but was late by more than 15 calendar days but less than or equal to 30 calendar days.	The applicable entity developed a Corrective Action Plan and provided it to UVLS entities in accordance with Requirement R5 but was late by more than 30 calendar days but less than or equal to 45 calendar days.	The applicable entity developed a Corrective Action Plan and provided it to UVLS entities in accordance with Requirement R5 but was late by more than 45 calendar days. OR The responsible entity failed to develop a Corrective Action Plan or provide it to UVLS entities in accordance with Requirement R5.

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R6	Operations Planning	Lower	The applicable entity updated the database in accordance with Requirement R6 but was late by less than or equal to 30 calendar days.	The applicable entity updated the database in accordance with Requirement R6 but was late by more than 30 calendar days but less than or equal to 60 calendar days.	The applicable entity updated the database in accordance with Requirement R6 but was late by more than 60 calendar days but less than or equal to 90 calendar days.	The applicable entity updated the database in accordance with Requirement R6 but was late by more than 90 calendar days. OR The applicable entity failed to update the database in accordance with Requirement R6.

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R7	Operations Planning	Lower	The applicable entity provided data in accordance with Requirement R7 but was late by less than or equal to 30 calendar days per the specified schedule. OR The applicable entity provided data in accordance with Requirement R7 but the data was not provided according to the specified format.	The applicable entity provided data in accordance with Requirement R7 but was late by more than 30 calendar days but less than or equal to 60 calendar days per the specified schedule.	The applicable entity provided data in accordance with Requirement R7 but was late by more than 60 calendar days but less than or equal to 90 calendar days per the specified schedule.	The applicable entity provided data in accordance with Requirement R7 but was late by more than 90 calendar days per the specified schedule. OR The applicable entity failed to provide data in accordance with Requirement R7.

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R8	Operations Planning	Lower	The applicable entity provided its UVLS Program database in accordance with Requirement R8 but was late by less than or equal to 15 calendar days.	The applicable entity provided its UVLS Program database in accordance with Requirement R8 but was late by more than 15 calendar days but less than or equal to 30 calendar days.	The applicable entity provided its UVLS Program database in accordance with Requirement R8 but was late by more than 30 calendar days but less than or equal to 45 calendar days.	The applicable entity provided its UVLS Program database in accordance with Requirement R8 but was late by more than 45 calendar days. OR The applicable entity failed to provide its UVLS Program database in accordance with Requirement R8.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
0	February 8, 2005	Adopted by NERC Board of Trustees	
0	April 1, 2005	Effective Date	
0	February 7, 2013	Adopted by NERC Board of Trustees	R2 and associated elements for retirement as part of the Paragraph 81 project (Project 2013-02) pending applicable regulatory approval.
1	November 13, 2014	Adopted by NERC Board of Trustees	Revisions made under Project 2008-02: Undervoltage Load Shedding (UVLS) & Underfrequency Load Shedding (UFLS) to address directive issued in FERC Order No. 763.
2	May 7, 2015	Adopted by NERC Board of Trustees	Revisions made under Project 2008-02.2: Undervoltage Load Shedding (UVLS): Misoperation to include UVLS equipment.

Guidelines and Technical Basis

Introduction

The standard drafting team provides the following discussion to support the approach to the standard. The information is meant to enhance the understanding of the reliability needs and deliverable expectations of each requirement, supported as necessary by technical principles and industry experience.

Guidelines for UVLS Program Definition

The definition for the term, “Undervoltage Load Shedding Program” or “UVLS Program” includes automatic load shedding programs that utilize only voltage inputs at locations where action is taken to shed load. As such, the failure of a single component is unlikely to affect the reliable operation of the program.

The UVLS Program definition excludes centrally controlled undervoltage-based load shedding, which utilizes inputs from multiple locations and may also utilize inputs other than voltages (such as generator reactive reserves, facility loadings, equipment statuses, etc.). The design and characteristics of a centrally controlled undervoltage-based load shedding system are the same as that of a Remedial Action Scheme (RAS), wherein load shedding is the remedial action. Therefore, just like for a RAS, the failure of a single component can compromise the reliable operation of centrally controlled undervoltage-based load shedding.

To ensure that the applicability of the standard includes only those undervoltage-based load shedding systems whose performance has an impact on system reliability, a UVLS Program must mitigate risk of one or more of the following: voltage instability, voltage collapse, or Cascading impacting the Bulk Electric System (BES). An example of a program that would not fall under this category is undervoltage-based load shedding installed to mitigate damage to equipment or local loads that are directly affected by the low voltage event.

Figure 1 below is an example of a BES subsystem for which a UVLS system could be used as a solution to mitigate various issues following the loss of the 345 kV double circuit line between buses A and B. If the consequence of this Contingency does not impact the BES by leading to voltage instability, voltage collapse, or Cascading, a UVLS system (installed at either, or both, bus B and D) used to mitigate this Contingency would not fall under the definition of a UVLS Program. However, if this same UVLS system is used to mitigate an Adverse Reliability Impact outside this contained area, it would be classified as a wide-area undervoltage problem and would fall under the definition of UVLS Program.

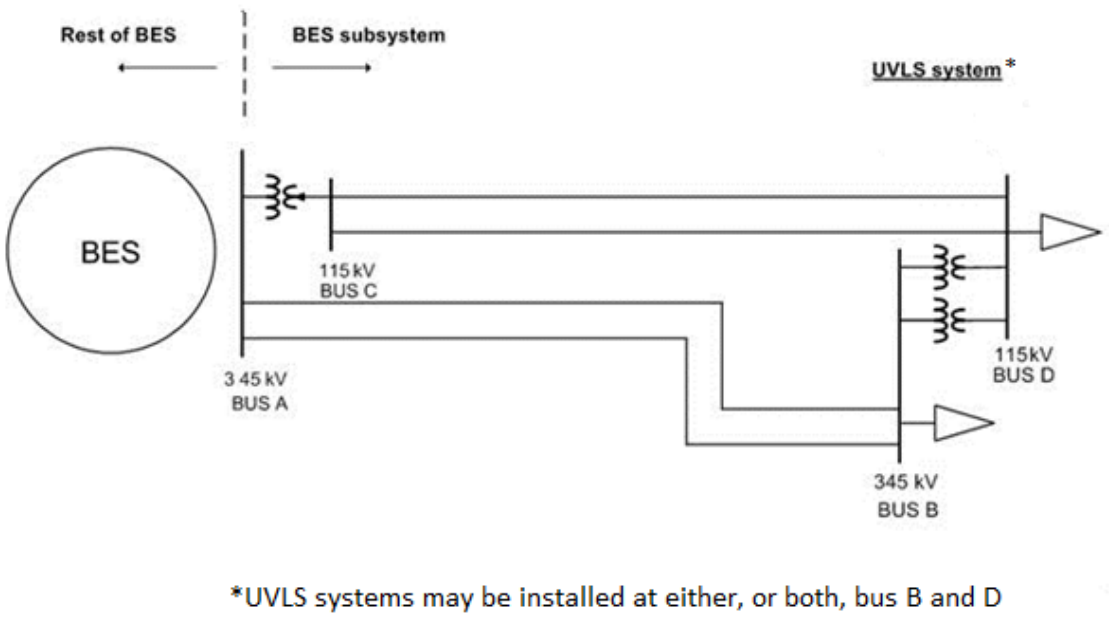


Figure 1: UVLS Subsystem

Guidelines for Requirements

Table 1 provides a high-level overview of the requirements contained in the standard.

Table 1: High-Level Requirement Overview

Requirement	Entity	Evaluate Program Effectiveness	Adhere to Program Specifications and Schedule	Perform Program Assessment (Periodic or Performance)	Develop a CAP to Address Program Deficiencies	Update and/or Share Program Data
R1	PC or TP	X				
R2	UVLS entity		X			
R3	PC or TP	X		X		
R4	PC or TP	X		X		
R5	PC or TP				X	
R6	PC					X
R7	UVLS entity					X
R8	PC					X

Guidelines for Requirement R1

A UVLS Program may be developed and implemented to either serve as a safety net system protection measure against unforeseen extreme Contingencies or to achieve specific system

performance for known transmission Contingencies for which dropping of load is allowed under Transmission Planning (TPL) Reliability Standards. Regardless of the purpose, it is important that the UVLS Program being implemented is effective in terms that it mitigates undervoltage conditions impacting the Bulk Electric System (BES), leading to voltage instability, voltage collapse, or Cascading. Consideration should be given to voltage set points and time delays, rate of voltage decay or recovery, power flow levels, etc. when designing a UVLS Program.

For the UVLS Program to be effective in achieving its goal, it is also necessary that the UVLS Program is coordinated with generator voltage ride-through capabilities and other protection and control systems that may have an impact on the performance of the UVLS Program. Some of these protection and control systems may include, but are not limited to, transmission line protection, RAS, other undervoltage-based load shedding programs, autoreclosing, and controls of shunt capacitors, reactors, and static voltampere-reactive systems (SVSs).

For example, if the purpose of a UVLS Program is to mitigate fault-induced delayed voltage recovery (FIDVR) events in a large load center that also includes local generation, it is important that such a UVLS Program is coordinated with local generators' voltage ride-through capabilities. Generators in the vicinity of a load center are critical to providing dynamic voltage support to the system during FIDVR events. To maximize the benefit of on-line generation, the best practice may be to shed load prior to generation trip. However, occasionally, it may be best to let generation trip prior to load shed. Therefore, the impact of generation tripping should be considered while designing a UVLS Program.

Another example that can be highlighted is the coordination of a UVLS Program with automatic shunt reactor tripping devices if there are any on the system. Most likely, any shunt reactors on the system will trip off automatically after some time delay during low voltage conditions. In such cases, shunt reactors should be tripped before the load is shed to preserve the system. This may require coordination of time delays associated with the UVLS Program with shunt reactor tripping devices.

The examples given above demonstrate that, for a UVLS Program to be effective, proper consideration should be given to coordination of a UVLS Program with generator ride-through capabilities and other protection and control systems.

Guidelines for Requirement R2

Once a Planning Coordinator (PC) or Transmission Planner (TP) has identified a need for a UVLS Program, the Planning Coordinator or Transmission Planner will develop a program that includes specifications and an implementation schedule, which are then provided to UVLS entities per Requirement R1. Specifications may include voltage set points, time delays, amount of load to be shed, and the location at which load needs to be shed. If UVLS entities do not implement the UVLS Program according to the specifications and schedule provided, the UVLS Program may not be effective and may not achieve its intended goal. The UVLS entity must document that all necessary actions were completed to implement the UVLS Program.

Similarly, when a Corrective Action Plan (CAP) to address UVLS Program deficiencies is developed by the Planning Coordinator or Transmission Planner and provided to UVLS entities per Requirement R5, UVLS entities must comply with the CAP and its associated implementation schedule to ensure that the UVLS Program is effective. The UVLS entity is required to complete the actions specified in the CAP, document the plan implementation, and retain the appropriate evidence to demonstrate implementation and completion.

Deferrals or other relevant changes to the UVLS Program specifications or CAP need to be documented so that the record includes not only what was planned, but what was implemented. Depending on the planning and documentation format used by the responsible entity, evidence of a successful execution could consist of signed-off work orders, printouts from work management systems, spreadsheets of planned versus completed work, timesheets, work inspection reports, paid invoices, photographs, walk-through reports, or other evidence.

For example, documentation of a CAP provides an auditable progress and completion confirmation for the identified UVLS Program deficiency:

CAP Example 1 - Corrective actions for a quick triggering problem; preemptive actions for similar installations:

The PC or TP obtains fault records from a UVLS entity that participates in its UVLS Program that indicate a group of UVLS relays triggered at the appropriate undervoltage level but with shorter delays than expected. The PC or TP directed the UVLS entity to schedule on-site inspections within three weeks. The results of the inspection confirmed that the delay-time programmed on the relays was 60 cycles instead of 90 cycles. The PC or TP then directed the UVLS entity to correct to a 90-cycle time delay setting of the UVLS relays identified to have shorter time delay settings within eight weeks.

Applicability to other UVLS relays: The PC or TP then developed a schedule with the UVLS entity to verify and adjust all remaining UVLS relays time delay settings within a one-year period.

The PC or TP verified completion of verification and adjustment of the time delay settings for all of the UVLS entity's equipment that participates in the PC or TP UVLS Program

CAP Example 2 - Corrective actions for a firmware problem; preemptive actions for similar installations:

The PC or TP obtains fault records on 6/4/2014 from a UVLS entity that participates in its UVLS Program. The UVLS entity also provided the fault records to the manufacturer, who responded on 6/11/2014 that the Misoperation[1] of the UVLS relay was caused by a bug in version 2 firmware, and recommended installing version 3 firmware. The PC or TP approved the UVLS entity's plan to schedule Version 3 firmware installation on 6/12/2014.

[1] Misoperation of Protection Systems reporting was initiated by the NERC Board of Trustees adopted NERC Rules of Procedure, Section 1600, Request for Data or Information. Refer to: *Request for Data of Information, Protection System Misoperation Data Collection*, August 14, 2014. http://www.nerc.com/pa/RAPA/ProctectionSystem Misoperations/PRC-004-3%20Section%201600%20Data%20Request_20140729.pdf.

Applicability to other UVLS relays: The PC or TP then developed a schedule with the UVLS entity to install firmware version 3 at all of the UVLS entity's UVLS relays that are determined to be programmed with version 2 firmware. The completion date was scheduled no-later-than 12/31/2014.

The firmware replacements were completed on 12/4/2014.

Guidelines for Requirement R3

In addition to the initial studies required to develop a UVLS Program, periodic comprehensive assessments (detailed analyses) are required to ensure its continued effectiveness. This assessment is required to be completed at least once every 60 calendar months to capture the accumulated effects of minor changes to the system that have occurred since the last assessment was completed. However, at any point in time, a Planning Coordinator or Transmission Planner may also determine that a material change[2] to system topology or operating conditions affects the performance of the UVLS Program and therefore necessitates the same comprehensive assessment. Regardless of the trigger, each assessment should include an evaluation of each UVLS Program to ensure the continued integration through coordination.

This comprehensive assessment complements the TPL-001-4 annual assessment requirement to evaluate the impact of protection systems. The 60-month period is the same time frame used in TPL-001-4 and in PRC-006-1.

As specified in Requirement R3, a comprehensive assessment must be performed at least once every 60 calendar months. If a Planning Coordinator or Transmission Planner conducts a comprehensive assessment sooner for the reasons discussed above, the 60-month time period would restart upon completion of this assessment.

Guidelines for Requirement R4

After a voltage excursion event, the goal of the assessment required in Requirement R4 is to evaluate: (1) whether the UVLS Program resolved the undervoltage issues, and (2) the performance of the UVLS Program equipment. The assessment should include event data analysis, such as the relevant sequence of events leading to the undervoltage conditions (e.g., Contingencies, operation of protection systems, and RAS) and field measurements useful to analyzing the behavior of the system. A comprehensive description of the UVLS Program operation should be presented, including conditions of the trigger (e.g., voltage levels, time delays) and amount of load shed for each affected substation. Assessment of the event is performed to evaluate the level of performance of the program for the event of interest and to identify deficiencies to be included in a CAP per Requirement R5. Misoperation of UVLS equipment is addressed as a deficiency. Reporting of UVLS equipment Misoperations are

[2] It is understood that the term material change is not transportable on a continent-wide basis. This determination must be made by the Planning Coordinator or Transmission Planner and should be accompanied by documentation to support the technical rationale for determining material changes.

addressed by the NERC *Request for Data and Information, Protection System Misoperation Data Collection*.[3]

The studies and analyses showing the effectiveness of the UVLS Program can be similar to what is required in Requirements R1 and R3, but should include a clear link between the evaluation of effectiveness (in studies using simulations) and the analysis of the event (with measurements and event data) that actually occurred. For example, differences between the expected and actual system behavior for the event of interest should be discussed and modeling assumptions should be evaluated. Important discrepancies between the simulations and the actual event should be investigated.

Considering the importance of an event that involves the operation of a UVLS Program, the 12-calendar-month period provides adequate time to analyze the event and perform an assessment while identifying deficiencies within a reasonable time. This time period is also required in PRC-006-1.

Guidelines for Requirement R5

Requirement R5 promotes the prudent correction of an identified problem during the assessment of a UVLS Program. Per Requirements R3 and R4, an assessment of an active UVLS Program is triggered:

- Within 12 calendar months of an event that resulted in a voltage excursion for which the program was designed to operate
- At least once every 60 calendar months. The default time frame of 60 calendar months or less between assessments has the intention to assure that the cumulative changes to the network and operating condition affecting the UVLS Program are evaluated

Since every UVLS is unique, if material changes are made to system topology or operating conditions, the Planning Coordinator or Transmission Planner will decide the degree to which the change in topology or operating condition becomes a material change sufficient to trigger an assessment of the existing UVLS Program.

A CAP is a list of actions and an associated timetable for implementation to remedy a specific problem. It is a proven tool for resolving operational problems. Per Requirement R5, the Planning Coordinator or Transmission Planner is required to develop a CAP and provide it to UVLS entities to accomplish the purpose of this requirement, which is to prevent future deficiencies in the UVLS Program, thereby minimizing risk to the system. Determining the cause of the deficiency is essential in developing an effective CAP to avoid future re-occurrence of the same problem. A CAP can be revised if additional causes are found.

Based on industry experience and operational coordination timeframes, three calendar months from the date an assessment is completed is a reasonable time frame for development of a CAP, including time to consider alternative solutions and coordination of resources. The “within three

[3] Id.

calendar months" time frame is solely to develop a CAP, including its implementation schedule, and provide it to UVLS entities. It does not include the time needed for its implementation by UVLS entities. This implementation time frame is dictated within the CAP's associated timetable for implementation, and the execution of the CAP according to its schedule is required in Requirement R2.

Guidelines for Requirements R6–R8

An accurate UVLS Program database is necessary for the Planning Coordinator or Transmission Planner to perform system reliability assessment studies and event analysis studies. Without accurate data, there is a possibility that annual reliability assessment studies that are performed by the Planning Coordinator or Transmission Planner can lead to erroneous results and therefore impact reliability. Also, without the accurate data, it is very difficult for the Planning Coordinator or Transmission Planner to duplicate a UVLS event and determine the root cause of the problem.

To support a UVLS Program database, it is necessary for each UVLS entity to provide accurate data to its Planning Coordinator. Each UVLS entity will provide the data according to the specified format and schedule provided by the Planning Coordinator. This is required in order for the Planning Coordinator to maintain and support a comprehensive UVLS Program database. By having a comprehensive database, the Planning Coordinator can embark on a reliability assessment or event analysis/benchmarking studies, identify the issues with the UVLS Program, and develop Corrective Action Plans.

The UVLS Program database may include, but is not limited to the following:

- Owner and operator of the UVLS Program
- Size and location of customer load, or percent of connected load, to be interrupted
- Corresponding voltage set points and clearing times
- Time delay from initiation to trip signal
- Breaker operating times
- Any other schemes that are part of or impact the UVLS Programs, such as related generation protection, islanding schemes, automatic load restoration schemes, underfrequency load shedding (UFLS), and RAS

Additionally, the UVLS Program database is required to be updated annually (once every calendar year) by the Planning Coordinator. The intent here is for UVLS entities to review the data annually and provide changes to the Planning Coordinators so that Planning Coordinators can keep the databases current and accurate for performing event analysis and other assessments.

Finally, a Planning Coordinator is required to provide information to other Planning Coordinators and Transmission Planners within its Interconnection, and other functional entities with a reliability need, within 30 calendar days of receipt of a written request. Thirty calendar days was selected as the time frame as it is considered to be reasonable and well- accepted by the industry. Also, this requirement of sharing the database with applicable functional entities supports the

directive provided by FERC that requires an integrated and coordinated approach to UVLS programs (Paragraph 1509 of FERC Order No. 693).

Frequently Asked Questions

To succinctly address common comment themes that require drafting team response on Project 2008-02 UVLS (proposed PRC-010-1), the drafting team provides the following discussion in the construct of an FAQ format.

Introduction

This Frequently Asked Questions (FAQ) document was created during the development of PRC-010-1 (*Undervoltage Load Shedding*)[4,5] to succinctly address common comment themes with respect to the approach and intent of the Project 2008-02 Undervoltage Load Shedding (UVLS)[6] standard drafting team ("drafting team"). This FAQ document is the outcome of comments received during comment periods and multiple outreach sessions with industry. All comments submitted by industry during comment periods may be reviewed on the project page.

Subsequent to the adoption of PRC-010-1, the UVLS drafting team made minor revisions to the standard address the UVLS Misoperation identification and correction.[7] This FAQ document was amended to reflect up the approach and intent of the drafting team during the development of PRC-010-2 concerning Misoperation of UVLS equipment.

Purpose of Standard Revision

1) What is the basis for a revision of the existing UVLS standards?

The initial input into a revision of the existing UVLS standards is FERC Order No. 693,[8] Paragraph 1509, which directed the ERO to develop a modification of PRC-010-0 that "requires that an integrated and coordinated approach be included in all protection systems on the Bulk-Power System, including generators and transmission lines, generators' low voltage ride through capabilities, and UFLS and UVLS programs." In addition, *The Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations*[9] ("August 14 Blackout Report") showed that proper coordination would have mitigated effects if UVLS was used as a tool.

[4] (http://www.nerc.com/_layouts/PrintStandard.aspx?standardnumber=PRC-010-1&title=Undervoltage%20Load%20Shedding).
[5] Adopted by the NERC Board of Trustees on November 14, 2014.
[6] (http://www.nerc.com/pa/Stand/Pages/Project-2008-02-Undervoltage-Load-Shedding.aspx).
[7] Refer to Project 2010-05.1, which developed PRC-004-3 (Protection System Misoperation Identification and Correction) concurrently with the development of PRC-010-1. (http://www.nerc.com/pa/Stand/Pages/Project2010-05_Protection_System_Misoperations.aspx).
[8] (http://www.nerc.com/docs/docs/ferc/order_693.pdf).
[9] (http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/BlackoutFinal-Web.pdf).

Additional inputs included 1) recommendations from the NERC System Protection and Control Subcommittee (SPCS) in its December 2010 *Technical Review of UVLS-Related Standards*[10] to combine the four existing UVLS standards, revise the applicability to entities responsible for UVLS program design, implementation, and coordination, specifically include a requirement for assessment of coordination between UVLS programs and all other protection systems, and differentiate post-event validation of UVLS program design from verifying correct operation of UVLS equipment; 2) the existing UVLS standards were not in the current results-based format; 3) the preceding revision of the underfrequency load shedding (UFLS) standards had similar types of requirements and had been completed under the construct of a consolidation; and 4) the Independent Expert Review Panel recommendations, which included an evaluation of the existing standards' applicability and level of specificity.

The drafting team agrees that a lack of coordination among protection systems is a key risk to reliability. As part of the revision to address this, the drafting team also agreed that an evaluation and consolidation of the existing UVLS standards was necessary to meet current Reliability Standard development initiatives and to provide clear, comprehensive requirements to address the application and coordination of UVLS.

2) UVLS programs are not mandatory—is compliance for an optional tool necessary?

The drafting team asserts that a key takeaway from the August 14 Blackout Report is that coordination of UVLS with other protection systems could have mitigated the effects if UVLS was used as a tool. Although the use of UVLS is not mandatory, if it is determined that this system preservation measure is necessary to support reliability and a UVLS program is installed, the program needs to be properly coordinated, implemented, and assessed due to the inherent associated reliability risks. As such, there needs to be a level of performance required to properly protect system reliability. Of note, PRC-010-1 and PRC-010-2 apply to the defined term "UVLS Program," which limits the standard's applicability to only those undervoltage-based load shedding programs whose performance has an impact on system reliability.[11]

Coordination with Project 2009-03 Emergency Operations

3) EOP-003-2 has potential redundant requirements with proposed PRC-010-1—how is this being addressed?

As part of its five-year review, Project 2009-03 – Emergency Operations (EOP) identified EOP-003-2 (*Load Shedding Plans*),[12] Requirements R2, R4, and R7 as being more properly covered by Project 2008-02 – UVLS. Both projects were strategically coordinated to move in lockstep from a timing perspective to address these requirements. Project 2009-03 – EOP proposed to revise and

[10] (http://www.nerc.com/docs/pc/spctf/PRC-010_022%20Report_Approved_20101208.pdf).
[11] The term "UVLS Program" used herein was adopted by the NERC Board of Trustees on November 14, 2014.
[12] (http://www.nerc.com/_layouts/PrintStandard.aspx?standardnumber=EOP-003-2&title=Load%20Shedding%20Plans).

consolidate EOP-001-2.1b (*Emergency Operations Planning*),[13] EOP-002-3 (Capacity and Energy Emergencies),[14] and EOP-003-2 to create EOP-011-1, will retire the noted EOP-003-2 requirements (among other revisions), and the Project 2008-02 – UVLS *Mapping Document* will show how PRC-010-1 encompasses the retired content accordingly. Slated to have aligning effective dates, both EOP-011-1 (*Emergency Operations*)[15] and PRC-010-1 will be posted and balloted separately but concurrently, so that industry stakeholders will be able to clearly evaluate the transition. Please see the posted Project 2008-02 UVLS Project Coordination Plan for more information.

"UVLS Program" Definition

4) Why is the introduction of the new defined term "UVLS Program" necessary?

The drafting team found it necessary to introduce the term "UVLS Program" for inclusion in the *Glossary of Terms Used in NERC Reliability Standards*[16] ("NERC Glossary") because different types of UVLS systems need to be treated appropriately with respect to reliability requirements. Therefore, the term establishes which UVLS systems PRC-010-1 will apply to an: "automatic load shedding program consisting of distributed relays and controls used to mitigate undervoltage conditions impacting the Bulk Electric System (BES), leading to voltage instability, voltage collapse, or Cascading. Centrally controlled undervoltage-based load shedding is not included."

The definition excludes locally-applied relays that are designed to protect a contained area or, in other words, are not designed to mitigate wide-area voltage collapse. This exclusion is not explicit in these terms in the enforceable language of the definition since the meaning and measurement of "local" or "wide-area" varies greatly on a continent-wide basis and could potentially be interpreted differently by auditors and the applicable functional entities. Therefore, the definition as written is meant to provide flexibility for the Planning Coordinator or Transmission Planner to determine if a UVLS system falls under the defined term with respect to its impact on the reliability of the BES (voltage instability, voltage collapse, or Cascading). To further support the intended exclusion, further discussion and an example are provided on in the PRC-010-1 and PRC-010-2 Guidelines and Technical Basis section under the heading "Guidelines for UVLS Program Definition."

The definition does explicitly note that the term excludes centrally controlled undervoltage-based load shedding. This type of load shedding is excluded because the drafting team asserts that the design and characteristics of centrally controlled undervoltage-based load shedding are commensurate with those of a Special Protection System (SPS) or Remedial Action Scheme (RAS) and should therefore be subject to SPS or RAS-related Reliability Standards. See PRC-010-1 and

[13] (http://www.nerc.com/_layouts/PrintStandard.aspx?standardnumber=EOP-001-2.1b&title=Emergency%20Operations%20Planning).
[14] (http://www.nerc.com/_layouts/PrintStandard.aspx?standardnumber=EOP-002-3&title=Capacity%20and%20Energy%20Emergencies).
[15] (http://www.nerc.com/_layouts/PrintStandard.aspx?standardnumber=EOP-011-1&title=Emergency%20Operations).
[16] (http://www.nerc.com/pa/Stand/Glossary%20of%20Terms/Glossary_of_Terms.pdf).

PRC-010-2 Guidelines and Technical Basis section under the heading "Guidelines for UVLS Program Definition" for further discussion.

5) If the definition excludes certain types of UVLS, does this preclude an "integrated" approach (FERC Order No. 693, Paragraph 1509)?

The defined term "UVLS Program" clarifies which UVLS systems are subject to the requirements in PRC-010-1 and PRC-010-2. The resulting exclusions from these versions of the standard do not preclude an "integrated" approach because the standard requires that an entity coordinate with all other protection and control systems as necessary, which may include other types of UVLS (i.e., locally-applied UVLS relays and centrally controlled undervoltage-based load shedding).

6) Where will centrally controlled undervoltage-based load shedding be covered?

As explained immediately above, the Requirements of PRC-010-1 and PRC-010-2 are applicable to the proposed NERC Glossary term "UVLS Program," which excludes centrally controlled undervoltage-based load shedding because its design and characteristics are commensurate with those of an SPS or RAS. However, the NERC Glossary during the development of PRC-010-1 definition of "Special Protection System" excluded UVLS. Therefore, the work under Project 2010-05.2 – Special Protection Systems (Phase 2 of Protection Systems) combined the NERC Glossary definition of "Special Protection System" into the single term "Remedial Action Scheme."[17] The definition revisions specifically excluded UVLS Programs, therefore including centrally controlled undervoltage-based shedding.

Consequently, the introduction of the term "UVLS Program" and the conforming revision to the term "Remedial Action Scheme" explicitly clarifies that RAS-related standards are applicable to centrally controlled undervoltage-based load shedding. The implementation plan for the revised definition of "Remedial Action Scheme" will address entities that will have newly identified RAS resulting from the application of the defined term.

Similar to the coordination effort with Project 2009-03 – EOP explained above, Project 2008-02 – UVLS and Project 2010-05.2 – SPS were coordinated to ensure that the effective dates of the adopted definitions of "Remedial Action Scheme" and "UVLS Program," the PRC-010-1 and PRC-010-1 Reliability Standards, and all associated retirements align.

7) Is the term "UVLS Program" inclusive of a collection of independent UVLS relays?

No; multiple independent relays do not constitute a program. While the definition stipulates that a UVLS Program consists of distributed relays and controls, the definition specifies that it must be "[a]n automatic load shedding program, consisting of distributed relays and controls, used to mitigate undervoltage conditions impacting the Bulk Electric System(BES), leading to voltage

[17] Adopted by the NERC Board of Trustees on November 14, 2014.

instability, voltage collapse, or Cascading. Centrally controlled undervoltage-based load shedding is not included."

Applicability

8) What is meant by the phrase "Planning Coordinator or Transmission Planner"?

The PRC-010-1 and PRC-010-2 Reliability Standards are applicable to both the Planning Coordinator and Transmission Planner because either may be responsible for designing and coordinating the program based on agreements, memorandums of understanding, or tariffs. The phrase "Planning Coordinator or Transmission Planner" provides the flexibility for applicability to the entity that will perform the action. The expectation is not that both parties will perform the action, but rather that the Planning Coordinator and Transmission Planner will engage in discussion to determine the appropriate responsible entity. In addition, the requirements containing this phrase have specific language to qualify the responsible entity. For example, Requirement R1 states: "Each Planning Coordinator or Transmission Planner *that is developing* a UVLS Program shall . . ." This language provides clarity that the applicable entity would be the one that is developing the program.

9) Why is the Transmission Operator not included?

While the Transmission Operator may be involved with UVLS Program activities, the drafting team did not identify any required performance for the Transmission Operator that was necessary to capture within PRC-010-1 and PRC-010-2, since the Transmission Operator does not have the resources necessary to implement program specifications. If responsibilities are delegated to the Transmission Operator by the Transmission Owner, the Transmission Owner is still the accountable party.

To the extent that the Transmission Operator is required to have knowledge of system relays and protection systems, the drafting team notes that this requirement is covered under PRC-001-1.1 (*System Protection Coordination*),[18] Requirement R1. It is also noted that manual load shedding, for which the Transmission Operator is responsible, is not in the purview of PRC-010-1 and PRC-010-2, as it is covered under current EOP-003-2 and will subsequently be covered by proposed EOP-011-1 (see Project 2009-03 – Emergency Operations).

10) What about UVLS schemes owned by Transmission Owners, Distribution Providers, or Transmission Operators that are not required by the planner?

The PRC-010-1 and PRC-010-2 Reliability Standards are applicable to the term "UVLS Program." The drafting team notes that, by its defining attributes, a UVLS Program would be required and developed by a Planning Coordinator or Transmission Planner. The nature of a UVLS scheme developed or required by a Distribution Provider, Transmission Operator, or Transmission Owner

[18] http://www.nerc.com/_layouts/PrintStandard.aspx?standardnumber=PRC-001-1.1&title=System%20Protection%20Coordination.

would not meet the attributes of the defined term and would therefore not have the design and characteristics necessary to be subject to the requirements of PRC-010-1 and PRC-010-2.

Requirements R1, R3, R4, and R5

11) What is required to evaluate the coordination referenced in Requirement R1, part 1.2?

Requirement R1 requires each Planning Coordinator or Transmission Planner that develops a UVLS Program to evaluate the program's viability and effectiveness prior to implementation. This evaluation should include studies and analyses used when developing the program that show implementation of the program resolves the identified undervoltage issues that led to its design. These studies and analyses should also show that the UVLS Program is integrated through coordination with generator voltage ride-through capabilities and other protection and control systems. As such, the requirement is meant to provide flexibility for an entity to make the proper determinations, including the considerations for coordination, with respect to program effectiveness based on system characteristics. For further guidance on and examples of coordination considerations, please see the portion of the Guidelines and Technical Basis section under the Requirement R1 heading.

12) Requirements R1, R3, and R4 seem to all require evaluations of program effectiveness—how are they different?

Requirements R1, R3, and R4 do require evaluations of program effectiveness, but they are each at distinct points in time.

Requirement R1 requires evaluation of program effectiveness (by way of the qualifying parts) at the onset of program development, or during the initial planning stage, prior to implementation. Requirement R3 requires the same objectives of an evaluation of effectiveness, but at the point of a mandatory periodic review (at least once every 60 calendar months). Requirement R4 addresses the performance of a UVLS Program after an event (for applicable voltage excursion) to evaluate whether the UVLS Program resolved the undervoltage issues associated with the event.

It is noted that, because of the separate activities of each requirement, UVLS Program deficiencies found as a result of the assessments performed in Requirement R3 or R4 would not be violations of Requirement R1.

13) Requirement R4 would require the Planning Coordinator or Transmission Planner to review all voltage excursions—isn't this unduly burdensome?

While Requirement R4 essentially requires the Planning Coordinator or Transmission Planner to review all voltage excursions to see if they fall below the initializing set points of the UVLS Program, the drafting team contends that it will be clearly evident if voltage falls below the UVLS

threshold because either a) UVLS devices will operate; or b) the system will experience the adverse conditions the UVLS Program was installed to mitigate.

In addition, the drafting team acknowledges that the Planning Coordinator or Transmission Planner may not have the ability to know when voltage excursions are occurring since they are not operating entities. However, a process for the Transmission Operator, Transmission Owner, or Distribution Provider to notify the Transmission Planner or Planning Coordinator of such voltage excursion events is consistent with standard utility practice.

14) PRC-022-1 required the analysis of UVLS Misoperations. How is this addressed in PRC-010-1?

One of the recommendations in the SPCS report was to clearly differentiate between the post-event process of validating the effectiveness of the UVLS program design, its coordination with other protection and control systems, and the potential need to modify the program design (activities addressed in PRC-010-1) and the process of verifying correct operation of UVLS equipment. Because PRC-010-1 was not specific concerning the Misoperation of UVLS equipment, the drafting team made a subsequent revision creating PRC-010-2. Version two (PRC-010-2) now requires that the assessment according to Requirement R4 include the performance (i.e., operation or non-operation) of the UVLS Program equipment.

Relative to the assessment, Requirement R5 requires that a Corrective Action Plan be developed to address any identified deficiencies. This structure ensures that UVLS Program equipment is assessed to identify any Misoperation which could affect BES reliability. Although, the UVLS drafting team maintained during development of PRC-010-1 that verifying correct operation of UVLS equipment should be addressed in PRC-004, the drafting team included UVLS that is intended to trip one or more BES Elements in the proposed PRC-004-5.

Requirements R6, R7, and R8

15) Do Requirements R6, R7, and R8 overlap with the requirements of MOD-032-1?

While both MOD-032-1 (*Data for Power System Modeling and Analysis*)[19] and Requirements R6, R7, and R8 of PRC-010-1 and PRC-010-2 address data requirements, MOD-032-1 establishes overarching modeling data requirements with respect to consistency in format and reporting procedures, whereas the PRC-010-1 and PRC-010-2 requirements address the need to maintain and share data and databases for the purposes of studies for use in event analyses for UVLS Programs specifically. While Reliability Standards in general may have overlap in this manner, the activities in these requirements remain distinctly different.

[19] (http://www.nerc.com/_layouts/PrintStandard.aspx?standardnumber=MOD-032-1&title=Data%20for%20Power%20System%20Modeling%20and%20Analysis).

16) Requirements R6, R7, and R8 appear to be administrative — doesn't this conflict with Paragraph 81 criteria?[20]

Proper maintenance and timely sharing of UVLS Program data as required by Requirements R6, R7, and R8 is necessary to inform the Planning Coordinator or Transmission Planner's studies and analyses. While administrative tasks are required, the tasks have a core reliability-based need.

In addition, Requirements R6, R7, and R8 were written to emulate FERC-approved PRC-006-2 (*Automatic Underfrequency Load Shedding*)[21,22] data requirements. While some of these analogous requirements in PRC-006-2 are listed as candidates for Phase 2 of the Paragraph 81 project, they are not yet approved as meeting the criteria; furthermore, the Independent Expert Review Panel has recommended that these Paragraph 81 candidates not be included for deletion, citing that "there should be a clear expectation for Planning Coordinators to share data necessary to determine their UFLS program parameters."

Rationale

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for Applicability

This standard is applicable to Planning Coordinators and Transmission Planners that have or are developing a UVLS Program, and to Distribution Providers and Transmission Owners responsible for the ownership, operation, or control of UVLS equipment as required by the UVLS Program established by the Transmission Planner or Planning Coordinator. These Distribution Providers and Transmission Owners are referred to as UVLS entities for the purpose of this standard.

The applicability includes both the Planning Coordinator and Transmission Planner because either may be responsible for designing and coordinating the program based on agreements, memorandums of understanding, or tariffs.

The phrase "Planning Coordinator or Transmission Planner" provides the latitude for applicability to the entity that will perform the action. The expectation is not that both parties will perform the action, but rather that the Planning Coordinator and Transmission Planner will engage in discussion to determine the appropriate responsible entity.

Rationale for R1

In Paragraph 1509 from Order No. 693, FERC directed NERC to require an integrated and coordinated approach to all protection systems. The drafting team agrees that a lack of coordination among protection systems is a key risk to reliability, and that each Planning

[20] Refer to Standards Independent Expert Review Project (IERP). (http://www.nerc.com/pa/Stand/Standard%20Development%20Plan/Standards_Independent_Experts_Review_Project_Report-SOTC_and_Board.pdf).
[21] (http://www.nerc.com/_layouts/PrintStandard.aspx?standardnumber=PRC-006-2&title=Automatic%20Underfrequency%20Load%20Shedding).
[22] Adopted by the NERC Board of Trustees on November 14, 2014.

Coordinator or Transmission Planner that develops a UVLS Program should evaluate the program's viability and effectiveness prior to implementation. This evaluation should include studies and analyses used when developing the program that show implementation of the program resolves the identified undervoltage conditions that led to its design. These studies and analyses should also show that the UVLS Program is integrated through coordination with generator voltage ride-through capabilities and other protection and control systems. Though presented as separate items, the drafting team recognizes that the studies that show coordination considerations and that the program addresses undervoltage issues may be interrelated and presented as one comprehensive analysis.

In addition, Requirement R1 also requires the Planning Coordinator or Transmission Planner to provide the UVLS Program's specifications and implementation schedule to applicable UVLS entities to implement the program. It is noted that studies to evaluate the effectiveness of the program should be completed prior to providing the specifications and schedule.

Rationale for R2

UVLS entities must implement a UVLS Program or address any necessary corrective actions for a UVLS Program according to the specifications and schedule provided by the Planning Coordinator or Transmission Planner. If UVLS entities do not implement the UVLS Program according to the specifications and schedule provided, the UVLS Program may not be effective and may not achieve its intended goal.

Rationale for R3

A periodic comprehensive assessment (detailed analysis) should be conducted to identify and catalogue the accumulated effects of minor changes to the system that have occurred since the last assessment was completed, and should include an evaluation of each UVLS Program to ensure the continued integration through coordination. This comprehensive assessment supplements the NERC Reliability Standard TPL-001-4 annual assessment requirement to evaluate the impact of protection systems.

Based on the drafting team's knowledge and experience, and in keeping with time frames contained in similar requirements from other PRC Reliability Standards, 60 calendar months was determined to be the maximum amount of time allowable between assessments. Assessments will be performed sooner than the end of the 60-calendar month period if the Planning Coordinator or Transmission Planner determines that there are material changes to system topology or operating conditions that affect the performance of a UVLS Program. Note that the 60-calendar-month time frame would reset after each assessment.

Rationale for R4

A UVLS Program not functioning as expected during a voltage excursion event for which the UVLS Program was designed to operate presents a critical risk to system reliability. Therefore, a timely assessment to evaluate (1) whether the UVLS Program resolved the undervoltage issues and (2) the performance of the UVLS Program equipment associated with the applicable event is essential. The 12 calendar months (from the date of the event) provides adequate time to coordinate with other Planning Coordinators, Transmission Planners, Transmission Operators,

and UVLS entities, simulate pre- and post-event conditions, and complete the performance assessment.

Rationale for R5

If program deficiencies are identified during an assessment performed in either Requirement R3 or R4, the Planning Coordinator or Transmission Planner must develop a Corrective Action Plan (CAP) to address the deficiencies. Based on the drafting team's knowledge and experience with UVLS studies, three calendar months was determined to provide a judicious balance between the reliability need to address deficiencies expeditiously and the time needed to consider potential solutions, coordinate resources, develop a CAP and implementation schedule, and provide the CAP and schedule to UVLS entities.

It is noted that the three-month time frame is only to develop the CAP and provide it to UVLS entities and does not encompass the time UVLS entities have to implement the CAP. Requirement R2 requires UVLS entities to execute the CAP according to the schedule provided by the Planning Coordinator or Transmission Planner.

Rationale for R6

Having accurate and current data is required for the Planning Coordinator to perform undervoltage studies and for use in event analyses. Requirement R6 supports this reliability need by requiring the Planning Coordinator to update its UVLS Program database at least once each calendar year.

Rationale for R7

Having accurate and current data is required for the Planning Coordinator to perform undervoltage studies and for use in event analyses. Requirement R7 supports this reliability need by requiring the UVLS entity to provide UVLS Program data in accordance with specified parameters.

Rationale for R8

Requirement R8 supports the integrated and coordinated approach to UVLS programs directed by Paragraph 1509 of Order No. 693 by requiring that UVLS Program data be shared with neighboring Planning Coordinators and Transmission Planners within a reasonable time period. Requests for the database should also be fulfilled for those functional entities that have a reliability need for the data (such as the Transmission Operators that develop System Operating Limits and Reliability Coordinators that develop Interconnection Reliability Operating Limits).

Standard PRC-010-2 — Undervoltage Load Shedding

Appendix QC-PRC-010-2
Provisions specific to the standard PRC-010-2 applicable in Québec

This appendix establishes specific provisions for the application of the standard in Québec. Provisions of the standard and of its appendix must be read together for the purposes of understanding and interpretation. Where the standard and appendix differ, the appendix shall prevail.

A. Introduction

1. Title: **Undervoltage Load Shedding**

2. Number: PRC-010-2

3. Purpose: No specific provision

4. Applicability:

None.

5. Effective Date:

5.1. Adoption of the standard by the Régie de l'énergie: February 14, 2017

5.2. Adoption of the appendix by the Régie de l'énergie: February 14, 2017

5.3. Effective date of the standard and its appendix in Québec: April 2, 2017

B. Requirements and Measures

No specific provision

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

The Régie de l'énergie is responsible, in Québec, for compliance monitoring with respect to the reliability standard and its appendix that it adopts.

1.2. Evidence Retention

No specific provision

1.3. Compliance Monitoring and Assessment Processes

Compliance Audit

Self-Certification

Spot Check

Compliance Investigation

Non-Compliance Self-Reporting

Periodic Data Submittal

Exception Reporting

Investigation following a complaint

1.4. Additional Compliance Information

No specific provisions

Appendix QC-PRC-010-2
Provisions specific to the standard PRC-010-2 applicable in Québec

Table of Compliance Elements

No specific provision

D. Regional Variances

No specific provision

E. Interpretations

No specific provision

F. Associated Documents

No specific provisions

Guidelines and Technical Basis

No specific provisions

Revision History

Revision	Adoption Date	Action	Change Tracking
0	February 14, 2017	New Appendix	New

A. Introduction

1. **Title:** Remedial Action Schemes
2. **Number:** PRC-012-2
3. **Purpose:** To ensure that Remedial Action Schemes (RAS) do not introduce unintentional or unacceptable reliability risks to the Bulk Electric System (BES).
4. **Applicability:**
   - **4.1. Functional Entities:**
     - **4.1.1.** Reliability Coordinator
     - **4.1.2.** Planning Coordinator
     - **4.1.3.** RAS-entity – the Transmission Owner, Generator Owner, or Distribution Provider that owns all or part of a RAS
   - **4.2. Facilities:**
     - **4.2.1.** Remedial Action Schemes (RAS)
5. **Effective Date:** See the Implementation Plan for PRC-012-2.

B. Requirements and Measures

R1. Prior to placing a new or functionally modified RAS in service or retiring an existing RAS, each RAS-entity shall provide the information identified in Attachment 1 for review to the Reliability Coordinator(s) where the RAS is located. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M1. Acceptable evidence may include, but is not limited to, a copy of the Attachment 1 documentation and the dated communications with the reviewing Reliability Coordinator(s) in accordance with Requirement R1.

R2. Each Reliability Coordinator that receives Attachment 1 information pursuant to Requirement R1 shall, within four full calendar months of receipt or on a mutually agreed upon schedule, perform a review of the RAS in accordance with Attachment 2, and provide written feedback to each RAS-entity. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M2. Acceptable evidence may include, but is not limited to, dated reports, checklists, or other documentation detailing the RAS review, and the dated communications with the RAS-entity in accordance with Requirement R2.

R3. Prior to placing a new or functionally modified RAS in service or retiring an existing RAS, each RAS-entity that receives feedback from the reviewing Reliability Coordinator(s) identifying reliability issue(s) shall resolve each issue to obtain approval of the RAS from each reviewing Reliability Coordinator. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. Acceptable evidence may include, but is not limited to, dated documentation and communications with the reviewing Reliability Coordinator that no reliability issues were identified during the review or that all identified reliability issues were resolved in accordance with Requirement R3.

R4. Each Planning Coordinator, at least once every five full calendar years, shall: *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

4.1. Perform an evaluation of each RAS within its planning area to determine whether:

4.1.1. The RAS mitigates the System condition(s) or Contingency(ies) for which it was designed.

4.1.2. The RAS avoids adverse interactions with other RAS, and protection and control systems.

4.1.3. For limited impact[1] RAS, the inadvertent operation of the RAS or the failure of the RAS to operate does not cause or contribute to BES Cascading, uncontrolled separation, angular instability, voltage instability, voltage collapse, or unacceptably damped oscillations.

4.1.4. Except for limited impact RAS, the possible inadvertent operation of the RAS, resulting from any single RAS component malfunction satisfies all of the following:

4.1.4.1. The BES shall remain stable.

4.1.4.2. Cascading shall not occur.

4.1.4.3. Applicable Facility Ratings shall not be exceeded.

4.1.4.4. BES voltages shall be within post-Contingency voltage limits and post-Contingency voltage deviation limits as established by the Transmission Planner and the Planning Coordinator.

4.1.4.5. Transient voltage responses shall be within acceptable limits as established by the Transmission Planner and the Planning Coordinator.

4.1.5. Except for limited impact RAS, a single component failure in the RAS, when the RAS is intended to operate does not prevent the BES from meeting the same performance requirements (defined in Reliability Standard TPL-001-4 or its successor) as those required for the events and conditions for which the RAS is designed.

[1] A RAS designated as limited impact cannot, by inadvertent operation or failure to operate, cause or contribute to BES Cascading, uncontrolled separation, angular instability, voltage instability, voltage collapse, or unacceptably damped oscillations.

4.2. Provide the results of the RAS evaluation including any identified deficiencies to each reviewing Reliability Coordinator and RAS-entity, and each impacted Transmission Planner and Planning Coordinator.

M4. Acceptable evidence may include, but is not limited to, dated reports or other documentation of the analyses comprising the evaluation(s) of each RAS and dated communications with the RAS-entity(ies), Transmission Planner(s), Planning Coordinator(s), and the reviewing Reliability Coordinator(s) in accordance with Requirement R4.

R5. Each RAS-entity, within 120 full calendar days of a RAS operation or a failure of its RAS to operate when expected, or on a mutually agreed upon schedule with its reviewing Reliability Coordinator(s), shall: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

5.1. Participate in analyzing the RAS operational performance to determine whether:

5.1.1. The System events and/or conditions appropriately triggered the RAS.

5.1.2. The RAS responded as designed.

5.1.3. The RAS was effective in mitigating BES performance issues it was designed to address.

5.1.4. The RAS operation resulted in any unintended or adverse BES response.

5.2. Provide the results of RAS operational performance analysis that identified any deficiencies to its reviewing Reliability Coordinator(s).

M5. Acceptable evidence may include, but is not limited to, dated documentation detailing the results of the RAS operational performance analysis and dated communications with participating RAS-entities and the reviewing Reliability Coordinator(s) in accordance with Requirement R5.

R6. Each RAS-entity shall participate in developing a Corrective Action Plan (CAP) and submit the CAP to its reviewing Reliability Coordinator(s) within six full calendar months of: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning, Long-term Planning]*

- Being notified of a deficiency in its RAS pursuant to Requirement R4, or
- Notifying the Reliability Coordinator of a deficiency pursuant to Requirement R5, Part 5.2, or
- Identifying a deficiency in its RAS pursuant to Requirement R8.

M6. Acceptable evidence may include, but is not limited to, a dated CAP and dated communications among each reviewing Reliability Coordinator and each RAS-entity in accordance with Requirement R6.

R7. Each RAS-entity shall, for each of its CAPs developed pursuant to Requirement R6: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning, Long-term Planning]*

7.1. Implement the CAP.

7.2. Update the CAP if actions or timetables change.

7.3. Notify each reviewing Reliability Coordinator if CAP actions or timetables change and when the CAP is completed.

M7. Acceptable evidence may include, but is not limited to, dated documentation such as CAPs, project or work management program records, settings sheets, work orders, maintenance records, and communication with the reviewing Reliability Coordinator(s) that documents the implementation, updating, or completion of a CAP in accordance with Requirement R7.

R8. Each RAS-entity shall participate in performing a functional test of each of its RAS to verify the overall RAS performance and the proper operation of non-Protection System components: *[Violation Risk Factor: High] [Time Horizon: Long-term Planning]*

- At least once every six full calendar years for all RAS not designated as limited impact, or
- At least once every twelve full calendar years for all RAS designated as limited impact

M8. Acceptable evidence may include, but is not limited to, dated documentation detailing the RAS operational performance analysis for a correct RAS segment or an end-to-end operation (Measure M5 documentation), or dated documentation demonstrating that a functional test of each RAS segment or an end-to-end test was performed in accordance with Requirement R8.

R9. Each Reliability Coordinator shall update a RAS database containing, at a minimum, the information in Attachment 3 at least once every twelve full calendar months. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M9. Acceptable evidence may include, but is not limited to, dated spreadsheets, database reports, or other documentation demonstrating a RAS database was updated in accordance with Requirement R9.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority:
As defined in the NERC Rules of Procedure, “Compliance Enforcement Authority” means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

The RAS-entity (Transmission Owner, Generator Owner, and Distribution Provider) shall each keep data or evidence to show compliance with Requirements R1, R3, R5, R6, R7, and R8, and Measures M1, M3, M5, M6, M7, and M8 since the last audit, unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

The Reliability Coordinator shall each keep data or evidence to show compliance with Requirements R2 and R9, and Measures M2 and M9 since the last audit, unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

The Planning Coordinator shall each keep data or evidence to show compliance with Requirement R4 and Measure M4 since the last audit, unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

If a RAS-entity (Transmission Owner, Generator Owner or Distribution Provider), Reliability Coordinator, or Planning Coordinator is found non-compliant, it shall keep information related to the non-compliance until mitigation is completed and approved, or for the time specified above, whichever is longer.

The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program

As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	N/A	N/A	N/A	The RAS-entity failed to provide the information identified in Attachment 1 to each Reliability Coordinator prior to placing a new or functionally modified RAS in service or retiring an existing RAS in accordance with Requirement R1.
R2.	The reviewing Reliability Coordinator performed the review and provided the written feedback in accordance with Requirement R2, but was late by less than or equal to 30 full calendar days.	The reviewing Reliability Coordinator performed the review and provided the written feedback in accordance with Requirement R2, but was late by more than 30 full calendar days but less than or equal to 60 full calendar days.	The reviewing Reliability Coordinator performed the review and provided the written feedback in accordance with Requirement R2, but was late by more than 60 full calendar days but less than or equal to 90 full calendar days.	The reviewing Reliability Coordinator performed the review and provided the written feedback in accordance with Requirement R2, but was late by more than 90 full calendar days. OR The reviewing Reliability Coordinator failed to perform the review or provide feedback in accordance with Requirement R2.

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R3.	N/A	N/A	N/A	The RAS-entity failed to resolve identified reliability issue(s) to obtain approval from each reviewing Reliability Coordinator prior to placing a new or functionally modified RAS in service or retiring an existing RAS in accordance with Requirement R3.
R4.	The Planning Coordinator performed the evaluation in accordance with Requirement R4, but was late by less than or equal to 30 full calendar days.	The Planning Coordinator performed the evaluation in accordance with Requirement R4, but was late by more than 30 full calendar days but less than or equal to 60 full calendar days.	The Planning Coordinator performed the evaluation in accordance with Requirement R4, but was late by more than 60 full calendar days but less than or equal to 90 full calendar days. OR The Planning Coordinator performed the evaluation in accordance with Requirement R4, but failed to evaluate one of the Parts 4.1.1 through 4.1.5.	The Planning Coordinator performed the evaluation in accordance with Requirement R4, but was late by more than 90 full calendar days. OR The Planning Coordinator performed the evaluation in accordance with Requirement R4, but failed to evaluate two or more of the Parts 4.1.1 through 4.1.5. OR

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				The Planning Coordinator performed the evaluation in accordance with Requirement R4, but failed to provide the results to one or more of the receiving entities listed in Part 4.2. OR The Planning Coordinator failed to perform the evaluation in accordance with Requirement R4.
R5.	The RAS-entity performed the analysis in accordance with Requirement R5, but was late by less than or equal to 10 full calendar days.	The RAS-entity performed the analysis in accordance with Requirement R5, but was late by more than 10 full calendar days but less than or equal to 20 full calendar days.	The RAS-entity performed the analysis in accordance with Requirement R5, but was late by more than 20 full calendar days but less than or equal to 30 full calendar days. OR The RAS-entity performed the analysis in accordance with Requirement R5, but failed to address one of the Parts 5.1.1 through 5.1.4.	The RAS-entity performed the analysis in accordance with Requirement R5, but was late by more than 30 full calendar days. OR The RAS-entity performed the analysis in accordance with Requirement R5, but failed to address two or more of the Parts 5.1.1 through 5.1.4.

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				OR The RAS-entity performed the analysis in accordance with Requirement R5, but failed to provide the results (Part 5.2) to one or more of the reviewing Reliability Coordinator(s). OR The RAS-entity failed to perform the analysis in accordance with Requirement R5.
R6.	The RAS-entity developed a Corrective Action Plan and submitted it to its reviewing Reliability Coordinator(s) in accordance with Requirement R6, but was late by less than or equal to 10 full calendar days.	The RAS-entity developed a Corrective Action Plan and submitted it to its reviewing Reliability Coordinator(s) in accordance with Requirement R6, but was late by more than 10 full calendar days but less than or equal to 20 full calendar days.	The RAS-entity developed a Corrective Action Plan and submitted it to its reviewing Reliability Coordinator(s) in accordance with Requirement R6, but was late by more than 20 full calendar days but less than or equal to 30 full calendar days.	The RAS-entity developed a Corrective Action Plan and submitted it to its reviewing Reliability Coordinator(s) in accordance with Requirement R6, but was late by more than 30 full calendar days. OR The RAS-entity developed a Corrective Action Plan but failed to submit it to one or

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				more of its reviewing Reliability Coordinator(s) in accordance with Requirement R6. OR The RAS-entity failed to develop a Corrective Action Plan in accordance with Requirement R6.
R7.	The RAS-entity implemented a CAP in accordance with Requirement R7, Part 7.1, but failed to update the CAP (Part 7.2) if actions or timetables changed, or failed to notify (Part 7.3) each of the reviewing Reliability Coordinator(s) of the updated CAP or completion of the CAP.	N/A	N/A	The RAS-entity failed to implement a CAP in accordance with Requirement R7, Part 7.1.
R8.	The RAS-entity performed the functional test for a RAS as specified in Requirement R8, but was late by less than	The RAS-entity performed the functional test for a RAS as specified in Requirement R8, but was late by more than 30 full calendar days	The RAS-entity performed the functional test for a RAS as specified in Requirement R8, but was late by more than 60 full calendar days	The RAS-entity performed the functional test for a RAS as specified in Requirement R8, but was late by more than 90 full calendar days.

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	or equal to 30 full calendar days.	but less than or equal to 60 full calendar days.	but less than or equal to 90 full calendar days.	OR The RAS-entity failed to perform the functional test for a RAS as specified in Requirement R8.
R9.	The Reliability Coordinator updated the RAS database in accordance with Requirement R9, but was late by less than or equal to 30 full calendar days.	The Reliability Coordinator updated the RAS database in accordance with Requirement R9, but was late by more than 30 full calendar days but less than or equal to 60 full calendar days.	The Reliability Coordinator updated the RAS database in accordance with Requirement R9, but was late by more than 60 full calendar days but less than or equal to 90 full calendar days.	The Reliability Coordinator updated the RAS database in accordance with Requirement R9 but was late by more than 90 full calendar days. OR The Reliability Coordinator failed to update the RAS database in accordance with Requirement R9.

D. Regional Variances

None.

E. Associated Documents

Version History

Version	Date	Action	Change Tracking
0	February 8, 2005	Adopted by the Board of Trustees	
0	March 16, 2007	Identified by Commission as “fill-in-the-blank” with no action taken on the standard	
1	November 13, 2014	Adopted by the Board of Trustees	
1	November 19, 2015	Accepted by Commission for informational purposes only	
2	May 5, 2016	Adopted by Board of Trustees	
2	September 20, 2017	FERC Order No. 837 issued approving PRC-012-2	

Attachment 1
Supporting Documentation for RAS Review

The following checklist identifies important Remedial Action Scheme (RAS) information for each new or functionally modified[2] RAS that the RAS-entity must document and provide to the reviewing Reliability Coordinator(s) (RC). If an item on this list does not apply to a specific RAS, a response of "Not Applicable" for that item is appropriate. When RAS are submitted for functional modification review and approval, only the proposed modifications to that RAS require review; however, the RAS-entity must provide a summary of the existing functionality. The RC may request additional information on any aspect of the RAS as well as any reliability issue related to the RAS. Additional entities (without decision authority) may be part of the RAS review process at the request of the RC.

I. General

1. Information such as maps, one-line drawings, substation and schematic drawings that identify the physical and electrical location of the RAS and related facilities.
2. Functionality of new RAS or proposed functional modifications to existing RAS and documentation of the pre- and post-modified functionality of the RAS.
3. The Corrective Action Plan (CAP) if RAS modifications are proposed in a CAP.
4. Data to populate the RAS database:
    a. RAS name.
    b. Each RAS-entity and contact information.
    c. Expected or actual in-service date; most recent RC-approval date (Requirement R3); most recent evaluation date (Requirement R4); and date of retirement, if applicable.
    d. System performance issue or reason for installing the RAS (e.g., thermal overload, angular instability, poor oscillation damping, voltage instability, under- or over-voltage, or slow voltage recovery).
    e. Description of the Contingencies or System conditions for which the RAS was designed (i.e., initiating conditions).
    f. Action(s) to be taken by the RAS.
    g. Identification of limited impact[3] RAS.
    h. Any additional explanation relevant to high-level understanding of the RAS.

---

[2] Functionally modified: Any modification to a RAS consisting of any of the following:
- Changes to System conditions or contingencies monitored by the RAS
- Changes to the actions the RAS is designed to initiate
- Changes to RAS hardware beyond in-kind replacement; i.e., match the original functionality of existing components
- Changes to RAS logic beyond correcting existing errors
- Changes to redundancy levels; i.e., addition or removal

[3] A RAS designated as limited impact cannot, by inadvertent operation or failure to operate, cause or contribute to BES Cascading, uncontrolled separation, angular instability, voltage instability, voltage collapse, or unacceptably damped oscillations.

II. Functional Description and Transmission Planning Information

1. Contingencies and System conditions that the RAS is intended to remedy.
2. The action(s) to be taken by the RAS in response to disturbance conditions.
3. A summary of technical studies, if applicable, demonstrating that the proposed RAS actions satisfy System performance objectives for the scope of System events and conditions that the RAS is intended to remedy. The technical studies summary shall also include information such as the study year(s), System conditions, and Contingencies analyzed on which the RAS design is based, and the date those technical studies were performed.
4. Information regarding any future System plans that will impact the RAS.
5. RAS-entity proposal and justification for limited impact designation, if applicable.
6. Documentation describing the System performance resulting from the possible inadvertent operation of the RAS, except for limited impact RAS, caused by any single RAS component malfunction. Single component malfunctions in a RAS not determined to be limited impact must satisfy all of the following:
    a. The BES shall remain stable.
    b. Cascading shall not occur.
    c. Applicable Facility Ratings shall not be exceeded.
    d. BES voltages shall be within post-Contingency voltage limits and post-Contingency voltage deviation limits as established by the Transmission Planner and the Planning Coordinator.
    e. Transient voltage responses shall be within acceptable limits as established by the Transmission Planner and the Planning Coordinator.
7. An evaluation indicating that the RAS settings and operation avoid adverse interactions with other RAS, and protection and control systems.
8. Identification of other affected RCs.

III. Implementation

1. Documentation describing the applicable equipment used for detection, dc supply, communications, transfer trip, logic processing, control actions, and monitoring.
2. Information on detection logic and settings/parameters that control the operation of the RAS.
3. Documentation showing that any multifunction device used to perform RAS function(s), in addition to other functions such as protective relaying or SCADA, does not compromise the reliability of the RAS when the device is not in service or is being maintained.
4. Documentation describing the System performance resulting from a single component failure in the RAS, except for limited impact RAS, when the RAS is intended to operate. A single component failure in a RAS not determined to be limited impact must not prevent the BES from meeting the same performance requirements (defined in Reliability Standard TPL-001-4 or its successor) as those required for the events and conditions for which the RAS is designed. The documentation should describe or illustrate how the design achieves this objective.
5. Documentation describing the functional testing process.

IV. RAS Retirement

The following checklist identifies RAS information that the RAS-entity shall document and provide to each reviewing RC.

1. Information necessary to ensure that the RC is able to understand the physical and electrical location of the RAS and related facilities.
2. A summary of applicable technical studies and technical justifications upon which the decision to retire the RAS is based.
3. Anticipated date of RAS retirement.

Attachment 2
Reliability Coordinator RAS Review Checklist

The following checklist identifies reliability-related considerations for the Reliability Coordinator (RC) to review and verify for each new or functionally modified[4] Remedial Action Scheme (RAS). The RC review is not limited to the checklist items and the RC may request additional information on any aspect of the RAS as well as any reliability issue related to the RAS. If a checklist item is not relevant to a particular RAS, it should be noted as "Not Applicable." If reliability considerations are identified during the review, the considerations and the proposed resolutions should be documented with the remaining applicable Attachment 2 items.

I. Design

1. The RAS actions satisfy performance objectives for the scope of events and conditions that the RAS is intended to mitigate.
2. The designed timing of RAS operation(s) is appropriate to its BES performance objectives.
3. The RAS arming conditions, if applicable, are appropriate to its System performance objectives.
4. The RAS avoids adverse interactions with other RAS, and protection and control systems.
5. The effects of RAS incorrect operation, including inadvertent operation and failure to operate, have been identified.
6. Determination whether or not the RAS is limited impact.[5] A RAS designated as limited impact cannot, by inadvertent operation or failure to operate, cause or contribute to BES Cascading, uncontrolled separation, angular instability, voltage instability, voltage collapse, or unacceptably damped oscillations.
7. Except for limited impact RAS as determined by the RC, the possible inadvertent operation of the RAS resulting from any single RAS component malfunction satisfies all of the following:
    a. The BES shall remain stable.
    b. Cascading shall not occur.
    c. Applicable Facility Ratings shall not be exceeded.

[4] Functionally modified: Any modification to a RAS consisting of any of the following:
- Changes to System conditions or contingencies monitored by the RAS
- Changes to the actions the RAS is designed to initiate
- Changes to RAS hardware beyond in-kind replacement; i.e., match the original functionality of existing components
- Changes to RAS logic beyond correcting existing errors
- Changes to redundancy levels; i.e., addition or removal

[5] A RAS designated as limited impact cannot, by inadvertent operation or failure to operate, cause or contribute to BES Cascading, uncontrolled separation, angular instability, voltage instability, voltage collapse, or unacceptably damped oscillations.

d. BES voltages shall be within post-Contingency voltage limits and post-Contingency voltage deviation limits as established by the Transmission Planner and the Planning Coordinator.

e. Transient voltage responses shall be within acceptable limits as established by the Transmission Planner and the Planning Coordinator.

8. The effects of future BES modifications on the design and operation of the RAS have been identified, where applicable.

II. Implementation

1. The implementation of RAS logic appropriately correlates desired actions (outputs) with events and conditions (inputs).
2. Except for limited impact RAS as determined by the RC, a single component failure in a RAS does not prevent the BES from meeting the same performance requirements as those required for the events and conditions for which the RAS is designed.
3. The RAS design facilitates periodic testing and maintenance.
4. The mechanism or procedure by which the RAS is armed is clearly described, and is appropriate for reliable arming and operation of the RAS for the conditions and events for which it is designed to operate.

III. RAS Retirement

RAS retirement reviews should assure that there is adequate justification for why a RAS is no longer needed.

Attachment 3
Database Information

1. RAS name.
2. Each RAS-entity and contact information.
3. Expected or actual in-service date; most recent RC-approval date (Requirement R3); most recent evaluation date (Requirement R4); and date of retirement, if applicable.
4. System performance issue or reason for installing the RAS (e.g., thermal overload, angular instability, poor oscillation damping, voltage instability, under- or over-voltage, or slow voltage recovery).
5. Description of the Contingencies or System conditions for which the RAS was designed (i.e., initiating conditions).
6. Action(s) to be taken by the RAS.
7. Identification of limited impact[6] RAS.
8. Any additional explanation relevant to high-level understanding of the RAS.

[6] A RAS designated as limited impact cannot, by inadvertent operation or failure to operate, cause or contribute to BES Cascading, uncontrolled separation, angular instability, voltage instability, voltage collapse, or unacceptably damped oscillations.

Technical Justification

4.1.1 Reliability Coordinator

The Reliability Coordinator (RC) is the best-suited functional entity to perform the Remedial Action Scheme (RAS) review because the RC has the widest area reliability perspective of all functional entities and an awareness of reliability issues in neighboring RC Areas. The Wide Area purview better facilitates the evaluation of interactions among separate RAS, as well as interactions among RAS and other protection and control systems. The selection of the RC also minimizes the possibility of a conflict of interest that could exist because of business relationships among the RAS-entity, Planning Coordinator, Transmission Planner, or other entities involved in the planning or implementation of a RAS. The RC is also less likely to be a stakeholder in any given RAS and can therefore maintain objective independence.

4.1.2 Planning Coordinator

The Planning Coordinator (PC) is the best-suited functional entity to perform the RAS evaluation to verify the continued effectiveness and coordination of the RAS, its inadvertent operation performance, and the performance for a single component failure. The items that must be addressed in the evaluations include: 1) RAS mitigation of the System condition(s) or event(s) for which it was designed; 2) RAS avoidance of adverse interactions with other RAS and with protection and control systems; 3) the impact of inadvertent operation; and 4) the impact of a single component failure. The evaluation of these items involves modeling and studying the interconnected transmission system, similar to the planning analyses performed by PCs.

4.1.3 RAS-entity

The RAS-entity is any Transmission Owner, Generator Owner, or Distribution Provider that owns all or part of a RAS. If all of the RAS (RAS components) have a single owner, then that RAS-entity has sole responsibility for all the activities assigned within the standard to the RAS-entity. If the RAS (RAS components) have more than one owner, then each separate RAS component owner is a RAS-entity and is obligated to participate in various activities identified by the Requirements.

The standard does not stipulate particular compliance methods. RAS-entities have the option of collaborating to fulfill their responsibilities for each applicable requirement. Such collaboration and coordination may promote efficiency in achieving the reliability objectives of the requirements; however, the individual RAS-entity must be able to demonstrate its participation for compliance. As an example, the individual RAS-entities could collaborate to produce and submit a single, coordinated Attachment 1 to the reviewing RC pursuant to Requirement R1 to initiate the RAS review process.

Limited impact

RAS are unique and customized assemblages of protection and control equipment that vary in complexity and impact on the reliability of the BES. These differences in RAS design, action, and risk to the BES are identified and verified within the construct of Requirements R1-R4 of PRC-012-2.

The reviewing RC has the authority to designate a RAS as limited impact if the RAS cannot, by inadvertent operation or failure to operate, cause or contribute to BES Cascading, uncontrolled

separation, angular instability, voltage instability, voltage collapse, or unacceptably damped oscillations. The reviewing RC makes the final determination as to whether a RAS qualifies for the limited impact designation based upon the studies and other information provided with the Attachment 1 submittal by the RAS-entity.

The standard recognizes the Local Area Protection Scheme (LAPS) classification in WECC (Western Electricity Coordinating Council) and the Type III classification in NPCC (Northeast Power Coordinating Council) as initially appropriate for limited impact designation. The following information describing the aforementioned WECC and NPCC RAS is excerpted from the respective regional documentation[7].The drafting team notes that the information below represents the state of the WECC and NPCC regional processes at the time of this standard development and is subject to change before the effective date of PRC-012-2.

WECC: Local Area Protection Scheme (LAPS)

A Remedial Action Scheme (RAS) whose failure to operate would NOT result in any of the following:

- Violations of TPL-001-WECC-RBP System Performance RBP,
- Maximum load loss ≥ 300 MW,
- Maximum generation loss ≥ 1000 MW.

NPCC: Type III

An SPS whose misoperation or failure to operate results in no **significant adverse impact** outside the **local area**.

The following terms are also defined by NPCC to assess the impact of the SPS for classification:

Significant adverse impact – With due regard for the maximum operating capability of the affected systems, one or more of the following conditions arising from faults or disturbances, shall be deemed as having significant adverse impact:

a. system instability;

b. unacceptable system dynamic response or equipment tripping;

c. voltage levels in violation of applicable emergency limits;

d. loadings on transmission facilities in violation of applicable emergency limits;

e. unacceptable loss of load.

Local area – An electrically confined or radial portion of the system. The geographic size and number of system elements contained will vary based on system characteristics. A local area may be relatively large geographically with relatively few buses in a sparse system, or be

[7] WECC Procedure to Submit a RAS for Assessment Information Required to Assess the Reliability of a RAS Guideline, Revised 10/28/2013 | NPCC Regional Reliability Reference Directory # 7, Special Protection Systems, Version 2, 3/31/2015

relatively small geographically with a relatively large number of buses in a densely networked system.

A RAS implemented prior to the effective date of PRC-012-2 that has been through the regional review processes of WECC or NPCC and classified as either a Local Area Protection Scheme (LAPS) in WECC or a Type III in NPCC, is recognized as a limited impact RAS upon the effective date of PRC-012-2 for the purposes of this standard and is subject to all applicable requirements.

To propose an existing RAS (a RAS implemented prior to the effective date of PRC-012-2) be designated as limited impact by the reviewing RC, the RAS-entity must prepare and submit the appropriate Attachment 1 information that includes the technical justification (evaluations) documenting that the System can meet the performance requirements (specified in Requirement R4, Parts 4.1.4 and 4.1.5) resulting from a single RAS component malfunction or failure, respectively.

There is nothing that precludes a RAS-entity from working with the reviewing RC during the implementation period of PRC-012-2, in anticipation of the standard becoming enforceable. However, even if the reviewing RC determines the RAS qualifies as limited impact, the designation is not relevant until the standard becomes effective. Until then, the existing regional processes remain in effect as well as the existing RAS classifications or lack thereof.

An example of a scheme that could be recognized as a limited impact RAS is a load shedding or generation rejection scheme used to mitigate the overload of a BES transmission line. The inadvertent operation of such a scheme would cause the loss of either a certain amount of generation or load. The evaluation by the RAS-entity should demonstrate that the loss of this amount of generation or load, without the associated contingency for RAS operation actually occurring, is acceptable and not detrimental to the reliability of BES; e.g., in terms of frequency and voltage stability. The failure of that scheme to operate when intended could potentially lead to the overloading of a transmission line beyond its acceptable rating. The RAS-entity would need to demonstrate that this overload, while in excess of the applicable Facility Rating, is not detrimental to the BES outside the contained area (predetermined by studies) affected by the contingency.

Other examples of limited impact RAS include:

- A scheme used to protect BES equipment from damage caused by overvoltage through generation rejection or equipment tripping.
- A centrally-controlled undervoltage load shedding scheme used to protect a contained area (predetermined by studies) of the BES against voltage collapse.
- A scheme used to trip a generating unit following certain BES Contingencies to prevent the unit from going out of synch with the System; where, if the RAS fails to operate and the unit pulls out of synchronism, the resulting apparent impedance swings do not

result in the tripping of any Transmission System Elements other than the generating unit and its directly connected Facilities.

Requirement R1

Each RAS is unique and its action(s) can have a significant impact on the reliability and integrity of the Bulk Electric System (BES); therefore, a review of a proposed new RAS or an existing RAS proposed for functional modification, or retirement (removal from service) must be completed prior to implementation.

Functional modifications consists of any of the following:

- Changes to System conditions or Contingencies monitored by the RAS
- Changes to the actions the RAS is designed to initiate
- Changes to RAS hardware beyond in-kind replacement; i.e., match the original functionality of existing components
- Changes to RAS logic beyond correcting existing errors
- Changes to redundancy levels; i.e., addition or removal

An example indicating the limits of an in-kind replacement of a RAS component is the replacement of one relay (or other device) with a relay (or other device) that uses similar functions. For instance, if a RAS included a CO-11 relay which was replaced by an IAC-53 relay, that would be an in-kind replacement. If the CO-11 relay were replaced by a microprocessor SEL-451 relay that used only the same functions as the original CO-11 relay, that would also be an in-kind replacement; however, if the SEL-451 relay was used to add new logic to what the CO-11 relay had provided, then the replacement relay would be a functional modification.

Changes to RAS pickup levels that require no other scheme changes are not considered a functional modification. For example, System conditions require a RAS to be armed when the combined flow on two lines exceeds 500 MW. If a periodic evaluation pursuant to Requirement R4, or other assessment, indicates that the arming level should be reduced to 450 MW without requiring any other RAS changes that would not be a functional modification. Similarly, if a RAS is designed to shed load to reduce loading on a particular line below 1000 amps, then a change in the load shedding trigger from 1000 amps to 1100 amps would not be a functional modification.

Another example illustrates a case where a System change may result in a RAS functional change. Assume that a generation center is connected to a load center through two transmission lines. The lines are not rated to accommodate full plant output if one line is out of service, so a RAS monitors the status of both lines and trips or ramps down the generation to a safe level following loss of either line. Later, one of the lines is tapped to serve additional load. The System that the RAS impacts now includes three lines, loss of any of which is likely to still require generation reduction. The modified RAS will need to monitor all three lines (add two line terminal status inputs to the RAS) and the logic to recognize the specific line outages would

change, while the generation reduction (RAS output) requirement may or may not change, depending on which line is out of service. These required RAS changes would be a functional modification.

Any functional modification to a RAS will need to be reviewed and approved through the process described in Requirements R1, R2, and R3. The need for such functional modifications may be identified in several ways including but not limited to the Planning evaluations pursuant to R4, incorrect operations pursuant to R5, a test failure pursuant to R8, or Planning assessments related to future additions or modifications of other facilities.

See Item 4a in the Implementation Section of Attachment 1 in the Supplemental Material section for typical RAS components for which a failure may be considered. The RC has the discretion to make the final determination regarding which components should be regarded as RAS components during its review.

To facilitate a review that promotes reliability, the RAS-entity(ies) must provide the reviewer with sufficient details of the RAS design, function, and operation. This data and supporting documentation are identified in Attachment 1 of this standard, and Requirement R1 mandates that the RAS-entity(ies) provide them to the reviewing Reliability Coordinator (RC). The RC that coordinates the area where the RAS is located is responsible for the review. In cases where a RAS crosses multiple RC Area boundaries, each affected RC is responsible for conducting either individual reviews or a coordinated review.

Requirement R1 does not specify how far in advance of implementation the RAS-entity(ies) must provide Attachment 1 data to the reviewing RC. The information will need to be submitted early enough to allow RC review in the allotted time pursuant to Requirement R2, including resolution of any reliability issues that might be identified, in order to obtain approval of the reviewing RC. Expeditious submittal of this information is in the interest of each RAS-entity to effect a timely implementation.

Requirement R2

Requirement R2 mandates that the RC perform reviews of all proposed new RAS and existing RAS proposed for functional modification, or retirement (removal from service) in its RC Area.

RAS are unique and customized assemblages of protection and control equipment. As such, they have a potential to introduce reliability risks to the BES, if not carefully planned, designed, and installed. A RAS may be installed to address a reliability issue, or achieve an economic or operational advantage, and could introduce reliability risks that might not be apparent to a RAS-entity(ies). An independent review by a multi-disciplinary panel of subject matter experts with planning, operations, protection, telecommunications, and equipment expertise is an effective means of identifying risks and recommending RAS modifications when necessary.

The RC is the functional entity best suited to perform the RAS reviews because it has the widest area reliability perspective of all functional entities and an awareness of reliability issues in

neighboring RC Areas. This Wide Area purview facilitates the evaluation of interactions among separate RAS as well as interactions among the RAS and other protection and control systems.

The selection of the RC also minimizes the possibility of a "conflict of interest" that could exist because of business relationships among the RAS-entity, Planning Coordinator (PC), Transmission Planner (TP), or other entities that are likely to be involved in the planning or implementation of a RAS. The RC may request assistance in RAS reviews from other parties such as the PC(s) or regional technical groups (e.g., Regional Entities); however, the RC retains responsibility for compliance with the requirement. It is recognized that the RC does not possesses more information or ability than anticipated by their functional registration as designated by NERC. The NERC Functional Model is a guideline for the development of standards and their applicability and does not contain compliance requirements. If Reliability Standards address functions that are not described in the model, the Reliability Standard requirements take precedence over the Functional Model. For further reference, please see the Introduction section of NERC's Reliability Functional Model, Version 5, November 2009. Attachment 2 of this standard is a checklist for assisting the RC in identifying design and implementation aspects of a RAS, and for facilitating consistent reviews of each RAS submitted for review. The time frame of four full calendar months is consistent with current utility practice; however, flexibility is provided by allowing the parties to negotiate a different schedule for the review. Note, an RC may need to include this task in its reliability plan(s) for the NERC Region(s) in which it is located.

Requirement R3

Requirement R3 mandates that each RAS-entity resolve all reliability issues (pertaining to its RAS) identified during the RAS review by the reviewing Reliability Coordinators. Examples of reliability issues include a lack of dependability, security, or coordination. RC approval of a RAS is considered to be obtained when the reviewing RC's feedback to each RAS-entity indicates that either no reliability issues were identified during the review or all identified reliability issues were resolved to the RC's satisfaction.

Dependability is a component of reliability that is the measure of certainty of a device to operate when required. If a RAS is installed to meet performance requirements of NERC Reliability Standards, a failure of the RAS to operate when intended would put the System at risk of violating NERC Reliability Standards if specified Contingency(ies) or System conditions occur. This risk is mitigated by designing the RAS so that it will accomplish the intended purpose while experiencing a single RAS component failure. This is often accomplished through redundancy. Other strategies for providing dependability include "over-tripping" load or generation, or alternative automatic backup schemes.

Security is a component of reliability that is the measure of certainty of a device to not operate inadvertently. False or inadvertent operation of a RAS results in taking a programmed action without the appropriate arming conditions, occurrence of specified Contingency(ies), or System conditions expected to trigger the RAS action. Typical RAS actions include shedding load or generation or re-configuring the System. Such actions, if inadvertently taken, are undesirable

and may put the System in a less secure state. Worst case impacts from inadvertent operation often occur if all programmed RAS actions occur. If the System performance still satisfies PRC-012-2 Requirement R4, Part 4.3, no additional mitigation is required. Security enhancements to the RAS design, such as voting schemes, are acceptable mitigations against inadvertent operations.

Any reliability issue identified during the review must be resolved before implementing the RAS to avoid placing the System at unacceptable risk. The RAS-entity or the reviewing RC(s) may have alternative ideas or methods available to resolve the issue(s). In either case, the concern needs to be resolved in deference to reliability, and the RC has the final decision.

A specific time period for the RAS-entity to respond to the RC(s) review is not necessary because an expeditious response is in the interest of each RAS-entity to effect a timely implementation.

A specific time period for the RC to respond to the RAS-entity following the RAS review is also not necessary because the RC will be aware of (1) any reliability issues associated with the RAS not being in service and (2) the RAS-entity's schedule to implement the RAS to address those reliability issues. Since the RC is the ultimate arbiter of BES operating reliability, resolving reliability issues is a priority for the RC and serves as an incentive to expeditiously respond to the RAS-entity.

Requirement R4

Requirement R4 mandates that an evaluation of each RAS be performed at least once every five full calendar years. The purpose of a periodic RAS evaluation is to verify the continued effectiveness and coordination of the RAS, as well as to verify that requirements for BES performance following inadvertent RAS operation and single component failure continue to be satisfied. A periodic evaluation is required because changes in System topology or operating conditions may change the effectiveness of a RAS or the way it interacts with and impacts the BES.

A RAS designated as limited impact cannot, by inadvertent operation or failure to operate, cause or contribute to BES Cascading, uncontrolled separation, angular instability, voltage instability, voltage collapse, or unacceptably damped oscillations. Limited impact RAS are not subject to the RAS single component malfunction and failure tests of Parts 4.1.4 and 4.1.5, respectively. Requiring a limited impact RAS to meet these tests would add complexity to the design with minimal benefit to BES reliability.

A RAS implemented after the effective date of this standard can only be designated as limited impact by the reviewing RC(s). A RAS implemented prior to the effective date of PRC-012-2 that has been through the regional review processes of WECC or NPCC and is classified as either a Local Area Protection Scheme (LAPS) in WECC or a Type III in NPCC is recognized as a limited impact RAS upon the effective date of PRC-012-2 for the purposes of this standard and is subject to all applicable requirements.

Requirement R4 also clarifies that the RAS single component failure and inadvertent operation tests do not apply to RAS which are determined to be limited impact. Requiring a limited impact RAS to meet the single component failure and inadvertent operation tests would just add complexity to the design with little or no improvement in the reliability of the BES.

For existing RAS, the initial performance of Requirement R4 must be completed within five full calendar years of the effective date of PRC-012-2. For new or functionally modified RAS, the initial performance of the requirement must be completed within five full calendar years of the RAS approval date by the reviewing RC(s). Five full calendar years was selected as the maximum time frame between evaluations based on the time frames for similar requirements in Reliability Standards PRC-006, PRC-010, and PRC-014. The RAS evaluation can be performed sooner if it is determined that material changes to System topology or System operating conditions could potentially impact the effectiveness or coordination of the RAS. System changes also have the potential to alter the reliability impact of limited impact RAS on the BES. Requirement 4, Part 4.1.3 explicitly requires the periodic evaluation of limited impact RAS to verify the limited impact designation remains applicable. The periodic RAS evaluation will typically lead to one of the following outcomes: 1) affirmation that the existing RAS is effective; 2) identification of changes needed to the existing RAS; or, 3) justification for RAS retirement.

The items required to be addressed in the evaluations (Requirement R4, Parts 4.1.1 through 4.1.5) are planning analyses that may involve modeling of the interconnected transmission system to assess BES performance. The PC is the functional entity best suited to perform the analyses because they have a wide-area planning perspective. To promote reliability, the PC is required to provide the results of the evaluation to each impacted Transmission Planner and Planning Coordinator, in addition to each reviewing RC and RAS-entity. In cases where a RAS crosses PC boundaries, each affected PC is responsible for conducting either individual evaluations or participating in a coordinated evaluation.

The intent of Requirement R4, Part 4.1.4 is to verify that the possible inadvertent operation of the RAS (other than limited impact RAS), caused by the malfunction of a single component of the RAS, meet the same System performance requirements as those required for the Contingency(ies) or System conditions for which it is designed. If the RAS is designed to meet one of the planning events (P0-P7) in TPL-001-4, the possible inadvertent operation of the RAS must meet the same performance requirements listed in the standard for that planning event. The requirement clarifies that the inadvertent operation to be considered is only that caused by the malfunction of a single RAS component. This allows features to be designed into the RAS to improve security, such that inadvertent operation due to malfunction of a single component is prevented; otherwise, the RAS inadvertent operation must satisfy Requirement R4, Part 4.1.4.

The intent of Requirement R4, Part 4.1.4 is also to verify that the possible inadvertent operation of the RAS (other than limited impact RAS) installed for an extreme event in TPL-001-4 or for some other Contingency or System conditions not defined in TPL-001-4 (therefore without performance requirements), meet the minimum System performance requirements of Category P7 in Table 1 of NERC Reliability Standard TPL-001-4. However, instead of referring to the TPL

standard, the requirement lists the System performance requirements that a potential inadvertent operation must satisfy. The performance requirements listed (Requirement R4, Parts 4.1.4.1 – 4.1.4.5) are the ones that are common to all planning events (P0-P7) listed in TPL-001-4.

With reference to Requirement 4, Part 4.1.4, note that the only differences in performance requirements among the TPL (P0-P7) events (not common to all of them) concern Non-Consequential Load Loss and interruption of Firm Transmission Service. It is not necessary for Requirement R4, Part 4.1.4 to specify performance requirements related to these areas because a RAS is only allowed to drop non-consequential load or interrupt Firm Transmission Service if that action is allowed for the Contingency for which it is designed. Therefore, the inadvertent operation should automatically meet Non-Consequential Load Loss or interrupting Firm Transmission Service performance requirements for the Contingency(ies) for which it was designed.

The intent of Requirement R4, Part 4.1.5 is to verify that a single component failure in a RAS, other than limited impact RAS, when the RAS is intended to operate, does not prevent the BES from meeting the same performance requirements (defined in Reliability Standard TPL-001-4 or its successor) as those required for the events and conditions for which the RAS is designed. This analysis is needed to ensure that changing System conditions do not result in the single component failure requirement not being met.

The following is an example of a single component failure causing the System to fail to meet the performance requirements for the P1 event for which the RAS was installed. Consider the instance where a three-phase Fault (P1 event) results in a generating plant becoming unstable (a violation of the System performance requirements of TPL-001-4). To resolve this, a RAS is installed to trip a single generating unit which allows the remaining units at the plant to remain stable. If failure of a single component (e.g., relay) in the RAS results in the RAS failing to operate for the P1 event, the generating plant would become unstable (failing to meet the System performance requirements of TPL-001-4 for a P1 event).

Requirement R4, Part 4.1.5 does not mandate that all RAS have redundant components. For example:

- Consider the instance where a RAS is installed to mitigate an extreme event in TPL-001-4. There are no System performance requirements for extreme events; therefore, the RAS does not need redundancy to meet the same performance requirements as those required for the events and conditions for which the RAS was designed.

- Consider a RAS that arms more load or generation than necessary such that failure of the RAS to drop a portion of load or generation due to that single component failure will still result in satisfactory System performance, as long as tripping the total armed amount of load or generation does not cause other adverse impacts to reliability.

The scope of the periodic evaluation does not include a new review of the physical implementation of the RAS, as this was confirmed by the RC during the initial review and verified by subsequent functional testing. However, it is possible that a RAS design which previously satisfied requirements for inadvertent RAS operation and single component failure by means other than component redundancy may fail to satisfy these requirements at a later time, and must be evaluated with respect to the current System. For example, if the actions of a particular RAS include tripping load, load growth could occur over time that impacts the amount of load to be tripped. These changes could result in tripping too much load upon inadvertent operation and result in violations of Facility Ratings. Alternatively, the RAS might be designed to trip more load than necessary (i.e., "over trip") in order to satisfy single component failure requirements. System changes could result in too little load being tripped and unacceptable BES performance if one of the loads failed to trip.

Requirement R5

The correct operation of a RAS is important to maintain the reliability and integrity of the BES. Any incorrect operation of a RAS indicates the RAS effectiveness and/or coordination may have been compromised. Therefore, all operations of a RAS and failures of a RAS to operate when expected must be analyzed to verify that the RAS operation was consistent with its intended functionality and design.

A RAS operational performance analysis is intended to: (1) verify RAS operation is consistent with implemented design; or (2) identify RAS performance deficiencies that manifested in the incorrect RAS operation or failure of RAS to operate when expected.

The 120 full calendar day time frame for the completion of RAS operational performance analysis aligns with the time frame established in Requirement R1 from PRC-004-4 regarding the investigation of a Protection System Misoperation; however, flexibility is provided by allowing the parties to negotiate a different schedule for the analysis. To promote reliability, the RAS-entity(s) is required to provide the results of RAS operational performance analyses to its reviewing RC(s) if the analyses revealed a deficiency.

The RAS-entity(ies) may need to collaborate with its associated Transmission Planner to comprehensively analyze RAS operational performance. This is because a RAS operational performance analysis involves verifying that the RAS operation was triggered correctly (Part 5.1.1), responded as designed (Part 5.1.2), and that the resulting BES response (Parts 5.1.3 and 5.1.4) was consistent with the intended functionality and design of the RAS. Ideally, when there is more than one RAS-entity for a RAS, the RAS-entities would collaborate to conduct and submit a single, coordinated operational performance analysis.

Requirement R6

RAS deficiencies potentially pose a reliability risk to the BES. RAS deficiencies may be identified in the periodic RAS evaluation conducted by the PC in Requirement R4, in the operational analysis conducted by the RAS-entity in Requirement R5, or in the functional test performed by the RAS-entity(ies) in Requirement R8. To mitigate potential reliability risks, Requirement R6

mandates that each RAS-entity participate in developing a CAP that establishes the mitigation actions and timetable necessary to address the deficiency.

The RAS-entity(ies) that owns the RAS components, is responsible for the RAS equipment, and is in the best position to develop the timelines and perform the necessary work to correct RAS deficiencies. If necessary, the RAS-entity(ies) may request assistance with development of the CAP from other parties such as its Transmission Planner or Planning Coordinator; however, the RAS-entity has the responsibility for compliance with this requirement.

A CAP may require functional changes be made to a RAS. In this case, Attachment 1 information must be submitted to the reviewing RC(s), an RC review must be performed to obtain RC approval before the RAS-entity can place RAS modifications in service, per Requirements R1, R2, and R3.

Depending on the complexity of the issues, development of a CAP may require study, engineering or consulting work. A timeframe of six full calendar months is allotted to allow enough time for RAS-entity collaboration on the CAP development, while ensuring that deficiencies are addressed in a reasonable time. Ideally, when there is more than one RAS-entity for a RAS, the RAS-entities would collaborate to develop and submit a single, coordinated CAP. A RAS deficiency may require the RC or Transmission Operator to impose operating restrictions so the System can operate in a reliable way until the RAS deficiency is resolved. The possibility of such operating restrictions will incent the RAS-entity to resolve the issue as quickly as possible.

The following are example situations of when a CAP is required:

- A determination after a RAS operation/non-operation investigation that the RAS did not meet performance expectations or did not operate as designed.
- Periodic planning assessment reveals RAS changes are necessary to correct performance or coordination issues.
- Equipment failures.
- Functional testing identifies that a RAS is not operating as designed.

Requirement R7

Requirement R7 mandates that each RAS-entity implement its CAP developed in Requirement R6 which mitigates the deficiencies identified in Requirements R4, R5, or R8. By definition, a CAP is: “A list of actions and an associated timetable for implementation to remedy a specific problem.”

A CAP can be modified if necessary to account for adjustments to the actions or scheduled timetable of activities. If the CAP is changed, the RAS-entity must notify the reviewing Reliability

Coordinator(s). The RAS-entity must also notify the Reliability Coordinator(s) when the CAP has been completed.

The implementation of a properly developed CAP ensures that RAS deficiencies are mitigated in a timely manner. A RAS deficiency may require the RC or Transmission Operator to impose operating restrictions so the System can operate in a reliable way until the CAP is completed. The possibility of such operating restrictions will incent the RAS-entity to complete the CAP as quickly as possible.

Requirement R8

The reliability objective of Requirement R8 is to test the non-Protection System components of a RAS (controllers such as programmable logic controllers (PLCs)) and to verify the overall performance of the RAS through functional testing. Functional tests validate RAS operation by ensuring System states are detected and processed, and that actions taken by the controls are correct and occur within the expected time using the in-service settings and logic. Functional testing is aimed at assuring overall RAS performance and not the component focused testing contained in the PRC-005 maintenance standard.

Since the functional test operates the RAS under controlled conditions with known System states and expected results, testing and analysis can be performed with minimum impact to the BES and should align with expected results. The RAS-entity is in the best position to determine the testing procedure and schedule due to their overall knowledge of the RAS design, installation, and functionality. Periodic testing provides the RAS-entity assurance that latent failures may be identified and also promotes identification of changes in the System that may have introduced latent failures.

The six and twelve full calendar year functional testing intervals are greater than the annual or bi-annual periodic testing performed in some NERC Regions. However, these intervals are a balance between the resources required to perform the testing and the potential reliability impacts to the BES created by undiscovered latent failures that could cause an incorrect operation of the RAS. Longer test intervals for limited impact RAS are acceptable because incorrect operations or failures to operate present a low reliability risk to the Bulk Power System.

Functional testing is not synonymous with end-to-end testing. End-to-end testing is an acceptable method but may not be feasible for many RAS. When end-to-end testing is not possible, a RAS-entity may use a segmented functional testing approach. The segments can be tested individually negating the need for complex maintenance schedules. In addition, actual RAS operation(s) can be used to fulfill the functional testing requirement. If a RAS does not operate in its entirety during a System event or System conditions do not allow an end-to-end scheme test, then the segmented approach should be used to fulfill this Requirement. Functional testing includes the testing of all RAS inputs used for detection, arming, operating, and data collection. Functional testing, by default operates the processing logic and infrastructure of a RAS, but focuses on the RAS inputs as well as the actions initiated by RAS

outputs to address the System condition(s) for which the RAS is designed. All segments and components of a RAS must be tested or have proven operations within the applicable maximum test interval to demonstrate compliance with the Requirement.

As an example of segment testing, consider a RAS controller implemented using a PLC that receives System data, such as loading or line status, from distributed devices. These distributed devices could include meters, protective relays, or other PLCs. In this example RAS, a line protective relay is used to provide an analog metering quantity to the RAS control PLC. A functional test would verify that the System data is received from the protective relay by the PLC, processed by the PLC, and that PLC outputs are appropriate. There is no need to verify the protective relay's ability to measure the power system quantities, as this is a requirement for Protection Systems used as RAS in PRC-005, Table 1-1, Component Type – Protective Relay. Rather the functional test is focused on the use of the protective relay data at the PLC, including the communications data path from relay to PLC if this data is essential for proper RAS operation. Additionally, if the control signal back to the protective relay is also critical to the proper functioning of this example RAS, then that path is also verified up to the protective relay. This example describes a test for one segment of a RAS which verifies RAS action, verifies PLC control logic, and verifies RAS communications.

IEEE C37.233, "IEEE Guide for Power System Protection Testing," 2009 section 8 (particularly 8.3-8.5), provides an overview of functional testing. The following opens section 8.3:

> Proper implementation requires a well-defined and coordinated test plan for performance evaluation of the overall system during agreed maintenance intervals. The maintenance test plan, also referred to as functional system testing, should include inputs, outputs, communication, logic, and throughput timing tests. The functional tests are generally not component-level testing, rather overall system testing. Some of the input tests may need to be done ahead of overall system testing to the extent that the tests affect the overall performance. The test coordinator or coordinators need to have full knowledge of the intent of the scheme, isolation points, simulation scenarios, and restoration to normal procedures.
>
> The concept is to validate the overall performance of the scheme, including the logic where applicable, to validate the overall throughput times against system modeling for different types of Contingencies, and to verify scheme performance as well as the inputs and outputs.

If a RAS passes a functional test, it is not necessary to provide that specific information to the RC because that is the expected result and requires no further action. If a segment of a RAS fails a functional test, the status of that degraded RAS is required to be reported (in Real-time) to the Transmission Operator via PRC-001, Requirement R6, then to the RC via TOP-001-3, Requirement R8. See Phase 2 of Project 2007-06 for the mapping document from PRC-001 to other standards regarding notification of RC by TOP if a deficiency is found during testing. Consequently, it is not necessary to include a similar requirement in this standard.

The initial test interval begins on the effective date of the standard pursuant to the implementation plan. Subsequently, the maximum allowable interval between functional tests

is six full calendar years for RAS that are not designated as limited impact RAS and twelve full calendar years for RAS that are designated as limited impact RAS. The interval between tests begins on the date of the most recent successful test for each individual segment or end-to-end test. A successful test of one segment only resets the test interval clock for that segment. A RAS-entity may choose to count a correct RAS operation as a qualifying functional test for those RAS segments which operate. If a System event causes a correct, but partial RAS operation, separate functional tests of the segments that did not operate are still required within the maximum test interval that started on the date of the previous successful test of those (non-operating) segments in order to be compliant with Requirement R8.

Requirement R9

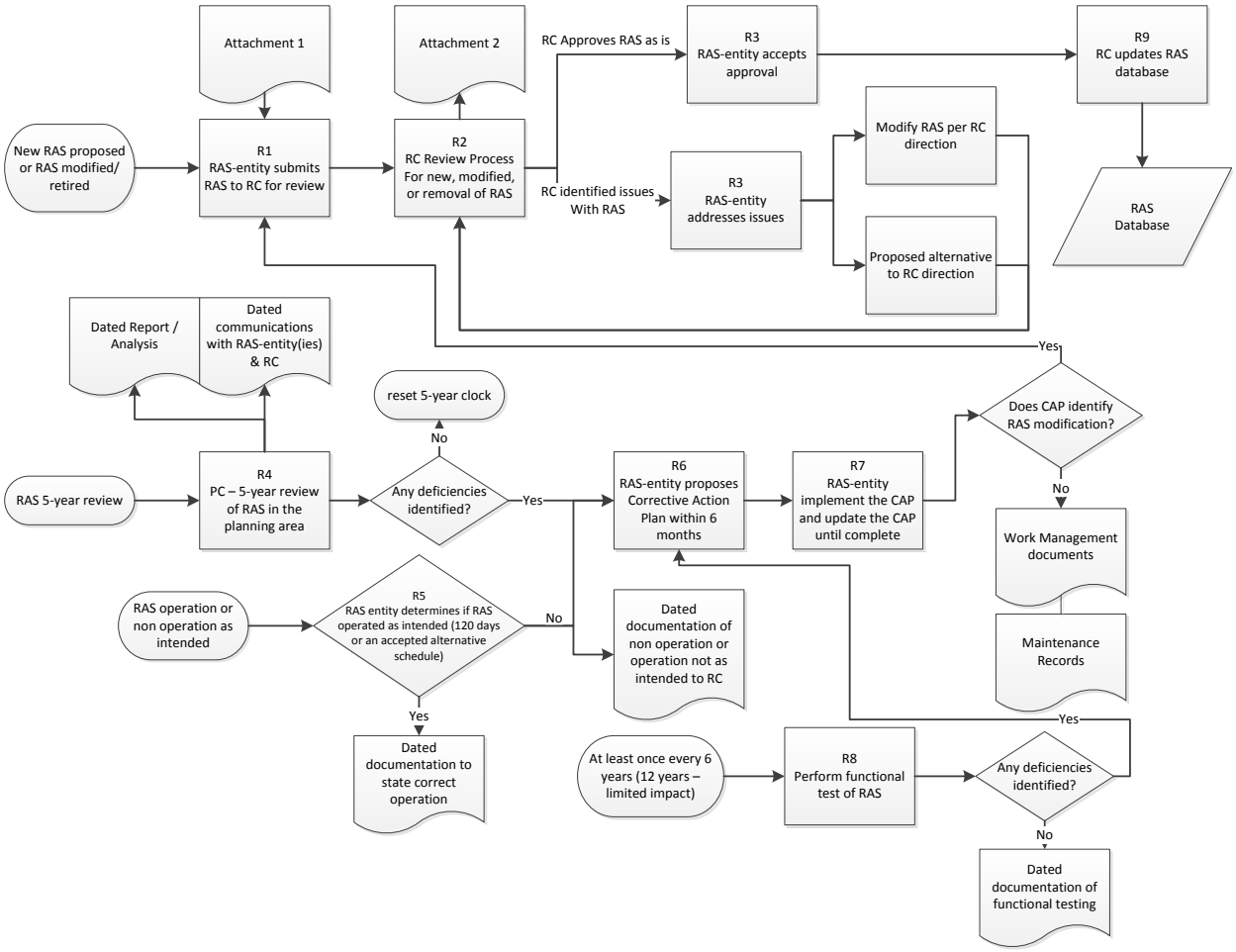
The RAS database required to be maintained by the RC in Requirement R9 ensures information regarding existing RAS is available. Attachment 3 contains the minimum information that is required to be included about each RAS listed in the database. Additional information can be requested by the RC.

The database enables the RC to provide other entities high-level information on existing RAS that could potentially impact the operational and/or planning activities of that entity. The information provided is sufficient for an entity with a reliability need to evaluate whether the RAS can impact its System. For example, a RAS performing generation rejection to mitigate an overload on a transmission line may cause a power flow change within an adjacent entity area. This entity should be able to evaluate the risk that a RAS poses to its System from the high-level information provided in the RAS database.

The RAS database does not need to list detailed settings or modeling information, but the description of the System performance issues, System conditions, and the intended corrective actions must be included. If additional details about the RAS operation are required, the entity may obtain the contact information of the RAS-entity from the RC.

Process Flow Diagram

The diagram below depicts the process flow of the PRC-012-2 requirements.



Technical Justifications for Attachment 1 Content Supporting Documentation for RAS Review

To perform an adequate review of the expected reliability implications of a Remedial Action Scheme (RAS), it is necessary for the RAS-entity(ies) to provide a detailed list of information describing the RAS to the reviewing RC. If there are multiple RAS-entities for a single RAS, information will be needed from all RAS-entities. Ideally, in such cases, a single RAS-entity will take the lead to compile all the data identified into a single Attachment 1.

The necessary data ranges from a general overview of the RAS to summarized results of transmission planning studies, to information about hardware used to implement the RAS. Coordination between the RAS and other RAS and protection and control systems will be examined for possible adverse interactions. This review can include wide-ranging electrical design issues involving the specific hardware, logic, telecommunications, and other relevant equipment and controls that make up the RAS.

Attachment 1

The following checklist identifies important RAS information for each new or functionally modified[8] RAS that the RAS-entity shall document and provide to the RC for review pursuant to Requirement R1. When a RAS has been previously reviewed, only the proposed modifications to that RAS require review; however, it will be helpful to each reviewing RC if the RAS-entity provides a summary of the existing RAS functionality.

I. General

1. Information such as maps, one-line drawings, substation and schematic drawings that identify the physical and electrical location of the RAS and related facilities.

   Provide a description of the RAS to give an overall understanding of the functionality and a map showing the location of the RAS. Identify other protection and control systems requiring coordination with the RAS. See RAS Design below for additional information.

   Provide a single-line drawing(s) showing all sites involved. The drawing(s) should provide sufficient information to allow the RC review team to assess design reliability, and should include information such as the bus arrangement, circuit breakers, the associated switches, etc. For each site, indicate whether detection, logic, action, or a combination of these is present.

2. Functionality of new RAS or proposed functional modifications to existing RAS and documentation of the pre- and post-modified functionality of the RAS.

[8] Functionally modified: Any modification to a RAS consisting of any of the following:
- Changes to System conditions or contingencies monitored by the RAS
- Changes to the actions the RAS is designed to initiate
- Changes to RAS hardware beyond in-kind replacement; i.e., match the original functionality of existing components
- Changes to RAS logic beyond correcting existing errors
- Changes to redundancy levels; i.e., addition or removal

3. The Corrective Action Plan (CAP) if RAS modifications are proposed in a CAP. [Reference NERC Reliability Standard PRC-012-2, Requirements R5 and R7]

   Provide a description of any functional modifications to a RAS that are part of a CAP that are proposed to address performance deficiency(ies) identified in the periodic evaluation pursuant to Requirement R4, the analysis of an actual RAS operation pursuant to Requirement R5, or functional test failure pursuant to Requirement R8. A copy of the most recent CAP must be submitted in addition to the other data specified in Attachment 1.

4. Initial data to populate the RAS database.

   a. RAS name.

   b. Each RAS-entity and contact information.

   c. Expected or actual in-service date; most recent (Requirement R3) RC-approval date; most recent five full calendar year (Requirement R4) evaluation date; and, date of retirement, if applicable.

   d. System performance issue or reason for installing the RAS (*e.g.*, thermal overload, angular instability, poor oscillation damping, voltage instability, under-/over-voltage, slow voltage recovery).

   e. Description of the Contingencies or System conditions for which the RAS was designed (initiating conditions).

   f. Corrective action taken by the RAS.

   g. Identification of limited impact[9] RAS.

   h. Any additional explanation relevant to high level understanding of the RAS.

      Note: This is the same information as is identified in Attachment 3. Supplying the data at this point in the review process ensures a more complete review and minimizes any administrative burden on the reviewing RC(s).

II. Functional Description and Transmission Planning Information

1. Contingencies and System conditions that the RAS is intended to remedy. [Reference NERC Reliability Standards PRC-012, R1.2 and PRC-013, R1.1]

   a. The System conditions that would result if no RAS action occurred should be identified.

   b. Include a description of the System conditions that should arm the RAS so as to be ready to take action upon subsequent occurrence of the critical System Contingencies or other operating conditions when RAS action is intended to occur. If no arming conditions are required, this should also be stated.

[9] A RAS designated as limited impact cannot, by inadvertent operation or failure to operate, cause or contribute to BES Cascading, uncontrolled separation, angular instability, voltage instability, voltage collapse, or unacceptably damped oscillations.

c. Event-based RAS are triggered by specific Contingencies that initiate mitigating action. Condition-based RAS may also be initiated by specific Contingencies, but specific Contingencies are not always required. These triggering Contingencies and/or conditions should be identified.

2. The actions to be taken by the RAS in response to disturbance conditions. [Reference NERC Reliability Standards PRC-012, R1.2 and PRC-013, R1.2]

   Mitigating actions are designed to result in acceptable System performance. These actions should be identified, including any time constraints and/or "backup" mitigating measures that may be required in case of a single RAS component failure.

3. A summary of technical studies, if applicable, demonstrating that the proposed RAS actions satisfy System performance objectives for the scope of System events and conditions that the RAS is intended to remedy. The technical studies summary shall also include information such as the study year(s), System conditions, and Contingencies analyzed on which the RAS design is based, and the date those technical studies were performed. [Reference NEC Reliability Standard PRC-014, R3.2]

   Review the scheme purpose and impact to ensure it is (still) necessary, serves the intended purposes, and meets current performance requirements. While copies of the full, detailed studies may not be necessary, any abbreviated descriptions of the studies must be detailed enough to allow the reviewing RC(s) to be convinced of the need for the scheme and the results of RAS-related operations.

4. Information regarding any future System plans that will impact the RAS. [Reference NERC Reliability Standard PRC-014, R3.2]

   The RC's other responsibilities under the NERC Reliability Standards focus on the Operating Horizon, rather than the Planning Horizon. As such, the RC is less likely to be aware of any longer range plans that may have an impact on the proposed RAS. Such knowledge of future Plans is helpful to provide perspective on the capabilities of the RAS.

5. RAS-entity proposal and justification for limited impact designation, if applicable.

   A RAS designated as limited impact cannot, by inadvertent operation or failure to operate, cause or contribute to BES Cascading, uncontrolled separation, angular instability, voltage instability, voltage collapse, or unacceptably damped oscillations. A RAS implemented prior to the effective date of PRC-012-2 that has been through the regional review processes of WECC or NPCC and is classified as either a Local Area Protection Scheme (LAPS) in WECC or a Type 3 in NPCC is recognized as a limited impact RAS upon the effective date of PRC-012-2 for the purposes of this standard and is subject to all applicable requirements.

6. Documentation describing the System performance resulting from the possible inadvertent operation of the RAS, except for limited impact RAS, caused by any single RAS component malfunction. Single component malfunctions in a RAS not determined to be limited impact must satisfy all of the following: [Reference NERC Reliability Standard PRC-012, R1.4]

a. The BES shall remain stable.

b. Cascading shall not occur.

c. Applicable Facility Ratings shall not be exceeded.

d. BES voltages shall be within post-Contingency voltage limits and post-Contingency voltage deviation limits as established by the Transmission Planner and the Planning Coordinator.

e. Transient voltage responses shall be within acceptable limits as established by the Transmission Planner and the Planning Coordinator.

7. An evaluation indicating that the RAS settings and operation avoids adverse interactions with other RAS, and protection and control systems.
[Reference NERC Reliability Standards PRC-012, R1.5 and PRC-014, R3.4]

   RAS are complex schemes that may take action such as tripping load or generation or re-configuring the System. Many RAS depend on sensing specific System configurations to determine whether they need to arm or take actions. An examples of an adverse interaction: A RAS that reconfigures the System also changes the available Fault duty, which can affect distance relay overcurrent ("fault detector") supervision and ground overcurrent protection coordination.

8. Identification of other affected RCs.

   This information is needed to aid in information exchange among all affected entities and coordination of the RAS with other RAS and protection and control systems.

III. Implementation

1. Documentation describing the applicable equipment used for detection, dc supply, communications, transfer trip, logic processing, control actions, and monitoring.

   Detection

   Detection and initiating devices, whether for arming or triggering action, should be designed to be secure. Several types of devices have been commonly used as disturbance, condition, or status detectors:

   - Line open status (event detectors),
   - Protective relay inputs and outputs (event and parameter detectors),
   - Transducer and IED (analog) inputs (parameter and response detectors),
   - Rate of change (parameter and response detectors).

   DC Supply

   Batteries and charges, or other forms of dc supply for RAS, are commonly also used for Protection Systems. This is acceptable, and maintenance of such supplies is covered by PRC-005. However, redundant RAS, when used, should be supplied from separately protected (fused or breakered) circuits.

Communications: Telecommunications Channels

Telecommunications channels used for sending and receiving RAS information between sites and/or transfer trip devices should meet at least the same criteria as other relaying protection communication channels. Discuss performance of any non-deterministic communication systems used (such as Ethernet).

The scheme logic should be designed so that loss of the channel, noise, or other channel or equipment failure will not result in a false operation of the scheme.

It is highly desirable that the channel equipment and communications media (power line carrier, microwave, optical fiber, etc.) be owned and maintained by the RAS-entity, or perhaps leased from another entity familiar with the necessary reliability requirements. All channel equipment should be monitored and alarmed to the dispatch center so that timely diagnostic and repair action shall take place upon failure. Publicly switched telephone networks are generally an undesirable option.

Communication channels should be well labeled or identified so that the personnel working on the channel can readily identify the proper circuit. Channels between entities should be identified with a common name at all terminals.

Transfer Trip

Transfer trip equipment, when separate from other RAS equipment, should be monitored and labeled similarly to the channel equipment.

Logic Processing

All RAS require some form of logic processing to determine the action to take when the scheme is triggered. Required actions are always scheme dependent. Different actions may be required at different arming levels or for different Contingencies. Scheme logic may be achievable by something as simple as wiring a few auxiliary relay contacts or by much more complex logic processing.

Platforms that have been used reliably and successfully include PLCs in various forms, personal computers (PCs), microprocessor protective relays, remote terminal units (RTUs), and logic processors. Single-function relays have been used historically to implement RAS, but this approach is now less common except for very simple new RAS or minor additions to existing RAS.

Control Actions

RAS action devices may include a variety of equipment such as transfer trip, protective relays, and other control devices. These devices receive commands from the logic processing function (perhaps through telecommunication facilities) and initiate RAS actions at the sites where action is required.

Monitoring by SCADA/EMS should include at least

- Whether the scheme is in service or out of service.
    - For RAS that are armed manually, the arming status may be the same as whether the RAS is in service or out of service.

- For RAS that are armed automatically, these two states are independent because a RAS that has been placed in service may be armed or unarmed based on whether the automatic arming criteria have been met.

- The current operational state of the scheme (available or not).
- In cases where the RAS requires single component failure performance; e.g., redundancy, the minimal status indications should be provided separately for each RAS.
  - The minimum status is generally sufficient for operational purposes; however, where possible it is often useful to provide additional information regarding partial failures or the status of critical components to allow the RAS-entity to more efficiently troubleshoot a reported failure. Whether this capability exists will depend in part on the design and vintage of equipment used in the RAS. While all schemes should provide the minimum level of monitoring, new schemes should be designed with the objective of providing monitoring at least similar to what is provided for microprocessor-based Protection Systems.

2. Information on detection logic and settings/parameters that control the operation of the RAS. [Reference NERC Reliability Standards PRC-012, R1.2 and PRC-013, R1.3]

   Several methods to determine line or other equipment status are in common use, often in combination:

   a. Auxiliary switch contacts from circuit breakers and disconnect switches (52a/b, 89a/b)—the most common status monitor; “a” contacts exactly emulate actual breaker status, while “b” contacts are opposite to the status of the breaker;

   b. Undercurrent detection—a low level indicates an open condition, including at the far end of a line; pickup is typically slightly above the total line-charging current;

   c. Breaker trip coil current monitoring—typically used when high-speed RAS response is required, but usually in combination with auxiliary switch contacts and/or other detection because the trip coil current ceases when the breaker opens; and

   d. Other detectors such as angle, voltage, power, frequency, rate of change of the aforementioned, out of step, etc. are dependent on specific scheme requirements, but some forms may substitute for or enhance other monitoring described in items ‘a’, ‘b’, and ‘c’ above.

   Both RAS arming and action triggers often require monitoring of analog quantities such as power, current, and voltage at one or more locations and are set to detect a specific level of the pertinent quantity. These monitors may be relays, meters, transducers, or other devices

3. Documentation showing that any multifunction device used to perform RAS function(s), in addition to other functions such as protective relaying or SCADA, does not compromise the reliability of the RAS when the device is not in service or is being maintained.

In this context, a multifunction device (e.g., microprocessor-based relay) is a single component that is used to perform the function of a RAS in addition to protective relaying and/or SCADA simultaneously. It is important that other applications in the multifunction device do not compromise the functionality of the RAS when the device is in service or when it is being maintained. The following list outlines considerations when the RAS function is applied in the same microprocessor-based relay as equipment protection functions:

a. Describe how the multifunction device is applied in the RAS.

b. Show the general arrangement and describe how the multi-function device is labeled in the design and application, so as to identify the RAS and other device functions.

c. Describe the procedures used to isolate the RAS function from other functions in the device.

d. Describe the procedures used when each multifunction device is removed from service and whether coordination with other protection schemes is required.

e. Describe how each multifunction device is tested, both for commissioning and during periodic maintenance testing, with regard to each function of the device.

f. Describe how overall periodic RAS functional and throughput tests are performed if multifunction devices are used for both local protection and RAS.

g. Describe how upgrades to the multifunction device, such as firmware upgrades, are accomplished. How is the RAS function taken into consideration?

Other devices that are usually not considered multifunction devices such as auxiliary relays, control switches, and instrument transformers may serve multiple purposes such as protection and RAS. Similar concerns apply for these applications as noted above.

4. Documentation describing the System performance resulting from a single component failure in the RAS, except for limited impact RAS, when the RAS is intended to operate. A single component failure in a RAS not determined to be limited impact must not prevent the BES from meeting the same performance requirements (defined in Reliability Standard TPL-001-4 or its successor) as those required for the events and conditions for which the RAS is designed. The documentation should describe or illustrate how the design achieves this objective. [Reference NERC Reliability Standard PRC-012, R1.3]

   RAS automatic arming, if applicable, is vital to RAS and System performance and is therefore included in this requirement.

   Acceptable methods to achieve this objective include, but are not limited to the following:

   a. Providing redundancy of RAS components. Typical examples are listed below:

      i. Protective or auxiliary relays used by the RAS.

ii. Communications systems necessary for correct operation of the RAS.

iii. Sensing devices used to measure electrical or other quantities used by the RAS.

iv. Station dc supply associated with RAS functions.

v. Control circuitry associated with RAS functions through the trip coil(s) of the circuit breakers or other interrupting devices.

vi. Logic processing devices that accept System inputs from RAS components or other sources, make decisions based on those inputs, or initiate output signals to take remedial actions.

b. Arming more load or generation than necessary such that failure of the RAS to drop a portion of load or generation due to that single component failure will still result in satisfactory System performance, as long as tripping the total armed amount of load or generation does not cause other adverse impacts to reliability.

c. Using alternative automatic actions to back up failures of single RAS components.

d. Manual backup operations, using planned System adjustments such as Transmission configuration changes and re-dispatch of generation, if such adjustments are executable within the time duration applicable to the Facility Ratings.

5. Documentation describing the functional testing process.

IV. RAS Retirement

The following checklist identifies important RAS information for each existing RAS to be retired that the RAS-entity shall document and provide to the Reliability Coordinator for review pursuant to Requirement R1.

1. Information necessary to ensure that the Reliability Coordinator is able to understand the physical and electrical location of the RAS and related facilities.

2. A summary of technical studies and technical justifications, if applicable, upon which the decision to retire the RAS is based.

3. Anticipated date of RAS retirement.

While the documentation necessary to evaluate RAS removals is not as extensive as for new or functionally modified RAS, it is still vital that, when the RAS is no longer available, System performance will still meet the appropriate (usually TPL) requirements for the Contingencies or System conditions that the RAS had been installed to remediate.

Technical Justification for Attachment 2 Content

Reliability Coordinator RAS Review Checklist

Attachment 2 is a checklist provided to facilitate consistent reviews continent-wide for new or functionally modified RAS prior to the RAS installation. The checklist is meant to assist the RC in identifying reliability-related considerations relevant to various aspects of RAS design and implementation.

Technical Justifications for Attachment 3 Content

Database Information

Attachment 3 contains the minimum information that the RC must consolidate into its database for each RAS in its area.

1. RAS name.
   - The name used to identify the RAS.
2. Each RAS-entity and contact information.
   - A reliable phone number or email address should be included to contact each RAS-entity if more information is needed.
3. Expected or actual in-service date; most recent (Requirement R3) RC-approval date; most recent five full calendar year (Requirement R4) evaluation date; and, date of retirement, if applicable.
   - Specify each applicable date.
4. System performance issue or reason for installing the RAS (e.g., thermal overload, angular instability, poor oscillation damping, voltage instability, under-/over-voltage, slow voltage recovery).
   - A short description of the reason for installing the RAS is sufficient, as long as the main System issues addressed by the RAS can be identified by someone with a reliability need.
5. Description of the Contingencies or System conditions for which the RAS was designed (initiating conditions).
   - A high level summary of the conditions/Contingencies is expected. Not all combinations of conditions are required to be listed.
6. Corrective action taken by the RAS.
   - A short description of the actions should be given. For schemes shedding load or generation, the maximum amount of megawatts should be included.

7. Identification of limited impact[10] RAS.
    - Specify whether or not the RAS is designated as limited impact.
8. Any additional explanation relevant to high-level understanding of the RAS.
    - If deemed necessary, any additional information can be included in this section, but is not mandatory.

[10] A RAS designated as limited impact cannot, by inadvertent operation or failure to operate, cause or contribute to BES Cascading, uncontrolled separation, angular instability, voltage instability, voltage collapse, or unacceptably damped oscillations.

Rationale

Rationale for Requirement R1: Each Remedial Action Scheme (RAS) is unique and its action(s) can have a significant impact on the reliability and integrity of the Bulk Electric System (BES). Therefore, a review of a proposed new RAS or an existing RAS proposed for functional modification or retirement; i.e., removal from service must be completed prior to implementation or retirement.

Functional modifications consist of any of the following:

- Changes to System conditions or Contingencies monitored by the RAS
- Changes to the actions the RAS is designed to initiate
- Changes to RAS hardware beyond in-kind replacement; i.e., match the original functionality of existing components
- Changes to RAS logic beyond correcting existing errors
- Changes to redundancy levels; i.e., addition or removal

To facilitate a review that promotes reliability, the RAS-entity must provide the reviewer with sufficient details of the RAS design, function, and operation. This data and supporting documentation are identified in Attachment 1 of this standard, and Requirement R1 mandates that the RAS-entity provide them to the reviewing Reliability Coordinator (RC). The RC (reviewing RC) that coordinates the area where the RAS is located is responsible for the review. Ideally, when there is more than one RAS-entity for a RAS, the RAS-entities would collaborate and submit a single, coordinated Attachment 1 to the reviewing RC. In cases where a RAS crosses RC Area boundaries, each affected RC is responsible for conducting either individual reviews or participating in a coordinated review.

Rationale for Requirement R2: The RC is the functional entity best suited to perform the RAS review because it has the widest area operational and reliability perspective of all functional entities and an awareness of reliability issues in any neighboring RC Area. This Wide Area purview facilitates the evaluation of interactions among separate RAS as well as interactions among RAS and other protection and control systems. Review by the RC also minimizes the possibility of a conflict of interest that could exist because of business relationships among the RAS-entity, Planning Coordinator (PC), Transmission Planner (TP), or other entities that are likely to be involved in the planning or implementation of a RAS. The RC is not expected to possess more information or ability than anticipated by their functional registration as designated by NERC. The RC may request assistance to perform RAS reviews from other parties such as the PC or regional technical groups; however, the RC will retain the responsibility for compliance with this requirement.

Attachment 2 of this standard is a checklist the RC can use to identify design and implementation aspects of RAS and facilitate consistent reviews for each submitted RAS. The time frame of four full calendar months is consistent with current utility and regional practice;

however, flexibility is provided by allowing the RC(s) and RAS-entity(ies) to negotiate a mutually agreed upon schedule for the review.

Note: An RC may need to include this task in its reliability plan(s) for the NERC Regions(s) in which it is located.

Rationale for Requirement R3: The RC review is intended to identify reliability issues that must be resolved before the RAS can be put in service. Examples of reliability issues include a lack of dependability, security, or coordination.

A specific time period for the RAS-entity to respond to the reviewing RC following identification of any reliability issue(s) is not necessary because the RAS-entity wants to expedite the timely approval and subsequent implementation of the RAS.

A specific time period for the RC to respond to the RAS-entity following the RAS review is also not necessary because the RC will be aware of (1) any reliability issues associated with the RAS not being in service and (2) the RAS-entity's schedule to implement the RAS to address those reliability issues. Since the RC is the ultimate arbiter of BES operating reliability, resolving reliability issues is a priority for the RC and serves as an incentive to expeditiously respond to the RAS-entity.

Rationale for Requirement R4: Requirement R4 mandates that an evaluation of each RAS be performed at least once every five full calendar years. The purpose of the periodic RAS evaluation is to verify the continued effectiveness and coordination of the RAS, as well as to verify that, if a RAS single component malfunction or single component failure were to occur, the requirements for BES performance would continue to be satisfied. A periodic evaluation is required because changes in System topology or operating conditions may change the effectiveness of a RAS or the way it impacts the BES.

RAS are unique and customized assemblages of protection and control equipment that vary in complexity and impact on the reliability of the BES. In recognition of these differences, RAS can be designated by the reviewing RC(s) as limited impact. A limited impact RAS cannot, by inadvertent operation or failure to operate, cause or contribute to BES Cascading, uncontrolled separation, angular instability, voltage instability, voltage collapse, or unacceptably damped oscillations. The "BES" qualifier in the preceding statement modifies all of the conditions that follow it. Limited impact RAS are not subject to the RAS single component malfunction and failure tests of Parts 4.1.4 and 4.1.5, respectively. Requiring a limited impact RAS to meet these tests would add complexity to the design with minimal benefit to BES reliability. See the Supplemental Material for more on the limited impact designation.

The standard recognizes the Local Area Protection Scheme (LAPS) classification in WECC (Western Electricity Coordinating Council) and the Type III classification in NPCC (Northeast Power Coordinating Council) as initially appropriate for limited impact designation. A RAS implemented prior to the effective date of PRC-012-2 that has been through the regional

review processes of WECC or NPCC and is classified as either a Local Area Protection Scheme (LAPS) in WECC or a Type III in NPCC is recognized as a limited impact RAS upon the effective date of PRC-012-2 for the purposes of this standard and is subject to all applicable requirements.

For existing RAS, the initial performance of Requirement R4 must be completed within five full calendar years of the effective date of PRC-012-2. For new or functionally modified RAS, the initial performance of the requirement must be completed within five full calendar years of the RAS approval date by the reviewing RC(s). Five full calendar years was selected as the maximum time frame between evaluations based on the time frames for similar requirements in Reliability Standards PRC-006, PRC-010, and PRC-014. The RAS evaluation can be performed sooner if it is determined that material changes to System topology or System operating conditions could potentially impact the effectiveness or coordination of the RAS. System changes also have the potential to alter the reliability impact of limited impact RAS on the BES. Requirement 4, Part 4.1.3 explicitly requires the periodic evaluation of limited impact RAS to verify the limited impact designation remains applicable; the PC can use its discretion as to how this evaluation is performed. The periodic RAS evaluation will typically lead to one of the following outcomes: 1) affirmation that the existing RAS is effective; 2) identification of changes needed to the existing RAS; or, 3) justification for RAS retirement.

The items required to be addressed in the evaluations (Requirement R4, Parts 4.1.1 through 4.1.5) are planning analyses that may involve modeling of the interconnected transmission system to assess BES performance. The Planning Coordinator (PC) is the functional entity best suited to perform this evaluation because they have a wide area planning perspective. To promote reliability, the PC is required to provide the results of the evaluation to each impacted Transmission Planner and Planning Coordinator, in addition to each reviewing RC and RAS-entity. In cases where a RAS crosses PC boundaries, each affected PC is responsible for conducting either individual evaluations or participating in a coordinated evaluation.

The previous version of this standard (PRC-012-1 Requirement 1, R1.4) states "… the inadvertent operation of a RAS shall meet the same performance requirement (TPL-001-0, TPL-002-0, and TPL-003-0) as that required of the Contingency for which it was designed, and not exceed TPL-003-0." Requirement R4 clarifies that the inadvertent operation to be considered would only be that caused by the malfunction of a single RAS component. This allows security features to be designed into the RAS such that inadvertent operation due to a single component malfunction is prevented. Otherwise, consistent with PRC-012-1 Requirement 1, R1.4, the RAS should be designed so that its whole or partial inadvertent operation due to a single component malfunction satisfies the System performance requirements for the same Contingency for which the RAS was designed.

If the RAS was installed for an extreme event in TPL-001-4 or for some other Contingency or System condition not defined in TPL-001-4 (therefore without performance requirements), its inadvertent operation still must meet some minimum System performance requirements. However, instead of referring to the TPL-001-4, Requirement R4 lists the System performance

requirements that the inadvertent operation must satisfy. The performance requirements listed (Parts 4.1.4.1 – 4.1.4.5) are the ones that are common to all planning events P0-P7 listed in TPL-001-4.

Rationale for Requirement R5: The correct operation of a RAS is important for maintaining the reliability and integrity of the BES. Any incorrect operation of a RAS indicates that the RAS effectiveness and/or coordination has been compromised. Therefore, all operations of a RAS and failures of a RAS to operate when expected must be analyzed to verify that the RAS operation was consistent with its intended functionality and design.

A RAS operational performance analysis is intended to: 1) verify RAS operation was consistent with the implemented design; or 2) identify RAS performance deficiencies that manifested in the incorrect RAS operation or failure of RAS to operate when expected.

The 120 full calendar day time frame for the completion of RAS operational performance analysis aligns with the time frame established in Requirement R1 from PRC-004-4 regarding the investigation of a Protection System Misoperation. To promote reliability, each RAS-entity is required to provide the results of RAS operational performance analyses that identified any deficiencies to its reviewing RC(s).

RAS-entities may need to collaborate with their associated Transmission Planner to comprehensively analyze RAS operational performance. This is because a RAS operational performance analysis involves verifying that the RAS operation was triggered correctly (Part 5.1.1), responded as designed (Part 5.1.2), and that the resulting BES response (Parts 5.1.3 and 5.1.4) was consistent with the intended functionality and design of the RAS. Ideally, when there is more than one RAS-entity for a RAS, the RAS-entities would collaborate to conduct and submit a single, coordinated operational performance analysis.

Rationale for Requirement R6: Deficiencies identified in the periodic RAS evaluation conducted by the PC pursuant to Requirement R4, in the operational performance analysis conducted by the RAS-entity pursuant to Requirement R5, or in the functional test performed by the RAS-entity pursuant to Requirement R8, potentially pose a reliability risk to the BES. To mitigate these potential reliability risks, Requirement R6 mandates that each RAS-entity develop a Corrective Action Plan (CAP) to address the identified deficiency. The CAP contains the mitigation actions and associated timetable necessary to remedy the specific deficiency. The RAS-entity may request assistance with CAP development from other parties such as its Transmission Planner or Planning Coordinator; however, the RAS-entity has the responsibility for compliance with this requirement.

If the CAP requires that a functional change be made to a RAS, the RAS-entity will need to submit information identified in Attachment 1 to the reviewing RC(s) prior to placing RAS modifications in service per Requirement R1.

Depending on the complexity of the identified deficiency(ies), development of a CAP may require studies, and other engineering or consulting work. A maximum time frame of six full calendar months is specified for RAS-entity collaboration on the CAP development. Ideally, when there is more than one RAS-entity for a RAS, the RAS-entities would collaborate to develop and submit a single, coordinated CAP.

Rationale for Requirement R7: Requirement R7 mandates each RAS-entity implement a CAP (developed in Requirement R6) that mitigates the deficiencies identified in Requirements R4, R5, or R8. By definition, a CAP is: "A list of actions and an associated timetable for implementation to remedy a specific problem." The implementation of a properly developed CAP ensures that RAS deficiencies are mitigated in a timely manner. Each reviewing Reliability Coordinator must be notified if CAP actions or timetables change, and when the CAP is completed.

Rationale for Requirement R8: Due to the wide variety of RAS designs and implementations, and the potential for impacting BES reliability, it is important that periodic functional testing of a RAS be performed. A functional test provides an overall confirmation of the RAS to operate as designed and verifies the proper operation of the non-Protection System (control) components of a RAS that are not addressed in PRC-005. Protection System components that are part of a RAS are maintained in accordance with PRC-005.

The six or twelve full calendar year test interval, which begins on the effective date of the standard pursuant to the PRC-012-2 implementation plan, is a balance between the resources required to perform the testing and the potential reliability impacts to the BES created by undiscovered latent failures that could cause an incorrect operation of the RAS. Extending to longer intervals increases the reliability risk to the BES posed by an undiscovered latent failure that could cause an incorrect operation or failure of the RAS. The RAS-entity is in the best position to determine the testing procedure and schedule due to its overall knowledge of the RAS design, installation, and functionality. Functional testing may be accomplished with end-to-end testing or a segmented approach. For segmented testing, each segment of a RAS must be tested. Overlapping segments can be tested individually negating the need for complex maintenance schedules and outages.

The maximum allowable interval between functional tests is six full calendar years for RAS that are not designated as limited impact RAS and twelve full calendar years for RAS that are designated as limited impact RAS. The interval between tests begins on the date of the most recent successful test for each individual segment or end-to-end test. A successful test of one segment only resets the test interval clock for that segment. A correct operation of a RAS qualifies as a functional test for those RAS segments which operate (documentation for compliance with Requirement R5 Part 5.1). If an event causes a partial operation of a RAS, the segments without an operation will require a separate functional test within the maximum interval with the starting date determined by the previous successful test of the segments that did not operate.

Rationale for Requirement R9: The RAS database is a comprehensive record of all RAS existing in a Reliability Coordinator Area. The database enables the RC to provide other entities high-level information on existing RAS that could potentially impact the operational and/or planning activities of that entity. Attachment 3 lists the minimum information required for the RAS database, which includes a summary of the RAS initiating conditions, corrective actions, and System issues being mitigated. This information allows an entity to evaluate the reliability need for requesting more detailed information from the RAS-entities identified in the database contact information. The RC is the appropriate entity to maintain the database because the RC receives the required database information when a new or modified RAS is submitted for review. The twelve full calendar month time frame is aligned with industry practice and allows sufficient time for the RC to collect the appropriate information from RAS-entities and update the RAS database.

Appendix PRC-012-2-QC-1

Specific provisions applicable in Québec for standard PRC-012-2 – Remedial Action Schemes

This appendix establishes specific provisions for the application of the standard in Québec. Provisions of the standard and of this appendix must be read jointly for comprehension and interpretation purposes. Where the standard and appendix differ, the appendix shall prevail.

A. Introduction

1. Title: No specific provisions.

2. Number: No specific provisions.

3. Purpose: No specific provisions.

4. Applicability:

4.1. Functional Entities

No specific provisions.

4.2. Facilities

No specific provisions.

5. Effective date:

5.1. Adoption of the standard by the Régie de l'énergie: October 8, 2020

5.2. Adoption of this appendix by the Régie de l'énergie: October 8, 2020

5.3. Effective date of the standard and of this appendix in Québec: January 1, 2021
The requirements will be implemented on the following dates:

Requirement	Implementation date
R1, R2, R3, R5, R6, R7	July 1, 2023
R4	July 1, 2025
R8	• July 1, 2026: Deadline to complete a first test of RAS not designated as limited impact. • July 1, 2032: deadline to complete a first test of RAS designated as limited impact.
R9	July 1, 2023: Deadline to establish a RAS database.

B. Requirements and Measures

Replace all references to "BES" with "RTP."

Specific provision applicable to Requirement R8:

Requirement R8 applies as stipulated in the Standard, except for those Remedial Action Schemes (RAS) installed prior to the effective date of the Standard, in which case Requirement R8 is replaced by the following text:

R8: Unless the Compliance Enforcement Authority has granted a technical feasibility exception for a functional test, each RAS-entity shall participate in performing a functional test of each of its RAS to

verify the overall RAS performance and the proper operation of non-Protection System components: [Violation Risk Factor: High] [Time Horizon: Long-term Planning]

- At least once every six full calendar years for all RAS not designated as limited impact, or
- At least once every twelve full calendar years for all RAS designated as limited impact.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

In Québec, "Compliance Enforcement Authority" means the Régie de l'énergie in its roles of monitoring and enforcing compliance with respect to the Reliability Standard and to this appendix.

1.2. Evidence Retention

No specific provisions.

1.3. Compliance Monitoring and Enforcement Program

The Régie de l'énergie establishes the monitoring processes used to evaluate data or information for the purpose of determining compliance or non-compliance with the Reliability Standard and with this appendix.

Violation Severity Levels

No specific provisions.

D. Regional Variances

No specific provisions.

E. Associated Documents

No specific provisions.

Attachment 1

Replace all references to "BES" with "RTP."

Attachment 2

Replace all references to "BES" with "RTP."

Attachment 3

No specific provisions.

Technical Justification

Replace all references to "BES" with "RTP."

Page 21, replace the second full paragraph with the following (changes underlined):

To propose an existing Remedial Action Scheme (a RAS implemented prior to the effective date of PRC-012-2) be designated as limited impact by the reviewing RC, the RAS-entity must prepare and submit the appropriate Attachment 1 information, including the technical justification (evaluations)

documenting that the System can meet the performance requirements (Requirement R4, Part 4.1.3) resulting from a single RAS component malfunction or failure, respectively.

Page 24, replace the last paragraph with the following (changes underlined):

Security is a component of reliability that is a measure of certainty that a device will not operate inadvertently. False or inadvertent operation of a RAS trips a programmed action without the appropriate arming conditions, occurrence of specified Contingency(ies) or System conditions expected to trigger a RAS action. Typical RAS actions include shedding load or generation or reconfiguring the System. Such actions, if inadvertently taken, are undesirable and may compromise System security. Worst-case impacts from inadvertent operation often occur if all programmed RAS actions occur. If System performance still satisfies PRC-012-2 Requirement R4, Part 4.1.4, no additional mitigation is required. Security enhancements to the RAS design, such as voting schemes, are acceptable mitigations against inadvertent operations.

Version history

Version	Date	Action	Change tracking
1	October 8, 2020	New appendix	New

A. Introduction

1. Title: Coordination of Generating Unit or Plant Capabilities, Voltage Regulating Controls, and Protection

2. Number: PRC-019-2

3. Purpose: To verify coordination of generating unit Facility or synchronous condenser voltage regulating controls, limit functions, equipment capabilities and Protection System settings.

4. Applicability:

4.1. Functional Entities

4.1.1 Generator Owner

4.1.2 Transmission Owner that owns synchronous condenser(s)

4.2. Facilities

For the purpose of this standard, the term, "applicable Facility" shall mean any one of the following:

4.2.1 Individual generating unit greater than 20 MVA (gross nameplate rating) directly connected to the Bulk Electric System.

4.2.2 Individual synchronous condenser greater than 20 MVA (gross nameplate rating) directly connected to the Bulk Electric System.

4.2.3 Generating plant/ Facility consisting of one or more units that are connected to the Bulk Electric System at a common bus with total generation greater than 75 MVA (gross aggregate nameplate rating).

4.2.3.1 This includes individual generating units of the dispersed power producing resources identified through Inclusion I4 of the Bulk Electric System definition where voltage regulating control for the facility is performed solely at the individual generating unit of the dispersed power producing resources.

4.2.4 Any generator, regardless of size, that is a blackstart unit material to and designated as part of a Transmission Operator's restoration plan.

5. Effective Date:

See the Implementation Plan for PRC-019-2.

B. Requirements

R1. At a maximum of every five calendar years, each Generator Owner and Transmission Owner with applicable Facilities shall coordinate the voltage regulating system controls, (including in-service[1] limiters and protection functions) with the applicable

[1] Limiters or protection functions that are installed and activated on the generator or synchronous condenser.

equipment capabilities and settings of the applicable Protection System devices and functions. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

1.1. Assuming the normal automatic voltage regulator control loop and steady-state system operating conditions, verify the following coordination items for each applicable Facility:

1.1.1. The in-service limiters are set to operate before the Protection System of the applicable Facility in order to avoid disconnecting the generator unnecessarily.

1.1.2. The applicable in-service Protection System devices are set to operate to isolate or de-energize equipment in order to limit the extent of damage when operating conditions exceed equipment capabilities or stability limits.

R2. Within 90 calendar days following the identification or implementation of systems, equipment or setting changes that will affect the coordination described in Requirement R1, each Generator Owner and Transmission Owner with applicable Facilities shall perform the coordination as described in Requirement R1. These possible systems, equipment or settings changes include, but are not limited to the following *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*:

- Voltage regulating settings or equipment changes;
- Protection System settings or component changes;
- Generating or synchronous condenser equipment capability changes; or
- Generator or synchronous condenser step-up transformer changes.

C. Measures

M1. Each Generator Owner and Transmission Owner with applicable Facilities will have evidence (such as examples provided in PRC-019 Section G) that it coordinated the voltage regulating system controls, including in-service[2] limiters and protection functions, with the applicable equipment capabilities and settings of the applicable Protection System devices and functions as specified in Requirement R1. This evidence should include dated documentation that demonstrates the coordination was performed.

M2. Each Generator Owner and Transmission Owner with applicable Facilities will have evidence of the coordination required by the events listed in Requirement R2. This evidence should include dated documentation that demonstrates the specified intervals in Requirement R2 have been met.

[2] Limiters or protection functions that are installed and activated on the generator or synchronous condenser.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

The Regional Entity shall serve as the Compliance enforcement authority unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention

The following evidence retention periods identify a period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention specified below is shorter than the time since the last compliance audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Generator Owner and Transmission Owner shall retain evidence of compliance with Requirements R1 and R2, Measures M1 and M2 for six years.

If a Generator Owner or Transmission Owner is found non-compliant, the entity shall keep information related to the non-compliance until mitigation is complete and approved or for the time period specified above, whichever is longer.

The Compliance Enforcement Authority shall keep the last periodic audit report and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes

Compliance Audit

Self-Certification

Spot Checking

Compliance Investigation

Self-Reporting

Complaint

1.4. Additional Compliance Information

None

2. Violation Severity Levels

R #	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	The Generator Owner or Transmission Owner coordinated equipment capabilities, limiters, and protection specified in Requirement R1 more than 5 calendar years but less than or equal to 5 calendar years plus 4 months after the previous coordination.	The Generator Owner or Transmission Owner coordinated equipment capabilities, limiters, and protection specified in Requirement R1 more than 5 calendar years plus 4 months but less than or equal to 5 calendar years plus 8 months after the previous coordination.	The Generator Owner or Transmission Owner coordinated equipment capabilities, limiters, and protection specified in Requirement R1 more than 5 calendar years plus 8 months but less than or equal to 5 calendar years plus 12 months after the previous coordination.	The Generator Owner or Transmission Owner failed to coordinate equipment capabilities, limiters, and protection specified in Requirement R1 within 5 calendar years plus 12 months after the previous coordination.
R2	The Generator Owner or Transmission Owner coordinated equipment capabilities, limiters, and protection specified in Requirement R1 more than 90 calendar days but less than or equal to 100 calendar days following the identification or implementation of a change in equipment or settings that affected the coordination.	The Generator Owner or Transmission Owner coordinated equipment capabilities, limiters, and protection specified in Requirement R1 more than 100 calendar days but less than or equal to 110 calendar days following the identification or implementation of a change in equipment or settings that affected the coordination.	The Generator Owner or Transmission Owner coordinated equipment capabilities, limiters, and protection specified in Requirement R1 more than 110 calendar days but less than or equal to 120 calendar days following the identification or implementation of a change in equipment or settings that affected the coordination.	The Generator Owner or Transmission Owner failed to coordinate equipment capabilities, limiters, and protection specified in Requirement R1 within 120 calendar days following the identification or implementation of a change in equipment or settings that affected the coordination.

E. Regional Variances

None.

F. Associated Documents

"Underexcited Operation of Turbo Generators", AIEE Proceedings T Section 881, Volume 67, 1948, Appendix 1, C. G. Adams and J. B. McClure.

,"Protective Relaying For Power Generation Systems", Boca Raton, FL, Taylor & Francis, 2006, Reimert, Donald

"Coordination of Generator Protection with Generator Excitation Control and Generator Capability", a report of Working Group J5 of the IEEE PSRC Rotating Machinery Subcommittee

"IEEE C37.102-2006 IEEE Guide for AC Generator Protection"

"IEEE C50.13-2005 IEEE Standard for Cylindrical-Rotor 50 Hz and 60 Hz Synchronous Generators Rated 10 MVA and Above"

Version History

Version	Date	Action	Change Tracking
1	February 7, 2013	Adopted by NERC Board of Trustees	New
1	March 20, 2014	FERC Order issued approving PRC-019-1. (Order becomes effective on 7/1/16.)	
2	February 12, 2015	Adopted by NERC Board of Trustees	Standard revised in Project 2014-01: Applicability revised to clarify application of requirements to BES dispersed power producing resources
2	May 29, 2015	FERC Letter Order in Docket No. RD15-3-000 approving PRC-019-2	Modifications to adjust the applicability to owners of dispersed generation resources.

G. Reference

Examples of Coordination

The evidence of coordination associated with Requirement R1 may be in the form of:

- P-Q Diagram (Example in Attachment 1), or
- R-X Diagram (Example in Attachment 2), or
- Inverse Time Diagram (Example in Attachment 3) or,
- Equivalent tables or other evidence

This evidence should include the equipment capabilities and the operating region for the limiters and protection functions

Equipment limits, types of limiters and protection functions which could be coordinated include (but are not limited to):

- Field over-excitation limiter and associated protection functions.
- Inverter over current limit and associated protection functions.
- Field under-excitation limiter and associated protection functions.
- Generator or synchronous condenser reactive capabilities.
- Volts per hertz limiter and associated protection functions.
- Stator over-voltage protection system settings.
- Generator and transformer volts per hertz capability.
- Time vs. field current or time vs. stator current.

NOTE: This listing is for reference only. This standard does not require the installation or activation of any of the above limiter or protection functions.

For this example, the Steady State Stability Limit (SSSL) is the limit to synchronous stability in the under-excited region with fixed field current.

On a P-Q diagram using X_d as the direct axis saturated synchronous reactance of the generator, X_s as the equivalent reactance between the generator terminals and the "infinite bus" including the reactance of the generator step-up transformer and V_g as the generator terminal voltage (all values in per-unit), the SSSL can be calculated as an arc with the center on the Q axis with the magnitude of the center and radius described by the following equations

$C = V^2_g/2*(1/X_s-1/X_d)$

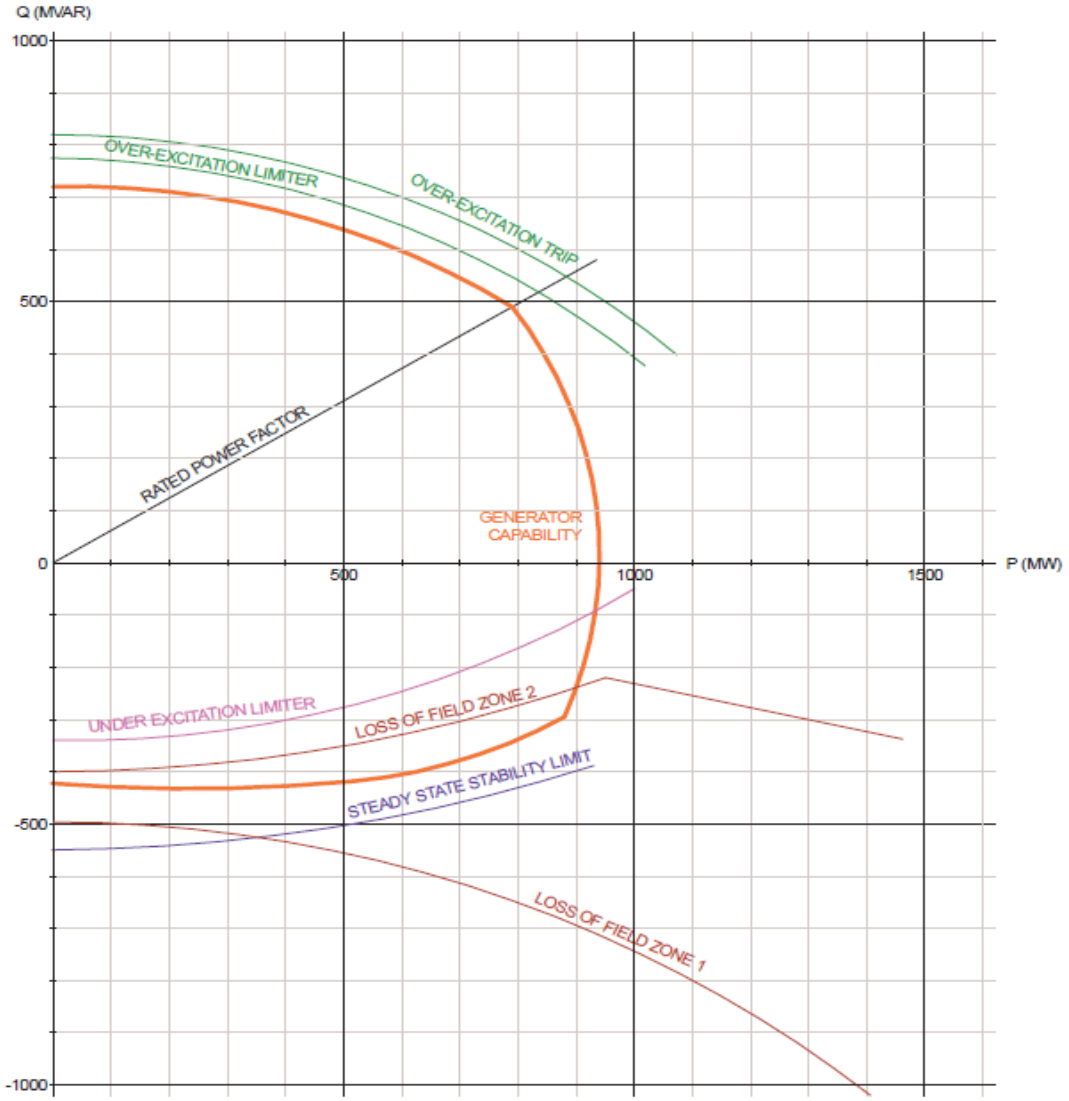
$R = V^2_g/2*(1/X_s+1/X_d)$

On an R-X diagram using X_d as the direct axis saturated synchronous reactance of the generator, and X_s as the equivalent reactance between the generator terminals and the "infinite bus" including the reactance of the generator step-up transformer the SSSL is an arc with the center on the X axis with the center and radius described by the following equations:

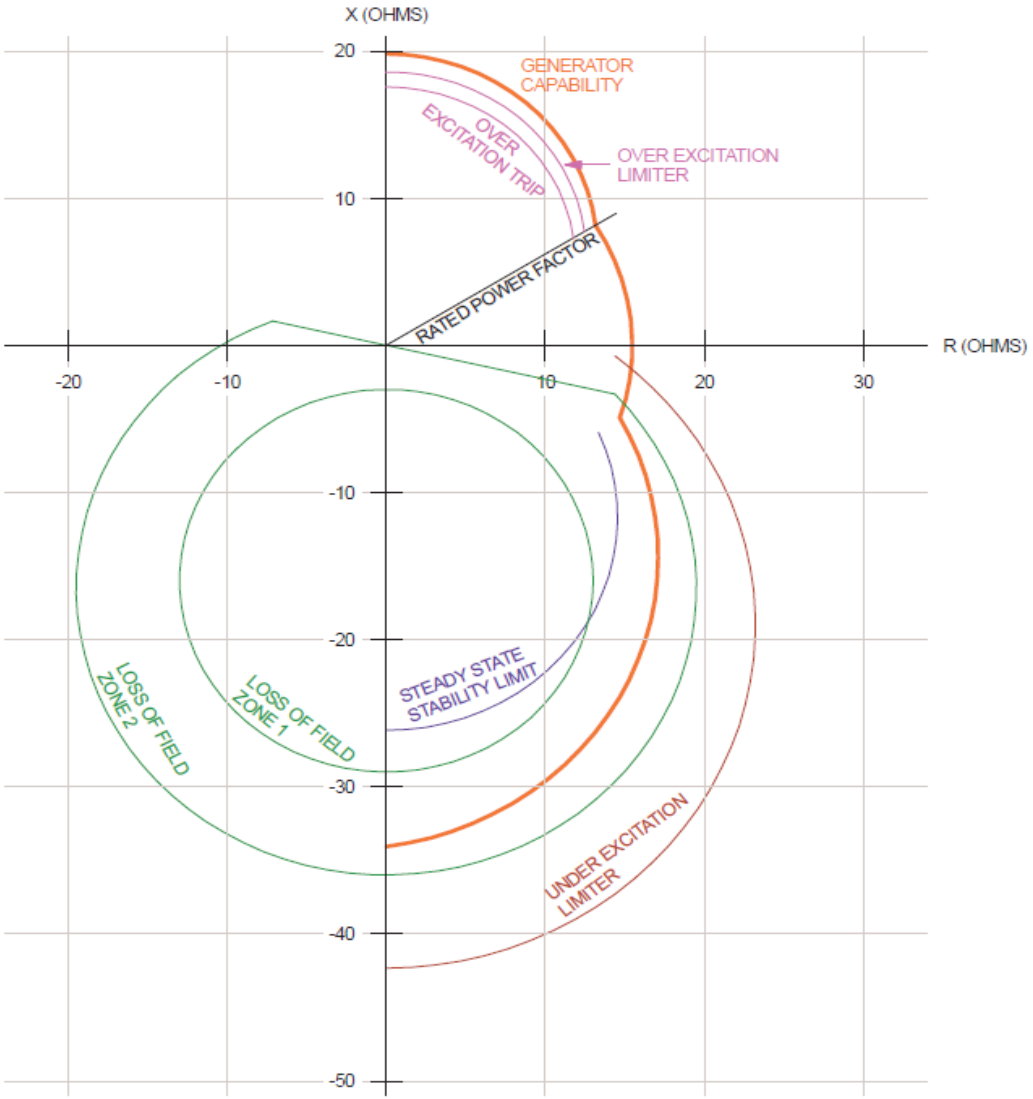
$C = (X_d-X_s)/2$

$R = (X_d+X_s)/2$

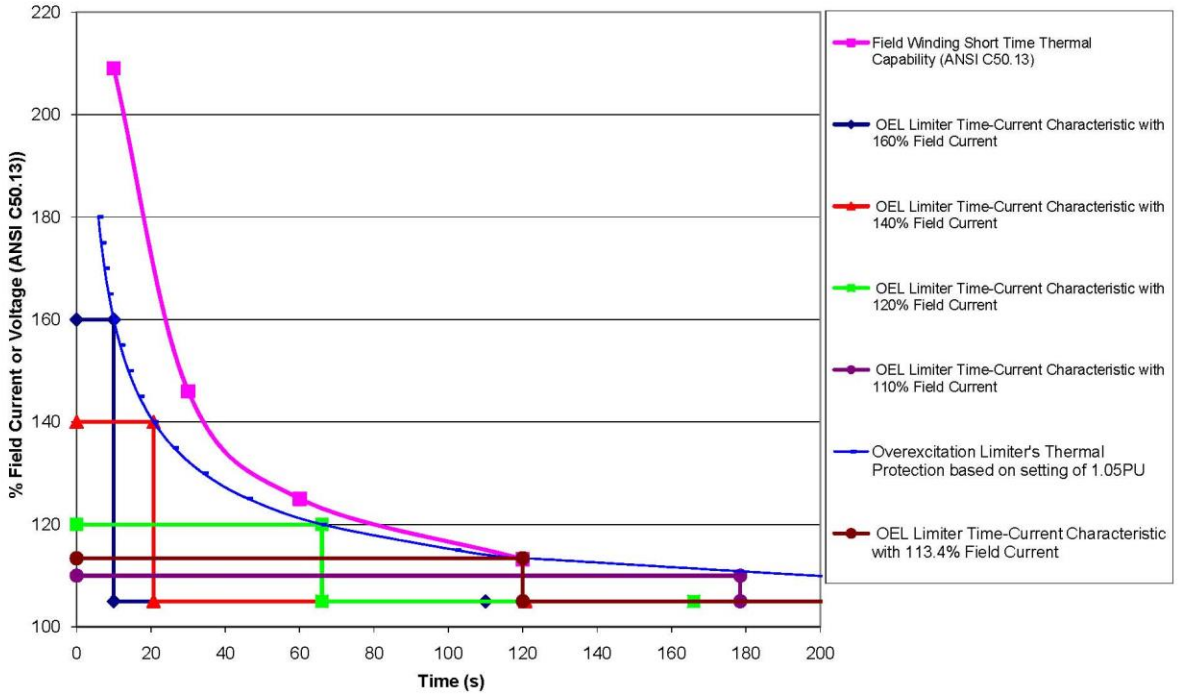
Section G Attachment 1 – Example of Capabilities, Limiters and Protection on a P-Q Diagram at nominal voltage and frequency



Section G Attachment 2 – Example of Capabilities, Limiters, and Protection on an R-X Diagram at nominal voltage and frequency



Section G Attachment 3 - Example of Capabilities, Limiters, and Protection on an Inverse Time Characteristic Plot



Rationale:

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for Facilities section 4.2.3.1

For those dispersed power producing facilities that only perform voltage regulating control at the individual generating unit level, the SDT believes that coordination should take place at the individual generating unit level of the dispersed power producing resource. These facilities need to consider the Protection Systems at the individual units and their compatibility with the reactive and voltage limitations of the units. Where voltage regulating control is done at an aggregate level, applicability is already included under Facilities section 4.2.3.

Appendix PRC-019-2-QC-1

Specific provisions applicable in Québec for standard PRC-019-2 – Coordination of Generating Unit or Plant Capabilities, Voltage Regulating Controls, and Protection

This appendix establishes specific provisions for the application of the standard in Québec. Provisions of the standard and of this appendix must be read jointly for comprehension and interpretation purposes. Where the standard and appendix differ, the appendix shall prevail.

A. Introduction

1. Title: No specific provisions.

2. Number: No specific provisions.

3. Purpose: No specific provisions.

4. Applicability:

4.1. Functional Entities

No specific provisions.

4.2. Facilities

Only the following sections are modified:

4.2.1 Generating unit that is part of the Main Transmission System (RTP).

4.2.2 Synchronous compensator that is part of the Main Transmission System (RTP).

4.2.3 Generating plant/Facility that is part of the Main Transmission System (RTP).

5. Effective date:

5.1. Adoption of the standard by the Régie de l'énergie: October 8, 2020

5.2. Adoption of this appendix by the Régie de l'énergie: October 8, 2020

Effective date of the standard and of this appendix in Québec: January 1, 2021
The implementation dates are those of PRC-019-1:

Requirements	Applicability to covered Facilities connected to the RTP	Applicability to covered Facilities not connected to the RTP	Implementation dates in Québec
R1 and R2	At least 40% of its Facilities covered	At least 15% of the Facilities covered	October 1, 2017
	At least 60% of its Facilities covered	At least 50% of the Facilities covered	October 1, 2018
	At least 80% of its Facilities covered	At least 75% of the Facilities covered	October 1, 2019
	100% of its Facilities covered	100% of the Facilities covered	January 1, 2021

B. Requirements

No specific provisions.

C. Measures

No specific provisions.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

In Québec, "Compliance Enforcement Authority" means the Régie de l'énergie in its roles of monitoring and enforcing compliance with respect to the Reliability Standard and to this appendix.

1.2. Evidence Retention

No specific provisions.

1.3. Compliance Monitoring and Assessment Processes

The Régie de l'énergie establishes the monitoring processes used to evaluate data or information for the purpose of determining compliance or non-compliance with the Reliability Standard and with this appendix.

1.4. Additional Compliance Information

No specific provisions.

2. Violation Severity Levels

No specific provisions.

E. Regional Variances

No specific provisions.

F. Associated Documents

No specific provisions.

G. Reference

No specific provisions.

Section G – Attachment 1

No specific provisions.

Section G – Attachment 2

No specific provisions.

Section G – Attachment 3

No specific provisions.

Rationale

No specific provisions.

Appendix PRC-019-2-QC-1

Specific provisions applicable in Québec for standard PRC-019-2 – Coordination of Generating Unit or Plant Capabilities, Voltage Regulating Controls, and Protection

Version history

Version	Date	Action	Change tracking
1	October 8, 2020	New appendix	New

A. Introduction

1. **Title:** **Transmission Relay Loadability**

2. **Number:** PRC-023-4

3. **Purpose:** Protective relay settings shall not limit transmission loadability; not interfere with system operators' ability to take remedial action to protect system reliability and; be set to reliably detect all fault conditions and protect the electrical network from these faults.

4. **Applicability:**

   4.1. Functional Entity:

   4.1.1 Transmission Owner with load-responsive phase protection systems as described in PRC-023-4 - Attachment A, applied at the terminals of the circuits defined in 4.2.1 *(Circuits Subject to Requirements R1 – R5)*.

   4.1.2 Generator Owner with load-responsive phase protection systems as described in PRC-023-4 - Attachment A, applied at the terminals of the circuits defined in 4.2.1 *(Circuits Subject to Requirements R1 – R5)*.

   4.1.3 Distribution Provider with load-responsive phase protection systems as described in PRC-023-4 - Attachment A, applied at the terminals of the circuits defined in 4.2.1 *(Circuits Subject to Requirements R1 – R5)*, provided those circuits have bi-directional flow capabilities.

   4.1.4 Planning Coordinator

   4.2. Circuits:

   4.2.1 Circuits Subject to Requirements R1 – R5:

   4.2.1.1 Transmission lines operated at 200 kV and above, except Elements that connect the GSU transformer(s) to the Transmission system that are used exclusively to export energy directly from a BES generating unit or generating plant. Elements may also supply generating plant loads.

   4.2.1.2 Transmission lines operated at 100 kV to 200 kV selected by the Planning Coordinator in accordance with Requirement R6.

   4.2.1.3 Transmission lines operated below 100 kV that are part of the BES and selected by the Planning Coordinator in accordance with Requirement R6.

   4.2.1.4 Transformers with low voltage terminals connected at 200 kV and above.

   4.2.1.5 Transformers with low voltage terminals connected at 100 kV to 200 kV selected by the Planning Coordinator in accordance with Requirement R6.

   4.2.1.6 Transformers with low voltage terminals connected below 100 kV that are part of the BES and selected by the Planning Coordinator in accordance with Requirement R6.

   4.2.2 Circuits Subject to Requirement R6:

   4.2.2.1 Transmission lines operated at 100 kV to 200 kV and transformers with low voltage terminals connected at 100 kV to 200 kV, except Elements that connect the GSU transformer(s) to the Transmission system that are used exclusively to export energy directly from a BES generating unit or generating plant. Elements may also supply generating plant loads.

4.2.2.2 Transmission lines operated below 100 kV and transformers with low voltage terminals connected below 100 kV that are part of the BES, except Elements that connect the GSU transformer(s) to the Transmission system that are used exclusively to export energy directly from a BES generating unit or generating plant. Elements may also supply generating plant loads.

5. Effective Dates: See Implementation Plan for the Revised Definition of "Remedial Action Scheme".

B. Requirements

R1. Each Transmission Owner, Generator Owner, and Distribution Provider shall use any one of the following criteria (Requirement R1, criteria 1 through 13) for any specific circuit terminal to prevent its phase protective relay settings from limiting transmission system loadability while maintaining reliable protection of the BES for all fault conditions. Each Transmission Owner, Generator Owner, and Distribution Provider shall evaluate relay loadability at 0.85 per unit voltage and a power factor angle of 30 degrees. *[Violation Risk Factor: High] [Time Horizon: Long Term Planning]*.

Criteria:

1. Set transmission line relays so they do not operate at or below 150% of the highest seasonal Facility Rating of a circuit, for the available defined loading duration nearest 4 hours (expressed in amperes).

2. Set transmission line relays so they do not operate at or below 115% of the highest seasonal 15-minute Facility Rating[1] of a circuit (expressed in amperes).

3. Set transmission line relays so they do not operate at or below 115% of the maximum theoretical power transfer capability (using a 90-degree angle between the sending-end and receiving-end voltages and either reactance or complex impedance) of the circuit (expressed in amperes) using one of the following to perform the power transfer calculation:

- An infinite source (zero source impedance) with a 1.00 per unit bus voltage at each end of the line.
- An impedance at each end of the line, which reflects the actual system source impedance with a 1.05 per unit voltage behind each source impedance.

4. Set transmission line relays on series compensated transmission lines so they do not operate at or below the maximum power transfer capability of the line, determined as the greater of:

- 115% of the highest emergency rating of the series capacitor.
- 115% of the maximum power transfer capability of the circuit (expressed in amperes), calculated in accordance with Requirement R1, criterion 3, using the full line inductive reactance.

5. Set transmission line relays on weak source systems so they do not operate at or below 170% of the maximum end-of-line three-phase fault magnitude (expressed in amperes).

6. Not used.

[1] When a 15-minute rating has been calculated and published for use in real-time operations, the 15-minute rating can be used to establish the loadability requirement for the protective relays.

7. Set transmission line relays applied at the load center terminal, remote from generation stations, so they do not operate at or below 115% of the maximum current flow from the load to the generation source under any system configuration.

8. Set transmission line relays applied on the bulk system-end of transmission lines that serve load remote to the system so they do not operate at or below 115% of the maximum current flow from the system to the load under any system configuration.

9. Set transmission line relays applied on the load-end of transmission lines that serve load remote to the bulk system so they do not operate at or below 115% of the maximum current flow from the load to the system under any system configuration.

10. Set transformer fault protection relays and transmission line relays on transmission lines terminated only with a transformer so that the relays do not operate at or below the greater of:

- 150% of the applicable maximum transformer nameplate rating (expressed in amperes), including the forced cooled ratings corresponding to all installed supplemental cooling equipment.
- 115% of the highest operator established emergency transformer rating.

10.1 Set load-responsive transformer fault protection relays, if used, such that the protection settings do not expose the transformer to a fault level and duration that exceeds the transformer's mechanical withstand capability[2].

11. For transformer overload protection relays that do not comply with the loadability component of Requirement R1, criterion 10 set the relays according to one of the following:

- Set the relays to allow the transformer to be operated at an overload level of at least 150% of the maximum applicable nameplate rating, or 115% of the highest operator established emergency transformer rating, whichever is greater, for at least 15 minutes to provide time for the operator to take controlled action to relieve the overload.
- Install supervision for the relays using either a top oil or simulated winding hot spot temperature element set no less than 100° C for the top oil temperature or no less than 140° C for the winding hot spot temperature[3].

12. When the desired transmission line capability is limited by the requirement to adequately protect the transmission line, set the transmission line distance relays to a maximum of 125% of the apparent impedance (at the impedance angle of the transmission line) subject to the following constraints:

a. Set the maximum torque angle (MTA) to 90 degrees or the highest supported by the manufacturer.

b. Evaluate the relay loadability in amperes at the relay trip point at 0.85 per unit voltage and a power factor angle of 30 degrees.

c. Include a relay setting component of 87% of the current calculated in Requirement R1, criterion 12 in the Facility Rating determination for the circuit.

---

[2] As illustrated by the "dotted line" in IEEE C57.109-1993 - *IEEE Guide for Liquid-Immersed Transformer Through-Fault-Current Duration,* Clause 4.4, Figure 4.

[3] IEEE standard C57.91, Tables 7 and 8, specify that transformers are to be designed to withstand a winding hot spot temperature of 180 degrees C, and Annex A cautions that bubble formation may occur above 140 degrees C.

13. Where other situations present practical limitations on circuit capability, set the phase protection relays so they do not operate at or below 115% of such limitations.

R2. Each Transmission Owner, Generator Owner, and Distribution Provider shall set its out-of-step blocking elements to allow tripping of phase protective relays for faults that occur during the loading conditions used to verify transmission line relay loadability per Requirement R1. *[Violation Risk Factor: High] [Time Horizon: Long Term Planning]*

R3. Each Transmission Owner, Generator Owner, and Distribution Provider that uses a circuit capability with the practical limitations described in Requirement R1, criterion 7, 8, 9, 12, or 13 shall use the calculated circuit capability as the Facility Rating of the circuit and shall obtain the agreement of the Planning Coordinator, Transmission Operator, and Reliability Coordinator with the calculated circuit capability. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning]*

R4. Each Transmission Owner, Generator Owner, and Distribution Provider that chooses to use Requirement R1 criterion 2 as the basis for verifying transmission line relay loadability shall provide its Planning Coordinator, Transmission Operator, and Reliability Coordinator with an updated list of circuits associated with those transmission line relays at least once each calendar year, with no more than 15 months between reports. *[Violation Risk Factor: Lower] [Time Horizon: Long Term Planning]*

R5. Each Transmission Owner, Generator Owner, and Distribution Provider that sets transmission line relays according to Requirement R1 criterion 12 shall provide an updated list of the circuits associated with those relays to its Regional Entity at least once each calendar year, with no more than 15 months between reports, to allow the ERO to compile a list of all circuits that have protective relay settings that limit circuit capability. *[Violation Risk Factor: Lower] [Time Horizon: Long Term Planning]*

R6. Each Planning Coordinator shall conduct an assessment at least once each calendar year, with no more than 15 months between assessments, by applying the criteria in PRC-023-4, Attachment B to determine the circuits in its Planning Coordinator area for which Transmission Owners, Generator Owners, and Distribution Providers must comply with Requirements R1 through R5. The Planning Coordinator shall: *[Violation Risk Factor: High] [Time Horizon: Long Term Planning]*

6.1 Maintain a list of circuits subject to PRC-023-4 per application of Attachment B, including identification of the first calendar year in which any criterion in PRC-023-4, Attachment B applies.

6.2 Provide the list of circuits to all Regional Entities, Reliability Coordinators, Transmission Owners, Generator Owners, and Distribution Providers within its Planning Coordinator area within 30 calendar days of the establishment of the initial list and within 30 calendar days of any changes to that list.

C. Measures

M1. Each Transmission Owner, Generator Owner, and Distribution Provider shall have evidence such as spreadsheets or summaries of calculations to show that each of its transmission relays is set according to one of the criteria in Requirement R1, criterion 1 through 13 and shall have evidence such as coordination curves or summaries of calculations that show that relays set per criterion 10 do not expose the transformer to fault levels and durations beyond those indicated in the standard. (R1)

M2. Each Transmission Owner, Generator Owner, and Distribution Provider shall have evidence such as spreadsheets or summaries of calculations to show that each of its out-of-step blocking elements is set to allow tripping of phase protective relays for faults that occur during the loading conditions used to verify transmission line relay loadability per Requirement R1. (R2)

M3. Each Transmission Owner, Generator Owner, and Distribution Provider with transmission relays set according to Requirement R1, criterion 7, 8, 9, 12, or 13 shall have evidence such as Facility Rating spreadsheets or Facility Rating database to show that it used the calculated circuit capability as the Facility Rating of the circuit and evidence such as dated correspondence that the resulting Facility Rating was agreed to by its associated Planning Coordinator, Transmission Operator, and Reliability Coordinator. (R3)

M4. Each Transmission Owner, Generator Owner, or Distribution Provider that sets transmission line relays according to Requirement R1, criterion 2 shall have evidence such as dated correspondence to show that it provided its Planning Coordinator, Transmission Operator, and Reliability Coordinator with an updated list of circuits associated with those transmission line relays within the required timeframe. The updated list may either be a full list, a list of incremental changes to the previous list, or a statement that there are no changes to the previous list. (R4)

M5. Each Transmission Owner, Generator Owner, or Distribution Provider that sets transmission line relays according to Requirement R1, criterion 12 shall have evidence such as dated correspondence that it provided an updated list of the circuits associated with those relays to its Regional Entity within the required timeframe. The updated list may either be a full list, a list of incremental changes to the previous list, or a statement that there are no changes to the previous list. (R5)

M6. Each Planning Coordinator shall have evidence such as power flow results, calculation summaries, or study reports that it used the criteria established within PRC-023-4, Attachment B to determine the circuits in its Planning Coordinator area for which applicable entities must comply with the standard as described in Requirement R6. The Planning Coordinator shall have a dated list of such circuits and shall have evidence such as dated correspondence that it provided the list to the Regional Entities, Reliability Coordinators, Transmission Owners, Generator Owners, and Distribution Providers within its Planning Coordinator area within the required timeframe. (R6)

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

As defined in the NERC Rules of Procedure, “Compliance Enforcement Authority” means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Data Retention

The Transmission Owner, Generator Owner, Distribution Provider and Planning Coordinator shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation:

The Transmission Owner, Generator Owner, and Distribution Provider shall each retain documentation to demonstrate compliance with Requirements R1 through R5 for three calendar years.

The Planning Coordinator shall retain documentation of the most recent review process required in Requirement R6. The Planning Coordinator shall retain the most recent list of circuits in its Planning Coordinator area for which applicable entities must comply with the standard, as determined per Requirement R6.

If a Transmission Owner, Generator Owner, Distribution Provider, or Planning Coordinator is found non-compliant, it shall keep information related to the non-compliance until found compliant or for the time specified above, whichever is longer.

The Compliance Enforcement Authority shall keep the last audit record and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Violation Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information

None.

2. Violation Severity Levels:

Requirement	Lower	Moderate	High	Severe
R1	N/A	N/A	N/A	The responsible entity did not use any one of the following criteria (Requirement R1 criterion 1 through 13) for any specific circuit terminal to prevent its phase protective relay settings from limiting transmission system loadability while maintaining reliable protection of the BES for all fault conditions. OR The responsible entity did not evaluate relay loadability at 0.85 per unit voltage and a power factor angle of 30 degrees.
R2	N/A	N/A	N/A	The responsible entity failed to ensure that its out-of-step blocking elements allowed tripping of phase protective relays for faults that occur during the loading conditions used to verify transmission line relay loadability per Requirement R1.
R3	N/A	N/A	N/A	The responsible entity that uses a circuit capability with the practical limitations described in Requirement R1 criterion 7, 8, 9, 12, or 13 did not use the calculated circuit capability as the Facility Rating of the circuit.

Requirement	Lower	Moderate	High	Severe
				OR The responsible entity did not obtain the agreement of the Planning Coordinator, Transmission Operator, and Reliability Coordinator with the calculated circuit capability.
R4	N/A	N/A	N/A	The responsible entity did not provide its Planning Coordinator, Transmission Operator, and Reliability Coordinator with an updated list of circuits that have transmission line relays set according to the criteria established in Requirement R1 criterion 2 at least once each calendar year, with no more than 15 months between reports.
R5	N/A	N/A	N/A	The responsible entity did not provide its Regional Entity, with an updated list of circuits that have transmission line relays set according to the criteria established in Requirement R1 criterion 12 at least once each calendar year, with no more than 15 months between reports.
R6	N/A	The Planning Coordinator used the criteria established within Attachment B to determine the circuits in its Planning Coordinator area for which applicable entities must comply with the standard and met parts 6.1 and 6.2, but more	The Planning Coordinator used the criteria established within Attachment B to determine the circuits in its Planning Coordinator area for which applicable entities must comply with the standard and met parts 6.1 and 6.2, but 24	The Planning Coordinator failed to use the criteria established within Attachment B to determine the circuits in its Planning Coordinator area for which applicable entities must comply with the standard.

Requirement	Lower	Moderate	High	Severe
		than 15 months and less than 24 months lapsed between assessments. OR The Planning Coordinator used the criteria established within Attachment B at least once each calendar year, with no more than 15 months between assessments to determine the circuits in its Planning Coordinator area for which applicable entities must comply with the standard and met 6.1 and 6.2 but failed to include the calendar year in which any criterion in Attachment B first applies. OR The Planning Coordinator used the criteria established within Attachment B at least once each calendar year, with no more than 15 months between assessments to determine the circuits in its Planning Coordinator area for which applicable entities must comply with the standard and met 6.1 and 6.2 but provided the list of circuits to the Reliability Coordinators, Transmission Owners, Generator Owners, and Distribution Providers within its Planning Coordinator area between 31 days and 45 days after	months or more lapsed between assessments. OR The Planning Coordinator used the criteria established within Attachment B at least once each calendar year, with no more than 15 months between assessments to determine the circuits in its Planning Coordinator area for which applicable entities must comply with the standard and met 6.1 and 6.2 but provided the list of circuits to the Reliability Coordinators, Transmission Owners, Generator Owners, and Distribution Providers within its Planning Coordinator area between 46 days and 60 days after list was established or updated. (part 6.2)	OR The Planning Coordinator used the criteria established within Attachment B, at least once each calendar year, with no more than 15 months between assessments to determine the circuits in its Planning Coordinator area for which applicable entities must comply with the standard but failed to meet parts 6.1 and 6.2. OR The Planning Coordinator used the criteria established within Attachment B at least once each calendar year, with no more than 15 months between assessments to determine the circuits in its Planning Coordinator area for which applicable entities must comply with the standard but failed to maintain the list of circuits determined according to the process described in Requirement R6. (part 6.1) OR The Planning Coordinator used the criteria established within Attachment B at least once each calendar year, with no more than 15 months between assessments to determine the circuits in its Planning Coordinator area for which applicable entities must comply with the standard and met

Requirement	Lower	Moderate	High	Severe
		the list was established or updated. (part 6.2)		6.1 but failed to provide the list of circuits to the Reliability Coordinators, Transmission Owners, Generator Owners, and Distribution Providers within its Planning Coordinator area or provided the list more than 60 days after the list was established or updated. (part 6.2) OR The Planning Coordinator failed to determine the circuits in its Planning Coordinator area for which applicable entities must comply with the standard.

E. Regional Differences

None.

F. Supplemental Technical Reference Document

1. The following document is an explanatory supplement to the standard. It provides the technical rationale underlying the requirements in this standard. The reference document contains methodology examples for illustration purposes it does not preclude other technically comparable methodologies.

"Determination and Application of Practical Relaying Loadability Ratings," Version 1.0, June 2008, prepared by the System Protection and Control Task Force of the NERC Planning Committee, available at:
http://www.nerc.com/fileUploads/File/Standards/Relay_Loadability_Reference_Doc_Clean_Final_2008July3.pdf

Version History

Version	Date	Action	Change Tracking
1	February 12, 2008	Approved by Board of Trustees	New
1	March 19, 2008	Corrected typo in last sentence of Severe VSL for Requirement 3 — "then" should be "than."	Errata
1	March 18, 2010	Approved by FERC	
1	Filed for approval April 19, 2010	Changed VRF for R3 from Medium to High; changed VSLs for R1, R2, R3 to binary Severe to comply with Order 733	Revision
2	March 10, 2011 approved by Board of Trustees	Revised to address initial set of directives from Order 733	Revision (Project 2010-13)
2	March 15, 2012	FERC order issued approving PRC-023-2 (approval becomes effective May 7, 2012)	
3	November 7, 2013	Adopted by NERC Board of Trustees	Supplemental SAR to Clarify applicability for consistency with PRC-025-1 and other minor corrections.

Version	Date	Action	Change Tracking
4	November 13, 2014	Adopted by the NERC Board of Trustees	Replaced references to Special Protection System and SPS with Remedial Action Scheme and RAS
4	November 19, 2015	FERC Order issued approving PRC-023-4. Docket No. RM15-13-000.	

PRC-023-4 — Attachment A

1. This standard includes any protective functions which could trip with or without time delay, on load current, including but not limited to:

1.1. Phase distance.

1.2. Out-of-step tripping.

1.3. Switch-on-to-fault.

1.4. Overcurrent relays.

1.5. Communications aided protection schemes including but not limited to:

1.5.1 Permissive overreach transfer trip (POTT).

1.5.2 Permissive under-reach transfer trip (PUTT).

1.5.3 Directional comparison blocking (DCB).

1.5.4 Directional comparison unblocking (DCUB).

1.6. Phase overcurrent supervisory elements (i.e., phase fault detectors) associated with current-based, communication-assisted schemes (i.e., pilot wire, phase comparison, and line current differential) where the scheme is capable of tripping for loss of communications.

2. The following protection systems are excluded from requirements of this standard:

2.1. Relay elements that are only enabled when other relays or associated systems fail. For example:

- Overcurrent elements that are only enabled during loss of potential conditions.
- Elements that are only enabled during a loss of communications except as noted in section 1.6.

2.2. Protection systems intended for the detection of ground fault conditions.

2.3. Protection systems intended for protection during stable power swings.

2.4. Not used.

2.5. Relay elements used only for Remedial Action Schemes applied and approved in accordance with NERC Reliability Standards PRC-012 through PRC-017 or their successors.

2.6. Protection systems that are designed only to respond in time periods which allow 15 minutes or greater to respond to overload conditions.

2.7. Thermal emulation relays which are used in conjunction with dynamic Facility Ratings.

2.8. Relay elements associated with dc lines.

2.9. Relay elements associated with dc converter transformers.

PRC-023-4 — Attachment B

Circuits to Evaluate

- Transmission lines operated at 100 kV to 200 kV and transformers with low voltage terminals connected at 100 kV to 200 kV.
- Transmission lines operated below 100 kV and transformers with low voltage terminals connected below 100 kV that are part of the Bulk Electric System.

Criteria

If any of the following criteria apply to a circuit, the applicable entity must comply with the standard for that circuit.

B1. The circuit is a monitored Facility of a permanent flowgate in the Eastern Interconnection, a major transfer path within the Western Interconnection as defined by the Regional Entity, or a comparable monitored Facility in the Québec Interconnection, that has been included to address reliability concerns for loading of that circuit, as confirmed by the applicable Planning Coordinator.

B2. The circuit is a monitored Facility of an Interconnection Reliability Operating Limit (IROL), where the IROL was determined in the planning horizon pursuant to FAC-010.

B3. The circuit forms a path (as agreed to by the Generator Operator and the transmission entity) to supply off-site power to a nuclear plant as established in the Nuclear Plant Interface Requirements (NPIRs) pursuant to NUC-001.

B4. The circuit is identified through the following sequence of power flow analyses[4] performed by the Planning Coordinator for the one-to-five-year planning horizon:

a. Simulate double contingency combinations selected by engineering judgment, without manual system adjustments in between the two contingencies (reflects a situation where a System Operator may not have time between the two contingencies to make appropriate system adjustments).

b. For circuits operated between 100 kV and 200 kV evaluate the post-contingency loading, in consultation with the Facility owner, against a threshold based on the Facility Rating assigned for that circuit and used in the power flow case by the Planning Coordinator.

c. When more than one Facility Rating for that circuit is available in the power flow case, the threshold for selection will be based on the Facility Rating for the loading duration nearest four hours.

d. The threshold for selection of the circuit will vary based on the loading duration assumed in the development of the Facility Rating.

[4] Past analyses may be used to support the assessment if no material changes to the system have occurred since the last assessment

i. If the Facility Rating is based on a loading duration of up to and including four hours, the circuit must comply with the standard if the loading exceeds 115% of the Facility Rating.

ii. If the Facility Rating is based on a loading duration greater than four and up to and including eight hours, the circuit must comply with the standard if the loading exceeds 120% of the Facility Rating.

iii. If the Facility Rating is based on a loading duration of greater than eight hours, the circuit must comply with the standard if the loading exceeds 130% of the Facility Rating.

e. Radially operated circuits serving only load are excluded.

B5. The circuit is selected by the Planning Coordinator based on technical studies or assessments, other than those specified in criteria B1 through B4, in consultation with the Facility owner.

B6. The circuit is mutually agreed upon for inclusion by the Planning Coordinator and the Facility owner.

Appendix PRC-023-4-QC-1

Specific provisions applicable in Québec for standard PRC-023-4 – Transmission Relay Loadability

This appendix establishes specific provisions for the application of the standard in Québec. Provisions of the standard and of this appendix must be read jointly for comprehension and interpretation purposes. Where the standard and appendix differ, the appendix shall prevail.

A. Introduction

1. Title: No specific provisions.

2. Number: No specific provisions.

3. Purpose: No specific provisions.

4. Applicability:

4.1. Functional Entity

No specific provisions.

4.2. Circuits:

4.2.1 Circuits Subject to Requirements R1 to R5

4.2.1.1 Transmission lines operated at 200 kV and above that are part of the Main Transmission System (RTP), except Elements that connect the GSU transformers to the Transmission system that are used exclusively to export energy directly from a generating unit or generating plant of the RTP. Elements may also supply generating plant loads.

4.2.1.2 Transmission lines operated at 100 kV to 200 kV that are part of the RTP and selected by the Planning Coordinator in accordance with Requirement R6.

4.2.1.3 Transmission lines operated below 100 kV that are part of the RTP and selected by the Planning Coordinator in accordance with Requirement R6.

4.2.1.4 Transformers with low voltage terminals connected at 200 kV and above that are part of the RTP.

4.2.1.5 Transformers with low voltage terminals connected at 100 kV to 200 kV that are part of the RTP and selected by the Planning Coordinator in accordance with Requirement R6.

4.2.1.6 Transformers with low voltage terminals connected below 100 kV that are part of the RTP and selected by the Planning Coordinator in accordance with Requirement R6.

4.2.2 Circuits Subject to Requirement R6

4.2.2.1 Transmission lines operated at 100 kV to 200 kV that are part of the RTP and transformers with low voltage terminals connected at 100 kV to 200 kV that are part of the RTP, except Elements that connect the GSU transformers to the Transmission system that are used exclusively to export energy directly from an RTP generating unit or generating plant. Elements may also supply generating plant loads.

4.2.2.2 Transmission lines operated below 100 kV and transformers with low voltage terminals connected below 100 kV that are part of the RTP, except Elements that connect the GSU transformers to the Transmission system that are used exclusively to export energy directly from an RTP generating unit or generating plant. Elements may also supply generating plant loads.

5. Effective date:

5.1. Adoption of the standard by the Régie de l'énergie: October 8, 2020

5.2. Adoption of this appendix by the Régie de l'énergie: October 8, 2020

Effective date of the standard and of this appendix in Québec: January 1, 2021
The implementation dates are those of PRC-023-3:

Requirements	Applicability	Date of implementation in Québec
R1	Each TO, GO or DP with transmission lines operated at 200 kV and above and transformers with low voltage terminals connected at 200 kV and above, with the exception of the following:	January 1st, 2018
	• For Requirement R1, Criterion 10.1	April 1st, 2018
	• For the supervisory elements described in PRC-023-4 – Attachment A, Section 1.6	October 1st, 2018
	• For the trip-on-fault devices described in PRC-023-4 – Attachment A, Section 1.3	October 1st, 2019
	Each TO, GO or DP with circuits identified by the Planning Coordinator in accordance with Requirement R6	The later of the following dates: First day of the first calendar quarter 39 months following notification by the Planning Coordinator of a circuit's inclusion on a list of circuits subject to

Appendix PRC-023-4-QC-1

Specific provisions applicable in Québec for standard PRC-023-4 – Transmission Relay Loadability

Requirements	Applicability	Date of implementation in Québec
		PRC-023-4, per the provisions of Attachment B OR First day of the first calendar year during which a criterion from Attachment B applies, unless the Planning Coordinator removes the circuit from the list of circuits selected prior to the applicable effective date.
R2 and R3	Each TO, GO or DP with transmission lines operated at 200 kV and above and transformers with low voltage terminals connected at 200 kV or above	January 1st, 2018
	Each TO, GO or DP with circuits selected by the Planning Coordinator in accordance with Requirement R6	The later of the following dates: First day of the first calendar quarter 39 months following notification by the Planning Coordinator of a circuit's inclusion on a list of circuits subject to PRC-023-4, per the provisions of Attachment B OR First day of the first calendar year during which a criterion from Attachment B applies, unless the Planning Coordinator removes the circuit from the list of circuits selected prior to the applicable effective date.
R4	Each TO, GO or DP that chooses criterion 2 of Requirement R1 as the basis for verifying transmission line relay loadability	April 1st, 2018
R5	Each TO, GO or DP that sets transmission line relays in accordance with Requirement R1 criterion 12	April 1st, 2018
R6	Each Planning Coordinator who must conduct an assessment by using Attachment B criteria to identify the circuits	July 1st, 2018

Requirements	Applicability	Date of implementation in Québec
	in its Planning Coordinator Area that require Transmission Owners, Generator Owners and Distribution Providers to comply with Requirements R1 through R5	

B. Requirements

Specific provision applicable to Requirement R1:

R1. Each Transmission Owner, Generator Owner and Distribution Provider shall use one of the following criteria (Requirement R1, criteria 1 through 13) for any specific circuit terminal to prevent the phase protective relay settings from limiting transmission system loadability while maintaining reliable protection of the RTP for all fault conditions. Each Transmission Owner, Generator Owner and Distribution Provider shall evaluate relay loadability at 0.85 per unit voltage and a power factor angle of 30 degrees. *[Violation Risk Factor: High] [Time Horizon: Long Term Planning].*

Specific provision applicable to criteria 10 and 11

10**.** Set transformer fault protection relays and transmission line relays on transmission lines terminated only with a transformer so that the relays do not operate at or below the greater of:

- No specific provisions.
- One of the following applicable values:
  - 115% of the highest operator established emergency transformer rating, if the operator has established one, or
  - 100% of the highest long duration emergency rating established by the Transformer Owner, if the Transformer Owner has established one and the operator has not established a highest transformer emergency rating.

10.1 No specific provisions.

11. For transformer overload protection relays that do not comply with the loadability component of Requirement R1 criterion 10, set the relays according to one of the following:
    - Set the relays to allow the transformer to be operated at an overload level as defined in criterion 10 for at least 15 minutes to provide time for the operator to take controlled action to relieve the overload.
    - No specific provisions.

C. Measures

No specific provisions.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

In Québec, "Compliance Enforcement Authority" means the Régie de l'énergie in its roles of monitoring and enforcing compliance with respect to the Reliability Standard and to this appendix.

1.2. Data Retention

No specific provisions.

1.3. Compliance Monitoring and Assessment Processes

The Régie de l'énergie establishes the monitoring processes used to evaluate data or information for the purpose of determining compliance or non-compliance with the Reliability Standard and with this appendix.

1.4. Additional Compliance Information

No specific provisions.

2. Violation Severity Levels

Specific provision applicable to Requirement R1:

	Low	Moderate	High	Severe
R1	Not applicable	Not applicable	Not applicable	The responsible entity did not use any of the following criteria (Requirement R1 criteria 1 through 13) for any specific circuit terminal to prevent the phase protective relay settings from limiting transmission system loadability while maintaining reliable protection of the RTP for all fault conditions. OR The responsible entity did not evaluate relay loadability at 0.85 per unit voltage and a power factor angle of 30 degrees.

E. Regional Differences

No specific provisions.

F. Supplemental Technical Reference Document

No specific provisions.

PRC-023-4 – Attachment A

No specific provisions.

PRC-023-4 – Attachment B

Circuits to Evaluate

- Transmission lines operated at 100 kV to 200 kV and transformers with low voltage terminals connected at 100 kV to 200 kV that are part of the RTP.
- Transmission lines operated below 100 kV and transformers with low voltage terminals connected below 100 kV that are part of the RTP.

Criteria

No specific provisions.

Version history

Version	Date	Action	Change tracking
1	October 8, 2020	New appendix	New

A. Introduction

1. **Title:** **Frequency and Voltage Protection Settings** for Generating Resources

2. **Number:** PRC-024-3

3. **Purpose:** To set protection such that generating resource(s) remain connected during defined frequency and voltage excursions in support of the Bulk Electric System (BES).

4. **Applicability:**

   4.1. Functional Entities:

   4.1.1 Generator Owners that apply protection listed in Section 4.2.1.

   4.1.2 Transmission Owners (in the Quebec Interconnection only) that own a BES generator step-up (GSU) transformer or main power transformer (MPT)[1] and apply protection listed in Section 4.2.1.

   4.1.3 Planning Coordinators (in the Quebec Interconnection only)

   4.2. Facilities[2]:

   4.2.1 Frequency, voltage, and volts per hertz protection (whether provided by relaying or functions within associated control systems) that respond to electrical signals and: (i) directly trip the generating resource(s); or (ii) provide signals to the generating resource(s) to either trip or cease injecting current; and are applied to the following:

   4.2.1.1 BES generating resource(s).

   4.2.1.2 BES GSU transformer(s).

   4.2.1.3 High side of the generator-connected unit auxiliary transformer[3] (UAT) installed on BES generating resource(s).

   4.2.1.4 Individual dispersed power producing resource(s) identified in the BES Definition, Inclusion I4.

   4.2.1.5 Elements that are designed primarily for the delivery of capacity from the individual dispersed power producing resources identified in the BES Definition, Inclusion I4, to the point where those resources aggregate to greater than 75 MVA.

[1] For the purpose of this standard, the MPT is the power transformer that steps up voltage from the collection system voltage to the nominal transmission/interconnecting system voltage for dispersed power producing resources.

[2] It is not required to install or activate the protections described in Facilities Section 4.2.

[3] These transformers are variably referred to as station power UAT, or station service transformer(s) used to provide overall auxiliary power to the generating resource(s). This UAT is the transformer connected on the generator bus between the low side of the GSU and the generator terminal.

4.2.1.6 MPT[4] of resource(s) identified in the BES Definition, Inclusion I4.

4.2.2 Exemptions: Protection on all auxiliary equipment within the generating Facility.

5. Effective Date: See the Implementation Plan for PRC-024-3.

[4] For the purpose of this standard, the MPT is the power transformer that steps up voltage from the collection system voltage to the nominal transmission/interconnecting system voltage for dispersed power producing resources

B. Requirements and Measures

R1. Each Generator Owner shall set its applicable frequency protection[5] in accordance with PRC-024 Attachment 1 such that the applicable protection does not cause the generating resource to trip or cease injecting current within the "no trip zone" during a frequency excursion with the following exceptions: *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

- Applicable frequency protection may be set to trip or cease injecting current within a portion of the "no trip zone" for documented and communicated regulatory or equipment limitations in accordance with Requirement R3.

M1. Each Generator Owner shall have evidence that the applicable frequency protection has been set in accordance with Requirement R1, such as dated setting sheets, calibration sheets, calculations, or other documentation.

R2. Each Generator Owner shall set its applicable voltage protection[5] in accordance with PRC-024 Attachment 2, such that the applicable protection does not cause the generating resource to trip or cease injecting current within the "no trip zone" during a voltage excursion at the high side of the GSU or MPT, subject to the following exceptions: *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

- If the Transmission Planner allows less stringent voltage protection settings than those required to meet PRC-024 Attachment 2, then the Generator Owner may set its protection within the voltage recovery characteristics of a location-specific Transmission Planner's study.
- Applicable voltage protection may be set to trip or cease injecting current during a voltage excursion within a portion of the "no trip zone" for documented and communicated regulatory or equipment limitations in accordance with Requirement R3.

M2. Each Generator Owner shall have evidence that applicable voltage protection has been set in accordance with Requirement R2, such as dated setting sheets, voltage-time boundaries, calibration sheets, coordination plots, dynamic simulation studies, calculations, or other documentation.

[5] Frequency, voltage, and volts per hertz protection (whether provided by relaying or functions within associated control systems) that respond to electrical signals and: (i) directly trip the generating resource(s); or (ii) provide signals to the generating resource(s) to either trip or cease injecting current.

R3. Each Generator Owner shall document each known regulatory or equipment limitation[6] that prevents an applicable generating resource(s) with frequency or voltage protection from meeting the protection setting criteria in Requirements R1 or R2, including (but not limited to) study results, experience from an actual event, or manufacturer's advice. *[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*

3.1. The Generator Owner shall communicate the documented regulatory or equipment limitation, or the removal of a previously documented regulatory or equipment limitation, to its Planning Coordinator and Transmission Planner within 30 calendar days of any of the following:

- Identification of a regulatory or equipment limitation.
- Repair of the equipment causing the limitation that removes the limitation.
- Replacement of the equipment causing the limitation with equipment that removes the limitation.
- Creation or adjustment of an equipment limitation caused by consumption of the cumulative turbine life-time frequency excursion allowance.

M3. Each Generator Owner shall have evidence that it has documented and communicated any known regulatory or equipment limitations that resulted in an exception to Requirements R1 or R2 in accordance with Requirement R3, such as a dated email or letter that contains such documentation as study results, experience from an actual event, or manufacturer's advice.

R4. Each Generator Owner shall provide its applicable protection settings associated with Requirements R1 and R2 to the Planning Coordinator or Transmission Planner that models the associated generating resource(s) within 60 calendar days of receipt of a written request for the data and within 60 calendar days of any change to those previously requested settings unless directed by the requesting Planning Coordinator or Transmission Planner that the reporting of protection setting changes is not required. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M4. Each Generator Owner shall have evidence that it communicated applicable protection settings in accordance with Requirement R4, such as dated e-mails, correspondence or other evidence and copies of any requests it has received for that information.

[6] Excludes limitations caused by the setting capability of the frequency, voltage, and volts per hertz protective relays for the generating resource(s). This does not exclude limitations originating in the equipment protected by the relay. This also does not exclude limitations of frequency, voltage, and volts per hertz protection embedded in control systems.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: "Compliance Enforcement Authority" means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

- The Generator Owner shall keep data or evidence Requirement R1 through R4; for 3 years or until the next audit, whichever is longer.
- If a Generator Owner is found non-compliant, the Generator Owner or Transmission Owner shall keep information related to the non-compliance until mitigation is complete and approved for the time period specified above, whichever is longer.

1.3. Compliance Monitoring and Assessment Program: As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	N/A	N/A	N/A	The Generator Owner failed to set its applicable frequency protection so that it does not trip or cease injecting current according to Requirement R1.
R2.	N/A	N/A	N/A	The Generator Owner failed to set its applicable voltage protection so that it does not trip or cease injecting current according to Requirement R2.
R3.	The Generator Owner documented the known non-protection system equipment limitation that prevented it from meeting the criteria in Requirement R1 or R2 and communicated the documented limitation to its Planning Coordinator and Transmission Planner more than 30 calendar days but less than or equal to 60 calendar	The Generator Owner documented the known non-protection system equipment limitation that prevented it from meeting the criteria in Requirement R1 or R2 and communicated the documented limitation to its Planning Coordinator and Transmission Planner more than 60 calendar days but less than or equal	The Generator Owner documented the known non-protection system equipment limitation that prevented it from meeting the criteria in Requirement R1 or R2 and communicated the documented limitation to its Planning Coordinator and Transmission Planner more than 90 calendar	The Generator Owner failed to document any known non-protection system equipment limitation that prevented it from meeting the criteria in Requirement R1 or R2. OR The Generator Owner failed to communicate the

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	days of identifying the limitation.	to 90 calendar days of identifying the limitation.	days but less than or equal to 120 calendar days of identifying the limitation.	documented limitation to its Planning Coordinator and Transmission Planner within 120 calendar days of identifying the limitation.
R4.	The Generator Owner provided its protection settings more than 60 calendar days but less than or equal to 90 calendar days of any change to those settings. OR The Generator Owner provided protection settings more than 60 calendar days but less than or equal to 90 calendar days of a written request.	The Generator Owner provided its protection settings more than 90 calendar days but less than or equal to 120 calendar days of any change to those settings. OR The Generator Owner provided protection settings more than 90 calendar days but less than or equal to 120 calendar days of a written request.	The Generator Owner provided its protection settings more than 120 calendar days but less than or equal to 150 calendar days of any change to those settings. OR The Generator Owner provided protection settings more than 120 calendar days but less than or equal to 150 calendar days of a written request.	The Generator Owner failed to provide its protection settings within 150 calendar days of any change to those settings. OR The Generator Owner failed to provide protection settings within 150 calendar days of a written request.

D. Regional Variances

D.A. Variance for the Quebec Interconnection

This Variance extends the applicability of Requirements R1, R3, and R4 to Transmission Owners in the Quebec Interconnection that own a BES GSU or MPT and apply protection listed in Section 4.2.1, Facilities. This Variance also replaces Requirement R2 of the continent-wide standard in its entirety and adds a new requirement, Requirement D.A.5., applicable to Planning Coordinators in the Quebec Interconnection.

In Requirements R1, R3, and R4, all references to "Generator Owner" are replaced with "Generator Owner and Transmission Owner."

This Variance replaces continent-wide Requirement R2 in its entirety with the following:

D.A.2. Each Generator Owner and Transmission Owner shall set its applicable voltage protection[5] in accordance with PRC-024 Attachment 2a, such that the applicable protection does not cause the generating resource to trip or cease injecting current during a voltage excursion within the "no trip zone" at the high side of the GSU or MPT, subject to the following exceptions: *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

- For newly designated strategic power plants, applicable protections must comply with the high voltage durations for such plants within 48 calendar months of the notification made pursuant to Requirement D.A.5. During this transition period, voltage protections must at least comply with the high voltage durations for "all power plants".
- The generating resource(s) are permitted to be set to trip or to cease injecting current during a voltage excursion bounded by the "no trip zone" of PRC-024 Attachment 2a for documented and communicated regulatory or equipment limitations in accordance with Requirement R3.
- If the Transmission Planner allows less stringent voltage protection settings than those required to meet PRC-024 Attachment 2a, then the Generator Owner or Transmission Owner may set its protection within the voltage recovery characteristics of a location-specific Transmission Planner's study.
- Inverter-based resources voltage protection settings may be set to cease injecting current momentarily during a voltage excursion at the high side of the MPT, bounded by the "no trip zone" of PRC-024 Attachment 2a, under the following conditions:

- After a minimum delay of 0.022 s, when the positive-sequence voltage exceeds 1.25 per unit (p.u.) Normal operation must resume once the voltage drops back below 1.25 p.u at the high side of the MPT.
- After a minimum delay of 0.022 s, when the phase-to-ground root mean square (RMS) voltages exceeds 1.4 p.u., as measured at generator terminals, on one or multiple phases. Normal operation must resume once the positive-sequence voltage drops back below the 1.25 p.u. at the high side of the MPT.

M.D.A.2. Each Generator Owner and Transmission Owner shall have evidence that applicable voltage protection has been set in accordance with Requirement R2, such as dated setting sheets, voltage-time boundaries, calibration sheets, coordination plots, dynamic simulation studies, calculations, or other documentation.

This Variance adds the following Requirement:

D.A.5 Each Planning Coordinator shall designate, at least once every five calendar years, the strategic power plants that must comply with Attachment 2a and notify, within 30 calendar days of its designation, each Generator Owner or Transmission Owner that owns facilities[7] in the strategic power plants. *[Violation Risk Factor: Medium] [Time Horizon: Long-term planning]*

M.D.A.5 Each Planning Coordinator shall have evidence that it designated, at least once every five calendar years, strategic power plants in accordance with Requirement D.A.5, Part 5 and shall have dated evidence that each Generator Owner or Transmission Owner has been notified in accordance with Requirement D.A.5, part 5.2. Evidence may include, but is not limited to: letters, emails, electronic files, or hard copy records demonstrating transmittal of information.

[7] Facilities in the strategic power plants include facilities from the generator up to and including the MPT or GSU.

Violation Severity Levels

This Variance adds a VSL for D.A.5 and modifies the VSL for R2 as follows:

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
D.A.2.	N/A	N/A	N/A	The Generator Owner or Transmission Owner failed to set its applicable voltage protection so that it does not trip or cease injecting current in accordance with Requirement D.A.2. OR The Generator Owner or Transmission Owner set its applicable voltage protection in accordance with Requirement D.A.2 but, for strategic power plants, failed to do so within 48 months of notification.
D.A.5.	N/A	The Planning Coordinator designated strategic power plants at least once every five calendar years but notified each Generator Owner or Transmission Owner that owns	The Planning Coordinator designated strategic power plants at least once every five calendar years but notified each Generator Owner or Transmission Owner that owns	The Planning Coordinator failed to designate, at least once every five years, the strategic power plants that must comply with Attachment 2a.

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		facilities in the strategic power plants between 31 days and 45 days after its designation.	facilities in the strategic power plants between 46 days and 60 days after its designation.	OR The Planning Coordinator failed to notify, each Generator Owner or Transmission Owner that owns facilities in the strategic power plants or notified them more than 60 days after the its designation.

E. Associated Documents

Implementation Plan

Version History

Version	Date	Action	Change Tracking
1	May 9, 2013	Adopted by the NERC Board of Trustees	
1	March 20, 2014	FERC Order issued approving PRC-024-1. (Order becomes effective on 7/1/16.)	
2	February 12, 2015	Adopted by the NERC Board of Trustees	Standard revised in Project 2014-01: Applicability revised to clarify application of requirements to BES dispersed power producing resources
2	May 29, 2015	FERC Letter Order in Docket No. RD15-3-000 approving PRC-024-2	Modifications to adjust the applicability to owners of dispersed generation resources.
3	February 6, 2020	Adopted by the NERC Board of Trustees	Standard revised in Project 2018-04
3	July 9, 2020	FERC Letter Order approved PRC-024-3. Docket No. RD20-7-000	

Attachment 1

(Frequency No Trip Boundaries by Interconnection[8])

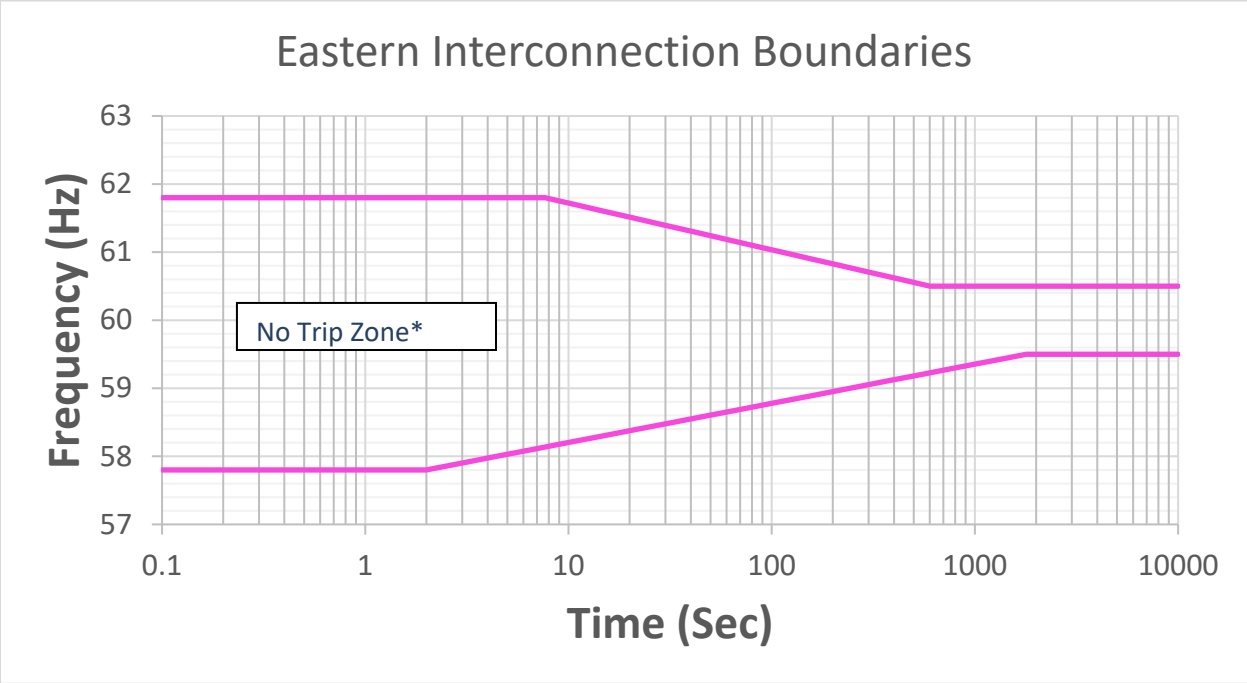


Figure 1

**** The area outside the "No Trip Zone" is not a "Must Trip Zone."***

Frequency Boundary Data Points - Eastern Interconnection

High Frequency Duration		Low Frequency Duration	
Frequency (Hz)	**Minimum Time (Sec)**	**Frequency (Hz)**	**Minimum Time (sec)**
≥61.8	Instantaneous[9]	≤57.8	Instantaneous[9]
≥60.5	$10^{(90.935-1.45713*f)}$	≤59.5	$10^{(1.7373*f-100.116)}$
<60.5	Continuous operation	> 59.5	Continuous operation

Table 1

[8] The figures do not visually represent the “no trip zone” boundaries before 0.1 seconds and after 10,000 seconds. The Frequency Boundary Data Points Table defines the entirety of the “no trip zone” boundaries.

[9] Frequency is calculated over a window of time. While the frequency boundaries include the option to trip instantaneously for frequencies outside the specified range, this calculation should occur over a time window. Typical window/filtering lengths are three to six cycles (50 – 100 milliseconds). Instantaneous trip settings based on instantaneously calculated frequency measurement is not permissible.

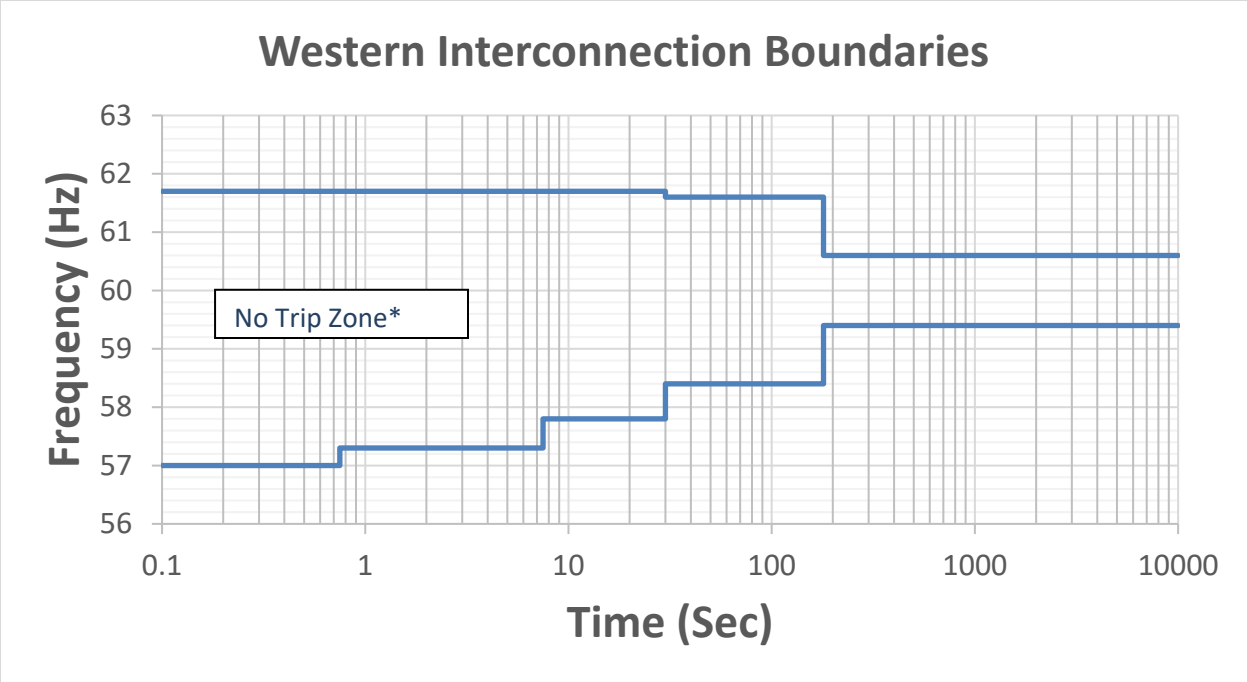


Figure 2

*** The area outside the "No Trip Zone" is not a "Must Trip Zone."**

Frequency Boundary Data Points –Western Interconnection

High Frequency Duration		Low Frequency Duration	
Frequency (Hz)	**Minimum Time (Sec)**	**Frequency (Hz)**	**Minimum Time (sec)**
≥61.7	Instantaneous[9]	≤57.0	Instantaneous[9]
≥61.6	30	≤57.3	0.75
≥60.6	180	≤57.8	7.5
<60.6	Continuous operation	≤58.4	30
		≤59.4	180
		>59.4	Continuous operation

Table 2

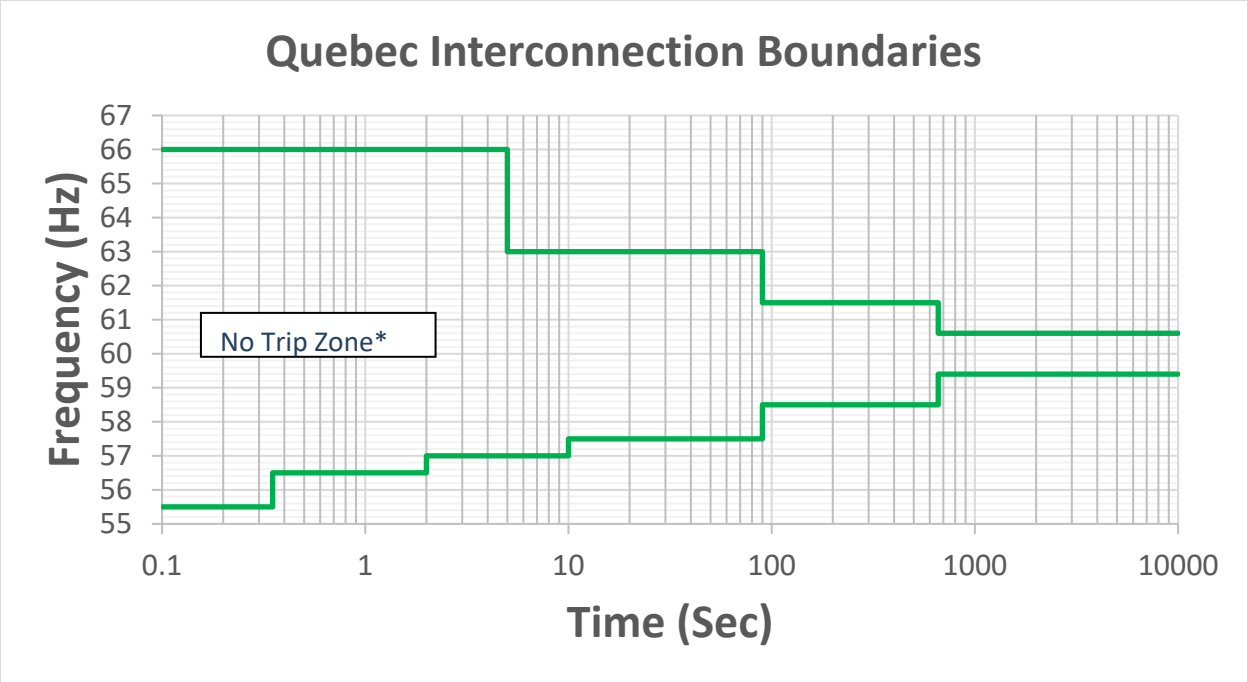


Figure 3

**** The area outside the "No Trip Zone" is not a "Must Trip Zone."***

Frequency Boundary Data Points – Quebec Interconnection

High Frequency Duration		Low Frequency Duration	
Frequency (Hz)	Minimum Time (Sec)	Frequency (Hz)	Minimum Time (Sec)
>66.0	Instantaneous[9]	<55.5	Instantaneous[9]
≥63.0	5	≤56.5	0.35
≥61.5	90	≤57.0	2
≥60.6	660	≤57.5	10
<60.6	Continuous operation	≤58.5	90
		≤59.4	660
		>59.4	Continuous operation

Table 3

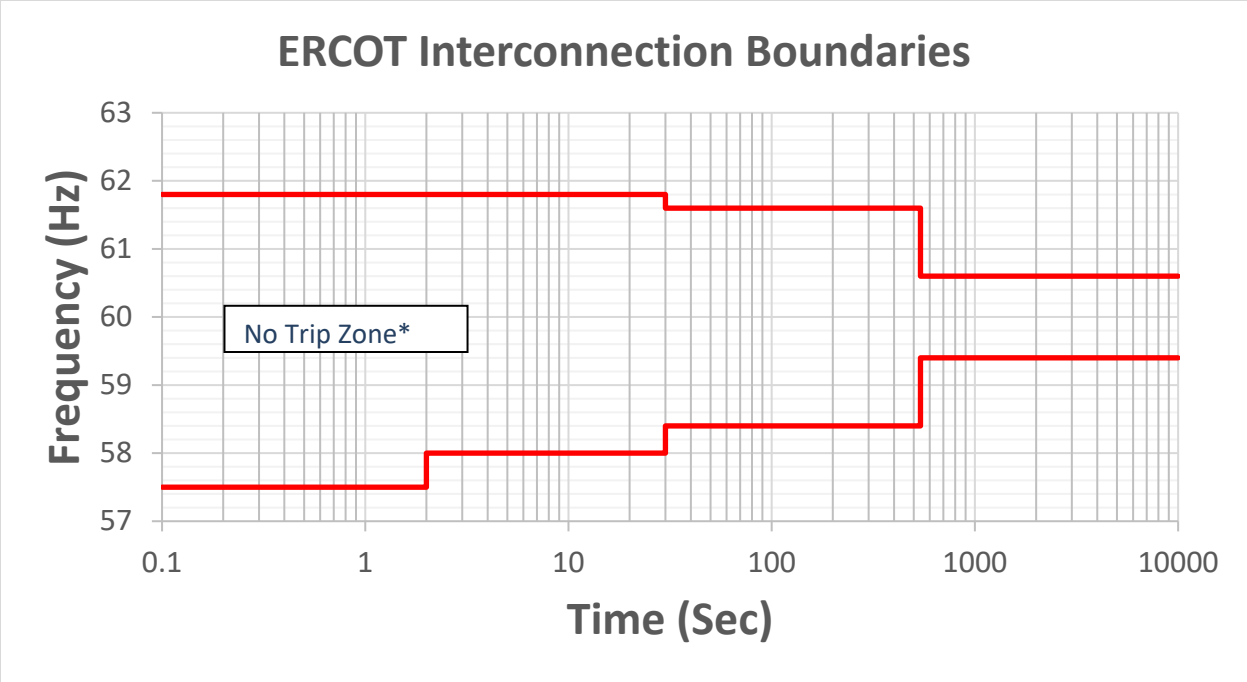


Figure 4

**** The area outside the "No Trip Zone" is not a "Must Trip Zone."***

Frequency Boundary Data Points – ERCOT Interconnection

High Frequency Duration		Low Frequency Duration	
Frequency (Hz)	Minimum Time (Sec)	Frequency (Hz)	Minimum Time (sec)
≥61.8	Instantaneous[9]	≤57.5	Instantaneous[9]
≥61.6	30	≤58.0	2
≥60.6	540	≤58.4	30
<60.6	Continuous operation	≤59.4	540
		>59.4	Continuous operation

Table 4

PRC-024 — Attachment 2

(Voltage No-Trip Boundaries – Eastern, Western, and ERCOT Interconnections)

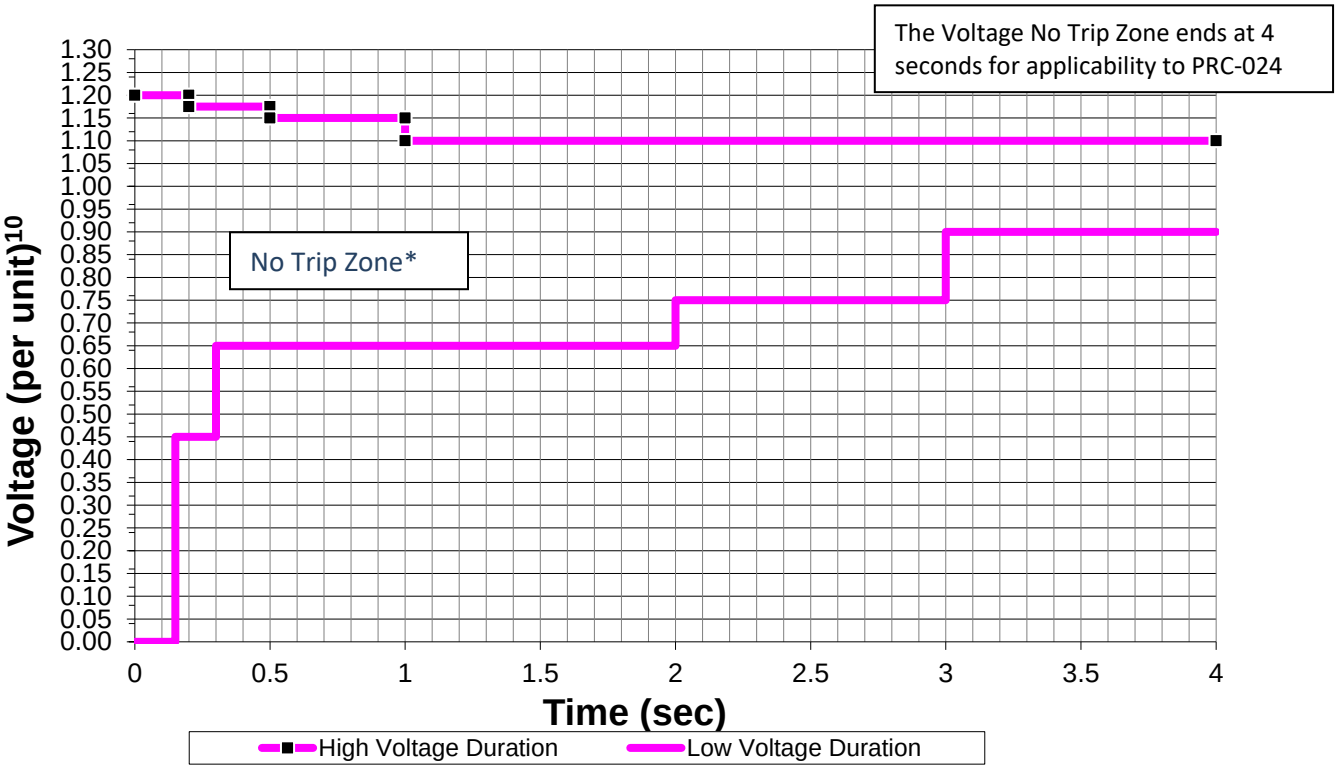


Figure 1

**** The area outside the "No Trip Zone" is not a "Must Trip Zone."***

Voltage Boundary Data Points

High Voltage Duration		Low Voltage Duration	
Voltage (pu)	Minimum Time (sec)	Voltage (pu)	Minimum Time (sec)
≥1.200	0.00	<0.45	0.15
≥1.175	0.20	<0.65	0.30
≥1.15	0.50	<0.75	2.00
≥1.10	1.00	<0.90	3.00
<1.10	4.00	≥ 0.90	4.00

Table 1

[10]Voltage at the high-side of the GSU or MPT.

Attachment 2: Voltage Boundary Clarifications – Eastern, Western, and ERCOT Interconnections

Boundary Details:

1. Unless otherwise specified by the Transmission Planner, the per unit voltage base for these boundaries is the nominal transmission system voltage (e.g., 100 kV, 115 kV, 138 kV, 161 kV, 230 kV, 345 kV, 400 kV, 500 kV, 765 kV, etc.).
2. The values in the table represent the minimum time durations allowed for specified voltage excursion thresholds.
3. When evaluating volts per hertz protection, either assume a system frequency of 60 Hertz or the magnitude of the high voltage boundary can be adjusted in proportion to deviations of frequency below 60 Hertz.
4. Voltages in the boundaries assume RMS fundamental frequency phase-to-ground or phase-to-phase per unit voltage.
5. For applicability to PRC-024, the “no trip zone” ends at 4 seconds.

Evaluating Protection Settings:

The voltage values in the Attachment 2 voltage boundaries are voltages at the high side of the GSU/MPT. For generating resources with multiple stages of step up to reach interconnecting voltage, this is the high side of the transformer with a low side below 100kV and a high side 100kV or above**.** When evaluating protection settings, consider the voltage differences between where the protection is measuring voltage and the high side of the GSU/MPT. A steady state calculation or dynamic simulation may be used.

If using a steady state calculation or dynamic simulation, use the following conditions when evaluating protection settings:

a. The most probable real and reactive loading conditions for the unit under study.

b. All installed generating plant reactive support (e.g., static VAR compensators, synchronous condensers, capacitors) equipment is available and operating normally.

c. Account for the actual tap settings of transformers between the generator terminals and the high side of the GSU/MPT.

d. For dynamic simulations, the automatic voltage regulator is in automatic voltage control mode with associated limiters in service.

PRC-024— Attachment 2a

(Voltage No-Trip Boundaries – Quebec Interconnection)

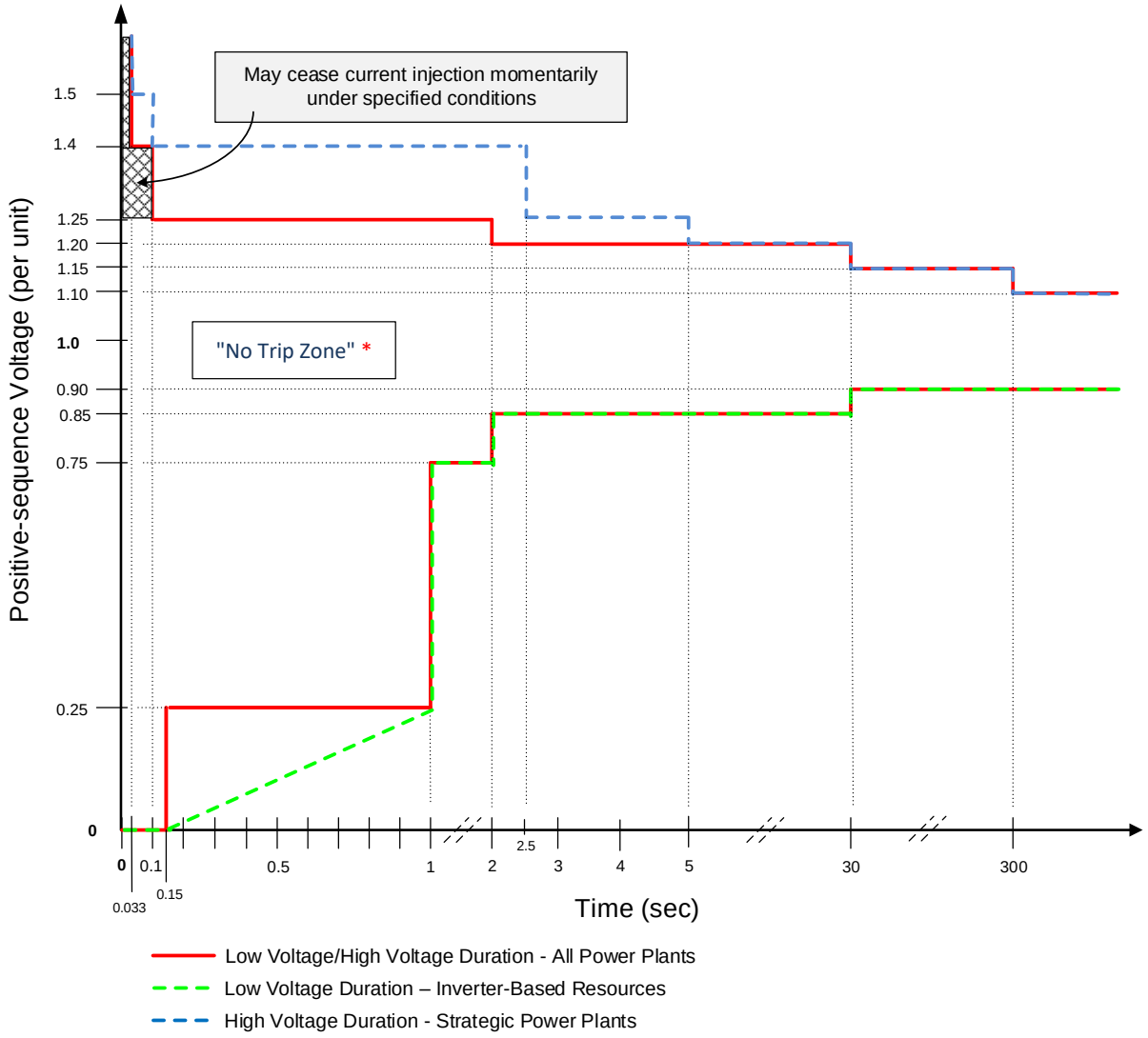


Figure 1

**** The area outside the "No Trip Zone" is not a "Must Trip Zone."***

Voltage Boundary Data Points – Quebec Interconnection

High Voltage Duration for all Power Plants		High Voltage Duration for strategic Power Plants	
Voltage (pu)	Minimum Time (sec)	Voltage (pu)	Minimum Time (sec)
---	---	>1.50	0.033
>1.40	0.033	>1.40	0.10
>1.25	0.10	>1.25	2.50
>1.20	2.00	>1.20	5.00
>1.15	30	>1.15	30
>1.10	300	>1.10	300
≤1.10	continuous	≤1.10	continuous

Table 1

Voltage Boundary Data Points – Quebec Interconnection

Low Voltage Duration for all Power Plants		Low Voltage Duration for Inverter-Based Resources	
Voltage (pu)	Minimum Time (sec)	Voltage (pu)	Minimum Time (sec)
<0.25	0.15	<0.25	3.4*V(pu)+0.15
<0.75	1.00	<0.75	1.00
<0.85	2.00	<0.85	2.00
<0.90	30	<0.90	30
≥0.90	continuous	≥0.90	continuous

Table 2

Attachment 2a: Voltage Boundary Clarifications – Quebec Interconnection

Boundary Details:

1. The per unit voltage base for these boundaries is the nominal operating voltage (e.g., 120 kV, 161 kV, 230 kV, 315 kV, 735 kV, etc.).
2. The values in the table represent the minimum time durations allowed for specified voltage excursion thresholds.
3. When evaluating volts per hertz protection, either assume a system frequency of 60 Hertz or the magnitude of the high voltage boundary can be adjusted in proportion to deviations of frequency below 60 Hertz.
4. Voltages in the Quebec Interconnection boundaries assume positive-sequence values.

Evaluating Protection Settings:

The voltage values in the Attachment 2a voltage boundaries are voltages at the high side of the GSU/MPT. For generating resources with multiple stages of step up to reach interconnecting voltage, this is the high side of the transformer that connects to the interconnecting voltage. When evaluating protection settings, consider the voltage differences between where the protection is measuring voltage and the high side of the GSU/MPT. A steady state calculation or dynamic simulation may be used.

If using a steady state calculation or dynamic simulation, use the following conditions when evaluating protection settings:

a. The most probable real and reactive loading conditions for the unit under study.
b. All installed generating plant reactive support (e.g., static VAR compensators, synchronous condensers, capacitors) equipment is available and operating normally.
c. Account for the actual tap settings of transformers between the generator terminals and the high side of the GSU/MPT.
d. For dynamic simulations, the automatic voltage regulator is in automatic voltage control mode with associated limiters in service.

Appendix PRC-024-3-QC-1

Specific provisions applicable in Québec for standard PRC-024-3 – Frequency and Voltage Protection Settings for Generating Resources

This appendix establishes specific provisions for the application of the standard in Québec. Provisions of the standard and of this appendix must be read jointly for comprehension and interpretation purposes. Where the standard and appendix differ, the appendix shall prevail.

A. Introduction

Title: No specific provisions.

Number: No specific provisions.

Purpose: No specific provisions.

Applicability:

1.1. Functional Entities

No specific provisions.

1.2. Facilities

The Facilities subject to this standard are the Facilities of the Main Transmission System (RTP).

Replace all references to Bulk Electric System (BES) with Main Transmission System (RTP).

Effective date:

1.3. Adoption of the standard by the Régie de l'énergie: December 21, 2021

1.4. Adoption of this appendix by the Régie de l'énergie: December 21, 2021

1.5. Effective date of the standard and of this appendix in Québec: July 1, 2025

For Facilities already subject to PRC-024-1, the requirements will be implemented on the following dates:

Requirements	Applicability	Implementation dates in Québec
R1 to R4	At least 40% of its applicable Facilities	October 1, 2018
	At least 60% of its applicable Facilities	October 1, 2019
	At least 80% of its applicable Facilities	October 1, 2020
	100% of its applicable Facilities	October 1, 2021

For Facilities already subject to PRC-024-2, the requirements will be implemented on the following dates:

Requirements	Applicability	Implementation dates in Québec
R1 to R4	At least 40% of its applicable Facilities	July 1, 2022
	At least 60% of its applicable Facilities	July 1, 2023
	At least 80% of its applicable Facilities	July 1, 2024
	100% of its applicable Facilities	July 1, 2025

For Facilities subject to PRC-024-3, the requirements will be implemented on the following dates:

Requirements	Applicability	Implementation dates in Québec
All requirements (R1 to R4, D.A.5) except requirement D.A.2	100% of its applicable Facilities	July 1, 2025
D.A.2	At least 50% of its applicable Facilities	July 1, 2025
	At least 70% of its applicable Facilities	July 1, 2027
	100% of its applicable Facilities	July 1, 2030

B. Requirements and Measures

Specific provision regarding Requirement R1:

Inverter-based resources, thermal generating stations, as well as generating stations equipped with asynchronous generators, shall adhere to the curves in Appendix 1, as specified by Requirement R1, except that they may be tripped at a frequency of ≥61.7 Hz.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

In Québec, “Compliance Enforcement Authority” means the Régie de l’énergie in its roles of monitoring and enforcing compliance with respect to the Reliability Standard and to this appendix.

1.2. Evidence Retention

No specific provisions.

1.3. Compliance Monitoring and Assessment Program

The Régie de l'énergie establishes the monitoring processes used to evaluate data or information for the purpose of determining compliance or non-compliance with the Reliability Standard and with this appendix.

Violation Severity Levels

No specific provisions.

D. Regional Variances

Replace all references to Bulk Electric System (BES) with Main Transmission System (RTP).

Violation Severity Levels

No specific provisions.

E. Associated Documents

No specific provisions.

PRC-024 — Attachment 1

No specific provisions.

PRC-024-2 — Attachment 2

No specific provisions.

PRC-024 – Attachment 2a

Specific provision regarding boundary details:

It is acceptable to use a measurement of the Root Mean Square (RMS) value of the overvoltage or undervoltage (phase-to-phase or phase-to-ground) provided that the trip associated with these protections occurs only when this overvoltage or undervoltage is present simultaneously on the three phases.

Appendix PRC-024-3-QC-1

Specific provisions applicable in Québec for standard PRC-024-3 – Frequency and Voltage Protection Settings for Generating Resources

Version history

Version	Date	Action	Change tracking
1	December 21, 2021	New appendix as per decision D-2021-168.	New

A. Introduction

1. **Title:** **Generator Relay Loadability**

2. **Number:** **PRC-025-2**

3. **Purpose:** To set load-responsive protective relays associated with generation Facilities at a level to prevent unnecessary tripping of generators during a system disturbance for conditions that do not pose a risk of damage to the associated equipment.

4. **Applicability:**

   4.1. Functional Entities:

   4.1.1. Generator Owner that applies load-responsive protective relays[1] at the terminals of the Elements listed in 4.2, Facilities.

   4.1.2. Transmission Owner that applies load-responsive protective relays[1] at the terminals of the Elements listed in 4.2, Facilities.

   4.1.3. Distribution Provider that applies load-responsive protective relays[1] at the terminals of the Elements listed in 4.2, Facilities.

   4.2. Facilities: The following Elements associated with Bulk Electric System (BES) generating units and generating plants, including those generating units and generating plants identified as Blackstart Resources in the Transmission Operator's system restoration plan:

   4.2.1. Generating unit(s).

   4.2.2. Generator step-up (i.e., GSU) transformer(s).

   4.2.3. Unit auxiliary transformer(s) (UAT) that supply overall auxiliary power necessary to keep generating unit(s) online.[2]

   4.2.4. Elements that connect the GSU transformer(s) to the Transmission system that are used exclusively to export energy directly from a BES generating unit or generating plant, except that Elements may also supply generating plant loads.

   4.2.5. Elements utilized in the aggregation of dispersed power producing resources.

5. **Effective Date:** See Implementation Plan

[1] Relays include low voltage protection devices that have adjustable settings.

[2] These transformers are variably referred to as station power, unit auxiliary transformer(s) (UAT), or station service transformer(s) used to provide overall auxiliary power to the generator station when the generator is running. Loss of these transformers will result in removing the generator from service. Refer to the PRC-025-2 Guidelines and Technical Basis for more detailed information concerning unit auxiliary transformers.

6. **Background:** After analysis of many of the major disturbances in the last 25 years on the North American interconnected power system, generators have been found to have tripped for conditions that did not apparently pose a direct risk to those generators and associated equipment within the time period where the tripping occurred. This tripping has often been determined to have expanded the scope and/or extended the duration of that disturbance. This was noted to be a serious issue in the August 2003 "blackout" in the northeastern North American continent.[3]

   During the recoverable phase of a disturbance, the disturbance may exhibit a "voltage disturbance" behavior pattern, where system voltage may be widely depressed and may fluctuate. In order to support the system during this transient phase of a disturbance, this standard establishes criteria for setting load-responsive protective relays such that individual generators may provide Reactive Power within their dynamic capability during transient time periods to help the system recover from the voltage disturbance. The premature or unnecessary tripping of generators resulting in the removal of dynamic Reactive Power exacerbates the severity of the voltage disturbance, and as a result changes the character of the system disturbance. In addition, the loss of Real Power could initiate or exacerbate a frequency disturbance.

7. **Standard Only Definition:** None.

B. Requirements and Measures

R1. Each Generator Owner, Transmission Owner, and Distribution Provider shall apply settings that are in accordance with PRC-025-2 – Attachment 1: Relay Settings, on each load-responsive protective relay while maintaining reliable fault protection. *[Violation Risk Factor: High] [Time Horizon: Long-Term Planning]*

M1. For each load-responsive protective relay, each Generator Owner, Transmission Owner, and Distribution Provider shall have evidence (e.g., summaries of calculations, spreadsheets, simulation reports, or setting sheets) that settings were applied in accordance with PRC-025-2 – Attachment 1: Relay Settings.

C. Compliance

1. **Compliance Monitoring Process**

   1.1. **Compliance Enforcement Authority:** "Compliance Enforcement Authority" means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring

[3] Interim Report: Causes of the August 14th Blackout in the United States and Canada, U.S.-Canada Power System Outage Task Force, November 2003 (http://www.nerc.com/docs/docs/blackout/814BlackoutReport.pdf).

and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. **Evidence Retention:** The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation:

- The Generator Owner, Transmission Owner, and Distribution Provider shall retain evidence of Requirement R1 and Measure M1 for the most recent three calendar years.
- If a Generator Owner, Transmission Owner, or Distribution Provider is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	N/A	N/A	N/A	The Generator Owner, Transmission Owner, and Distribution Provider did not apply settings in accordance with *PRC-025-2 – Attachment 1: Relay Settings*, on an applied load-responsive protective relay.

D. Regional Variances

None.

E. Associated Documents

NERC System Protection and Control Subcommittee, "Considerations for Power Plant and Transmission System Protection Coordination," technical reference document, Revision 2. (Date of Publication: July 2015)

NERC System Protection and Control Subcommittee, "Unit Auxiliary Transformer Overcurrent Relay Loadability During a Transmission Depressed Voltage Condition." (Date of Publication: March 2016)

IEEE C37.102-2006, "IEEE Guide for AC Generator Protection." (Date of Publication: 2006)

IEEE C37.17-2012, "IEEE Standard for Trip Systems for Low-Voltage (1000 V and below) AC and General Purpose (1500 V and below) DC Power Circuit Breakers." (Date of Publication: September 18, 2012)

IEEE C37.2-2008, "IEEE Standard for Electrical Power System Device Function Numbers, Acronyms, and Contact Designations." (Date of Publication: October 3, 2008)

Version History

Version	Date	Action	Change Tracking
1	August 15, 2013	Adopted by NERC Board of Trustees	New
1	July 17, 2014	FERC order issued approving PRC-025-1	
2	April 19, 2017	SAR accepted by Standards Committee	Project 2016-04
2	February 8, 2018	Adopted by NERC Board of Trustees	Revision
2	May 2, 2018	FERC Order issued approving PRC-025-2. Docket No. RD18-4-000	

PRC-025-2 – Attachment 1: Relay Settings

Introduction

This standard does not require the Generator Owner, Transmission Owner, or Distribution Provider to use any of the protective functions listed in Table 1. Each Generator Owner, Transmission Owner, and Distribution Provider that applies load-responsive protective relays on their respective Elements listed in 4.2, Facilities, shall use one of the following Options in Table 1, Relay Loadability Evaluation Criteria ("Table 1"), to set each load-responsive protective relay element according to its application and relay type. The bus voltage is based on the criteria for the various applications listed in Table 1.

Generators

Synchronous generator relay setting criteria values are derived from the unit's maximum gross Real Power capability, in megawatts (MW), as reported to the Transmission Planner, and the unit's Reactive Power capability, in megavoltampere-reactive (Mvar), is determined by calculating the MW value based on the unit's nameplate megavoltampere (MVA) rating at rated power factor. If different seasonal capabilities are reported, the maximum capability shall be used for the purposes of this standard as a minimum requirement. The Generator Owner may base settings on a capability that is higher than what is reported to the Transmission Planner.

Asynchronous generator relay setting criteria values (including inverter-based installations) are derived from the site's aggregate maximum complex power capability, in MVA, as reported to the Transmission Planner, including the Mvar output of any static or dynamic reactive power devices. If different seasonal capabilities are reported, the maximum capability shall be used for the purposes of this standard as a minimum requirement. The Generator Owner may base settings on a capability that is higher than what is reported to the Transmission Planner.

For applications where synchronous and asynchronous generator types are combined on a generator step-up transformer or on Elements that connect the generator step-up (GSU) transformer(s) to the Transmission system that are used exclusively to export energy directly from a BES generating unit or generating plant (except that Elements may also supply generating plant loads), the setting criteria shall be determined by vector summing the setting criteria of each generator type, and using the bus voltage for the given synchronous generator application and relay type.

Transformers

Calculations using the GSU transformer turns ratio shall use the actual tap that is applied (i.e., in service) for GSU transformers with de-energized tap changers (DETC). If load tap changers (LTC) are used, the calculations shall reflect the tap that results in the lowest generator bus voltage. When the criterion specifies the use of the GSU transformer's impedance, the nameplate impedance at the nominal GSU transformer turns ratio shall be used.

Applications that use more complex topology, such as generators connected to a multiple winding transformer, are not directly addressed by the criteria in Table 1. These topologies can

result in complex power flows, and may require simulation to avoid overly conservative assumptions to simplify the calculations. Entities with these topologies should set their relays in such a way that they do not operate for the conditions being addressed in this standard.

Multiple Lines

Applications that use more complex topology, such as multiple lines that connect the generator step-up (GSU) transformer(s) to the Transmission system that are used exclusively to export energy directly from a BES generating unit or generating plant (except that Elements may also supply generating plant loads) are not directly addressed by the criteria in Table 1. These topologies can result in complex power flows, and it may require simulation to avoid overly conservative assumptions to simplify the calculations. Entities with these topologies should set their relays in such a way that they do not operate for the conditions being addressed in this standard.

Exclusions

The following protection systems are excluded from the requirements of this standard:

1. Any relay elements that are in service only during start up.
2. Load-responsive protective relay elements that are armed only when the generator is disconnected from the system, (e.g., non-directional overcurrent elements used in conjunction with inadvertent energization schemes, and open breaker flashover schemes).
3. Phase fault detector relay elements employed to supervise other load-responsive phase distance elements (e.g., in order to prevent false operation in the event of a loss of potential) provided the distance element is set in accordance with the criteria outlined in the standard.
4. Protective relay elements that are only enabled when other protection elements fail (e.g., overcurrent elements that are only enabled during loss of potential conditions).
5. Protective relay elements used only for Remedial Action Schemes that are subject to one or more requirements in a NERC or Regional Reliability Standard.
6. Protection systems that detect generator overloads that are designed to coordinate with the generator short time capability by utilizing an extremely inverse characteristic set to operate no faster than 7 seconds at 218% of full load current (e.g., rated armature current), and prevent operation below 115% of full-load current.[4]
7. Protection systems that detect overloads and are designed only to respond in time periods which allow an operator 15 minutes or greater to respond to overload conditions.
8. Low voltage protection devices that do not have adjustable settings.

Table 1

Table 1 below is structured and formatted to aid the reader with identifying an option for a given load-responsive protective relay.

[4] IEEE C37.102-2006, "Guide for AC Generator Protection," Section 4.1.1.2.

The first column identifies the application (e.g., synchronous or asynchronous generators, generator step-up transformers, unit auxiliary transformers, Elements that connect the GSU transformer(s) to the Transmission system that are used exclusively to export energy directly from a BES generating unit or generating plant). Dark blue horizontal bars, excluding the header which repeats at the top of each page, demarcate the various applications.

The second column identifies the load-responsive distance or overcurrent protective relay by IEEE device numbers (e.g., 21, 50, 51, 51V-C, 51V-R, or 67) according to the application in the first column. This also includes manufacture protective device trip unit designations for long-time delay, short-time delay, and instantaneous (e.g., L, S, and I). A light blue horizontal bar between the relay types is the demarcation between relay types for a given application. These light blue bars will contain no text, except when the same application continues on the next page of the table with a different relay type.

The third column uses numeric and alphabetic options (i.e., index numbering) to identify the available options for setting load-responsive protective relays according to the application and applied relay type. Another, shorter, light blue bar contains the word “OR,” and reveals to the reader that the relay for that application has one or more options (i.e., “ways”) to determine the bus voltage and setting criteria in the fourth and fifth column, respectively. The bus voltage column and setting criteria columns provide the criteria for determining an appropriate setting. The table is further formatted by shading groups of relays associated with asynchronous generator applications. Synchronous generator applications and the unit auxiliary transformer applications are not shaded. Also, intentional buffers were added to the table such that similar options, as possible, would be paired together on a per page basis. Note that some applications may have an additional pairing that might occur on adjacent pages.

Table 1. Relay Loadability Evaluation Criteria				
Application	**Relay Type**	**Option**	**Bus Voltage[5]**	**Setting Criteria**
Synchronous generating unit(s), including Elements utilized in the aggregation of dispersed power producing resources	Phase distance relay (e.g., 21) – directional toward the Transmission system	1a	Generator bus voltage corresponding to 0.95 per unit of the high-side nominal voltage times the turns ratio of the generator step-up transformer	The impedance element shall be set less than the calculated impedance derived from 115% of: (1) Real Power output – 100% of the gross MW capability reported to the Transmission Planner, and (2) Reactive Power output – 150% of the MW value, derived from the generator nameplate MVA rating at rated power factor
		OR		
		1b	Calculated generator bus voltage corresponding to 0.85 per unit nominal voltage on the high-side terminals of the generator step-up transformer (including the transformer turns ratio and impedance)	The impedance element shall be set less than the calculated impedance derived from 115% of: (1) Real Power output – 100% of the gross MW capability reported to the Transmission Planner, and (2) Reactive Power output – 150% of the MW value, derived from the generator nameplate MVA rating at rated power factor
		OR		
		1c	Simulated generator bus voltage coincident with the highest Reactive Power output achieved during field-forcing in response to a 0.85 per unit nominal voltage on the high-side terminals of the generator step-up transformer prior to field-forcing	The impedance element shall be set less than the calculated impedance derived from 115% of: (1) Real Power output – 100% of the gross MW capability reported to the Transmission Planner, and (2) Reactive Power output –100% of the maximum gross Mvar output during field-forcing as determined by simulation
	The same application continues on the next page with a different relay type			

[5] Calculations using the generator step-up (GSU) transformer turns ratio shall use the actual tap that is applied (i.e., in service) for GSU transformers with de-energized tap changers (DETC). If load tap changers (LTC) are used, the calculations shall reflect the tap that results in the lowest generator bus voltage. When the criterion specifies the use of the GSU transformer's impedance, the nameplate impedance at the nominal GSU turns ratio shall be used.

Table 1. Relay Loadability Evaluation Criteria				
Application	**Relay Type**	**Option**	**Bus Voltage[5]**	**Setting Criteria**
Synchronous generating unit(s), including Elements utilized in the aggregation of dispersed power producing resources	Phase overcurrent relay (e.g., 50, 51, or 51V-R – voltage-restrained)	2a	Generator bus voltage corresponding to 0.95 per unit of the high-side nominal voltage times the turns ratio of the generator step-up transformer	The overcurrent element shall be set greater than 115% of the calculated current derived from: (1) Real Power output – 100% of the gross MW capability reported to the Transmission Planner, and (2) Reactive Power output – 150% of the MW value, derived from the generator nameplate MVA rating at rated power factor
		OR		
		2b	Calculated generator bus voltage corresponding to 0.85 per unit nominal voltage on the high-side terminals of the generator step-up transformer (including the transformer turns ratio and impedance)	The overcurrent element shall be set greater than 115% of the calculated current derived from: (1) Real Power output – 100% of the gross MW capability reported to the Transmission Planner, and (2) Reactive Power output – 150% of the MW value, derived from the generator nameplate MVA rating at rated power factor
		OR		
		2c	Simulated generator bus voltage coincident with the highest Reactive Power output achieved during field-forcing in response to a 0.85 per unit nominal voltage on the high-side terminals of the generator step-up transformer prior to field-forcing	The overcurrent element shall be set greater than 115% of the calculated current derived from: (1) Real Power output – 100% of the gross MW capability reported to the Transmission Planner or, and (2) Reactive Power output –100% of the maximum gross Mvar output during field-forcing as determined by simulation
	Phase time overcurrent relay (e.g., 51V-C) – voltage controlled (Enabled to operate as a function of voltage)	3	Generator bus voltage corresponding to 1.0 per unit of the high-side nominal voltage times the turns ratio of the generator step-up transformer	Voltage control setting shall be set less than 75% of the calculated generator bus voltage
A different application starts on the next page				

Table 1. Relay Loadability Evaluation Criteria				
Application	**Relay Type**	**Option**	**Bus Voltage[5]**	**Setting Criteria**
Asynchronous generating unit(s) (including inverter-based installations), including Elements utilized in the aggregation of dispersed power producing resources	Phase distance relay (e.g., 21) – directional toward the Transmission system	4	Generator bus voltage corresponding to 1.0 per unit of the high-side nominal voltage times the turns ratio of the generator step-up transformer	The impedance element shall be set less than the calculated impedance derived from 130% of the maximum aggregate nameplate MVA output at rated power factor (including the Mvar output of any static or dynamic reactive power devices)
	Phase overcurrent relay (e.g., 50, 51, or 51V-R – voltage-restrained)	5a	Generator bus voltage corresponding to 1.0 per unit of the high-side nominal voltage times the turns ratio of the generator step-up transformer	The overcurrent element shall be set greater than 130% of the calculated current derived from the maximum aggregate nameplate MVA output at rated power factor (including the Mvar output of any static or dynamic reactive power devices)
		OR		
		5b	Generator bus voltage corresponding to 1.0 per unit of the high-side nominal voltage times the turns ratio of the generator step-up transformer	The lower tolerance of the overcurrent element tripping characteristic shall not infringe upon the resource capability (including the Mvar output of the resource and any static or dynamic reactive power devices) See Figure A.
	Phase time overcurrent relay (e.g., 51V-C) – voltage controlled (Enabled to operate as a function of voltage)	6	Generator bus voltage corresponding to 1.0 per unit of the high-side nominal voltage times the turns ratio of the generator step-up transformer	Voltage control setting shall be set less than 75% of the calculated generator bus voltage
A different application starts on the next page				

Table 1. Relay Loadability Evaluation Criteria				
Application	**Relay Type**	**Option**	**Bus Voltage[5]**	**Setting Criteria**
Relays installed on generator-side[6] of the Generator step-up transformer(s) connected to synchronous generators	Phase distance relay (e.g., 21) – directional toward the Transmission system	7a	Generator bus voltage corresponding to 0.95 per unit of the high-side nominal voltage times the turns ratio of the generator step-up transformer	The impedance element shall be set less than the calculated impedance derived from 115% of: (1) Real Power output – 100% of the aggregate generation gross MW reported to the Transmission Planner, and (2) Reactive Power output – 150% of the aggregate generation MW value, derived from the generator nameplate MVA rating at rated power factor
		OR		
		7b	Calculated generator bus voltage corresponding to 0.85 per unit nominal voltage on the high-side terminals of the generator step-up transformer (including the transformer turns ratio and impedance)	The impedance element shall be set less than the calculated impedance derived from 115% of: (1) Real Power output – 100% of the aggregate generation gross MW reported to the Transmission Planner, and (2) Reactive Power output – 150% of the aggregate generation MW value, derived from the generator nameplate MVA rating at rated power factor
		OR		
		7c	Simulated generator bus voltage coincident with the highest Reactive Power output achieved during field-forcing in response to a 0.85 per unit nominal voltage on the high-side terminals of the generator step-up transformer prior to field-forcing	The impedance element shall be set less than the calculated impedance derived from 115% of: (1) Real Power output – 100% of the aggregate generation gross MW reported to the Transmission Planner, and (2) Reactive Power output –100% of the aggregate generation maximum gross Mvar output during field-forcing as determined by simulation
	The same application continues on the next page with a different relay type			

[6] If the relay is installed on the high-side of the GSU transformer, use Option 14.

Table 1. Relay Loadability Evaluation Criteria				
Application	**Relay Type**	**Option**	**Bus Voltage[5]**	**Setting Criteria**
Relays installed on generator-side[7] of the Generator step-up transformer(s) connected to synchronous generators	Phase overcurrent relay (e.g., 50 or 51)	8a	Generator bus voltage corresponding to 0.95 per unit of the high-side nominal voltage times the turns ratio of the generator step-up transformer	The overcurrent element shall be set greater than 115% of the calculated current derived from: (1) Real Power output – 100% of the aggregate generation gross MW reported to the Transmission Planner, and (2) Reactive Power output – 150% of the aggregate generation MW value, derived from the generator nameplate MVA rating at rated power factor
		OR		
		8b	Calculated generator bus voltage corresponding to 0.85 per unit nominal voltage on the high-side terminals of the generator step-up transformer (including the transformer turns ratio and impedance)	The overcurrent element shall be set greater than 115% of the calculated current derived from: (1) Real Power output – 100% of the aggregate generation gross MW reported to the Transmission Planner, and (2) Reactive Power output – 150% of the aggregate generation MW value, derived from the generator nameplate MVA rating at rated power factor
		OR		
		8c	Simulated generator bus voltage coincident with the highest Reactive Power output achieved during field-forcing in response to a 0.85 per unit nominal voltage on the high-side terminals of the generator step-up transformer prior to field-forcing	The overcurrent element shall be set greater than 115% of the calculated current derived from: (1) Real Power output – 100% of the aggregate generation gross MW reported to the Transmission Planner, and (2) Reactive Power output –100% of the aggregate generation maximum gross Mvar output during field-forcing as determined by simulation
	The same application continues on the next page with a different relay type			

[7] If the relay is installed on the high-side of the GSU transformer use, Option 15.

Table 1. Relay Loadability Evaluation Criteria				
Application	**Relay Type**	**Option**	**Bus Voltage[5]**	**Setting Criteria**
Relays installed on generator-side[8] of the Generator step-up transformer(s) connected to synchronous generators	Phase directional overcurrent relay (e.g., 67) – directional toward the Transmission system	9a	Generator bus voltage corresponding to 0.95 per unit of the high-side nominal voltage times the turns ratio of the generator step-up transformer	The overcurrent element shall be set greater than 115% of the calculated current derived from: (1) Real Power output – 100% of the aggregate generation gross MW reported to the Transmission Planner, and (2) Reactive Power output – 150% of the aggregate generation MW value, derived from the generator nameplate MVA rating at rated power factor
		OR		
		9b	Calculated generator bus voltage corresponding to 0.85 per unit nominal voltage on the high-side terminals of the generator step-up transformer (including the transformer turns ratio and impedance)	The overcurrent element shall be set greater than 115% of the calculated current derived from: (1) Real Power output – 100% of the aggregate generation gross MW reported to the Transmission Planner, and (2) Reactive Power output – 150% of the aggregate generation MW value, derived from the generator nameplate MVA rating at rated power factor
		OR		
		9c	Simulated generator bus voltage coincident with the highest Reactive Power output achieved during field-forcing in response to a 0.85 per unit nominal voltage on the high-side terminals of the generator step-up transformer prior to field-forcing	The overcurrent element shall be set greater than 115% of the calculated current derived from: (1) Real Power output – 100% of the aggregate generation gross MW reported to the Transmission Planner, and (2) Reactive Power output –100% of the aggregate generation maximum gross Mvar output during field-forcing as determined by simulation
A different application starts on the next page				

[8] If the relay is installed on the high-side of the GSU transformer use, Option 16.

Table 1. Relay Loadability Evaluation Criteria				
Application	**Relay Type**	**Option**	**Bus Voltage[5]**	**Setting Criteria**
Relays installed on generator-side of the Generator step-up transformer(s) connected to asynchronous generators only (including inverter-based installations)	Phase distance relay (e.g., 21) – directional toward the Transmission system[9]	10	Generator bus voltage corresponding to 1.0 per unit of the high-side nominal voltage times the turns ratio of the generator step-up transformer	The impedance element shall be set less than the calculated impedance derived from 130% of the maximum aggregate nameplate MVA output at rated power factor (including the Mvar output of any static or dynamic reactive power devices)
	Phase overcurrent relay (e.g., 50 or 51)[10]	11	Generator bus voltage corresponding to 1.0 per unit of the high-side nominal voltage times the turns ratio of the generator step-up transformer for overcurrent relays installed on the low-side	The overcurrent element shall be set greater than 130% of the calculated current derived from the maximum aggregate nameplate MVA output at rated power factor (including the Mvar output of any static or dynamic reactive power devices)
	Phase directional overcurrent relay (e.g., 67) – directional toward the Transmission system[11]	12	Generator bus voltage corresponding to 1.0 per unit of the high-side nominal voltage times the turns ratio of the generator step-up transformer	The overcurrent element shall be set greater than 130% of the calculated current derived from the maximum aggregate nameplate MVA output at rated power factor (including the Mvar output of any static or dynamic reactive power devices)
A different application starts on the next page				

[9] If the relay is installed on the high-side of the GSU transformer, use Option 17.
[10] If the relay is installed on the high-side of the GSU transformer, use Option 18.
[11] If the relay is installed on the high-side of the GSU transformer, use Option 19.

Table 1. Relay Loadability Evaluation Criteria				
Application	**Relay Type**	**Option**	**Bus Voltage[5]**	**Setting Criteria**
Unit auxiliary transformer(s) (UAT)	Phase overcurrent relay (e.g., 50 or 51) applied at the high-side terminals of the UAT, for which operation of the relay will cause the associated generator to trip	13a	1.0 per unit of the winding nominal voltage of the unit auxiliary transformer	The overcurrent element shall be set greater than 150% of the calculated current derived from the unit auxiliary transformer maximum nameplate MVA rating
		OR		
		13b	Unit auxiliary transformer bus voltage corresponding to the measured current	The overcurrent element shall be set greater than 150% of the unit auxiliary transformer measured current at the generator maximum gross MW capability reported to the Transmission Planner
Relays installed on the high-side of the GSU transformer,[12] including relays installed on the remote end of line, for Elements that connect the GSU transformer(s) to the Transmission system that are used exclusively to export energy directly from a BES generating unit or generating plant (except that Elements may also supply generating plant loads) – connected to synchronous generators	Phase distance relay (e.g., 21) – directional toward the Transmission system	14a	0.85 per unit of the line nominal voltage at the relay location	The impedance element shall be set less than the calculated impedance derived from 115% of: (1) Real Power output – 100% of the aggregate generation gross MW reported to the Transmission Planner, and (2) Reactive Power output – 120% of the aggregate generation MW value, derived from the generator nameplate MVA rating at rated power factor
		OR		
		14b	Simulated line voltage at the relay location coincident with the highest Reactive Power output achieved during field-forcing in response to a 0.85 per unit of the line nominal voltage at the remote end of the line prior to field-forcing	The impedance element shall be set less than the calculated impedance derived from 115% of: (1) Real Power output – 100% of the aggregate generation gross MW reported to the Transmission Planner, and (2) Reactive Power output –100% of the aggregate generation maximum gross Mvar output during field-forcing as determined by simulation
	The same application continues on the next page with a different relay type			

[12] If the relay is installed on the generator-side of the GSU transformer, use Option 7.

Table 1. Relay Loadability Evaluation Criteria				
Application	**Relay Type**	**Option**	**Bus Voltage[5]**	**Setting Criteria**
Relays installed on the high-side of the GSU transformer,[13] including relays installed at the remote end of the line, for Elements that connect the GSU transformer(s) to the Transmission system that are used exclusively to export energy directly from a BES generating unit or generating plant (except that Elements may also supply generating plant loads) – connected to synchronous generators	Phase instantaneous overcurrent supervisory element (e.g., 50) – associated with current-based, communication-assisted schemes where the scheme is capable of tripping for loss of communications and/or phase time overcurrent relay (e.g., 51)	15a	0.85 per unit of the line nominal voltage at the relay location	The overcurrent element shall be set greater than 115% of the calculated current derived from: (1) Real Power output – 100% of the aggregate generation gross MW reported to the Transmission Planner, and (2) Reactive Power output – 120% of the aggregate generation MW value, derived from the generator nameplate MVA rating at rated power factor
		OR		
		15b	Simulated line voltage at the relay location coincident with the highest Reactive Power output achieved during field-forcing in response to a 0.85 per unit of the line nominal voltage at the remote end of the line prior to field-forcing	The overcurrent element shall be set greater than 115% of the calculated current derived from: (1) Real Power output – 100% of the aggregate generation gross MW reported to the Transmission Planner, and (2) Reactive Power output –100% of the aggregate generation maximum gross Mvar output during field-forcing as determined by simulation
	The same application continues on the next page with a different relay type			

[13] If the relay is installed on the generator-side of the GSU transformer, use Option 8.

Table 1. Relay Loadability Evaluation Criteria				
Application	**Relay Type**	**Option**	**Bus Voltage[5]**	**Setting Criteria**
Relays installed on the high-side of the GSU transformer,[14] including relays installed at the remote end of the line, for Elements that connect the GSU transformer(s) to the Transmission system that are used exclusively to export energy directly from a BES generating unit or generating plant (except that Elements may also supply generating plant load.) –connected to synchronous generators	Phase directional instantaneous overcurrent supervisory element (e.g., 67) – associated with current-based, communication-assisted schemes where the scheme is capable of tripping for loss of communications directional toward the Transmission system and/or phase directional time overcurrent relay (e.g., 67) – directional toward the Transmission system	16a	0.85 per unit of the line nominal voltage at the relay location	The overcurrent element shall be set greater than 115% of the calculated current derived from: (1) Real Power output – 100% of the aggregate generation gross MW reported to the Transmission Planner, and (2) Reactive Power output – 120% of the aggregate generation MW value, derived from the generator nameplate MVA rating at rated power factor
		OR		
		16b	Simulated line voltage at the relay location coincident with the highest Reactive Power output achieved during field-forcing in response to a 0.85 per unit of the line nominal voltage at the remote end of the line prior to field-forcing	The overcurrent element shall be set greater than 115% of the calculated current derived from: (1) Real Power output – 100% of the aggregate generation gross MW reported to the Transmission Planner, and (2) Reactive Power output –100% of the aggregate generation maximum gross Mvar output during field-forcing as determined by simulation
A different application starts on the next page				

[14] If the relay is installed on the generator-side of the GSU transformer, use Option 9.

Table 1. Relay Loadability Evaluation Criteria				
Application	**Relay Type**	**Option**	**Bus Voltage[5]**	**Setting Criteria**
Relays installed on the high-side of the GSU transformer,[15] including relays installed on the remote end of line, for Elements that connect the GSU transformer(s) to the Transmission system that are used exclusively to export energy directly from a BES generating unit or generating plant (except that Elements may also supply generating plant loads) –connected to asynchronous generators only (including inverter-based installations)	Phase distance relay (e.g., 21) – directional toward the Transmission system	17	1.0 per unit of the line nominal voltage at the relay location	The impedance element shall be set less than the calculated impedance derived from 130% of the maximum aggregate nameplate MVA output at rated power factor (including the Mvar output of any static or dynamic reactive power devices)
	The same application continues on the next page with a different relay type			

[15] If the relay is installed on the generator-side of the GSU transformer, use Option 10.

Table 1. Relay Loadability Evaluation Criteria				
Application	**Relay Type**	**Option**	**Bus Voltage[5]**	**Setting Criteria**
Relays installed on the high-side of the GSU transformer,[16] including, relays installed on the remote end of the line, for Elements that connect the GSU transformer(s) to the Transmission system that are used exclusively to export energy directly from a BES generating unit or generating plant (except that Elements may also supply generating plant loads) – connected to asynchronous generators only (including inverter-based installations)	Phase instantaneous overcurrent supervisory element (e.g., 50) – associated with current-based, communication-assisted schemes where the scheme is capable of tripping for loss of communications and/or Phase time overcurrent relay (e.g., 51)	18	1.0 per unit of the line nominal voltage at the relay location	The overcurrent element shall be set greater than 130% of the calculated current derived from the maximum aggregate nameplate MVA output at rated power factor (including the Mvar output of any static or dynamic reactive power devices)
	The same application continues on the next page with a different relay type			

[16] If the relay is installed on the generator-side of the GSU transformer, use Option 11.

Table 1. Relay Loadability Evaluation Criteria				
Application	**Relay Type**	**Option**	**Bus Voltage[5]**	**Setting Criteria**
Relays installed on the high-side of the GSU transformer,[17] including relays installed on the remote end of the line, for Elements that connect the GSU transformer(s) to the Transmission system that are used exclusively to export energy directly from a BES generating unit or generating plant (except that Elements may also supply generating plant loads) –connected to asynchronous generators only (including inverter-based installations)	Phase directional instantaneous overcurrent supervisory element (e.g., 67) – associated with current-based, communication-assisted schemes where the scheme is capable of tripping for loss of communications directional toward the Transmission system and/or Phase directional time overcurrent relay (e.g., 67)	19	1.0 per unit of the line nominal voltage at the relay location	The overcurrent element shall be set greater than 130% of the calculated current derived from the maximum aggregate nameplate MVA output at rated power factor (including the Mvar output of any static or dynamic reactive power devices)
End of Table 1				

[17] If the relay is installed on the generator-side of the GSU transformer, use Option 12.

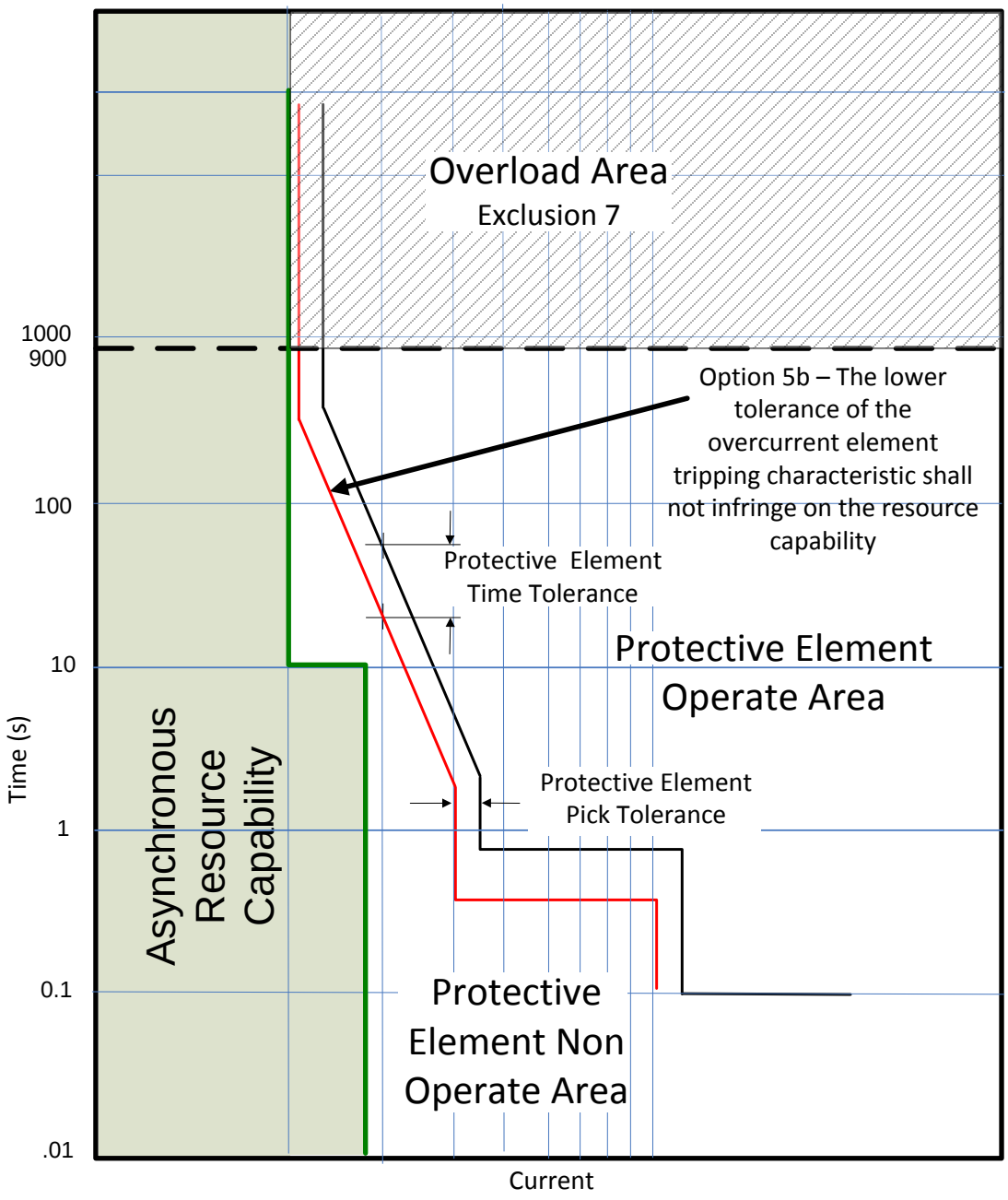


Figure A

This figure is for demonstration of Option 5b and does not mandate a specific type of protective curve or device manufacturer.

PRC-025-2 Guidelines and Technical Basis

Introduction

The document, "Considerations for Power Plant and Transmission System Protection Coordination," published by the NERC System Protection and Control Subcommittee (SPCS) provides extensive general discussion about the protective functions and generator performance addressed within this standard. This document was last revised in July 2015.[18]

The basis for the standard's loadability criteria for relays applied at the generator terminals or low-side of the generator step-up (GSU) transformer is the dynamic generating unit loading values observed during the August 14, 2003 blackout, other subsequent system events, and simulations of generating unit response to similar system conditions. The Reactive Power output observed during field-forcing in these events and simulations approaches a value equal to 150 percent of the Real Power (MW) capability of the generating unit when the generator is operating at its Real Power capability. In the SPCS technical reference document, two operating conditions were examined based on these events and simulations: (1) when the unit is operating at rated Real Power in MW with a level of Reactive Power output in Mvar which is equivalent to 150 percent times the rated MW value (representing some level of field-forcing) and (2) when the unit is operating at its declared low active Real Power operating limit (e.g., 40 percent of rated Real Power) with a level of Reactive Power output in Mvar which is equivalent to 175 percent times the rated MW value (representing some additional level of field-forcing).

Both conditions noted above are evaluated with the GSU transformer high-side voltage at 0.85 per unit. These load operating points are believed to be conservatively high levels of Reactive Power out of the generator with a 0.85 per unit high-side voltage which was based on these observations. However, for the purposes of this standard it was determined that the second load point (40 percent) offered no additional benefit and only increased the complexity for an entity to determine how to comply with the standard. Given the conservative nature of the criteria, which may not be achievable by all generating units, an alternate method is provided to determine the Reactive Power output by simulation. Also, to account for Reactive Power losses in the GSU transformer, a reduced level of output of 120 percent times the rated MW value is provided for relays applied at the high-side of the GSU transformer and on Elements that connect a GSU transformer to the Transmission system and are used exclusively to export energy directly from a BES generating unit or generating plant.

The phrase, "while maintaining reliable fault protection" in Requirement R1, describes that the Generator Owner, Transmission Owner, and Distribution Provider is to comply with this standard while achieving its desired protection goals. Load-responsive protective relays, as addressed within this standard, may be intended to provide a variety of backup protection functions, both within the generating unit or generating plant and on the Transmission system, and this standard is not intended to result in the loss of these protection functions. Instead, it is suggested that the

[18] http://www.nerc.com/comm/PC/System%20Protection%20and%20Control%20Subcommittee%20SPCS%2020/SPCS%20Gen%20Prot%20Coordination%20Technical%20Reference%20Document.pdf.

Generator Owner, Transmission Owner, and Distribution Provider consider both the requirement within this standard and its desired protection goals, and perform modifications to its protective relays or protection philosophies as necessary to achieve both.

For example, if the intended protection purpose is to provide backup protection for a failed Transmission breaker, it may not be possible to achieve this purpose while complying with this standard if a simple mho relay is being used. In this case, it may be possible to meet this purpose by replacing the legacy relay with a modern advanced-technology relay that can be set using functions such as load encroachment. It may otherwise be necessary to reconsider whether this is an appropriate method of achieving protection for the failed Transmission breaker, and whether this protection can be better provided by, for example, applying a breaker failure relay with a transfer trip system.

Requirement R1 establishes that the Generator Owner, Transmission Owner, and Distribution Provider must understand the applications of Attachment 1: Relay Settings, Table 1: Relay Loadability Evaluation Criteria ("Table 1") in determining the settings that it must apply to each of its load-responsive protective relays to prevent an unnecessary trip of its generator during the system conditions anticipated by this standard.

Applicability

To achieve the reliability objective of this standard it is necessary to include all load-responsive protective relays that are affected by increased generator output in response to system disturbances. This standard is therefore applicable to relays applied by the Generator Owner, Transmission Owner, and Distribution Provider at the terminals of the generator, GSU transformer, unit auxiliary transformer (UAT), Elements that connect a GSU transformer to the Transmission system that are used exclusively to export energy directly from a BES generating unit or generating plant, and Elements utilized in the aggregation of dispersed power producing resources.

The Generator Owner's interconnection facility (in some cases labeled a "transmission Facility" or "generator leads") consists of Elements between the GSU transformer and the interface with the portion of the Bulk Electric System (BES) where Transmission Owners take over the ownership. This standard does not use the industry recognized term "generator interconnection Facility" consistent with the work of Project 2010-07 (Generator Requirements at the Transmission Interface), because the term generator interconnection Facility implies ownership by the Generator Owner. Instead, this standard refers to these Facilities as "Elements that connect a GSU transformer to the Transmission system that are used exclusively to export energy directly from a BES generating unit or generating plant" to include these Facilities when they are also owned by the Transmission Owner or Distribution Provider. The load-responsive protective relays in this standard for which an entity shall be in compliance are dependent on the location and the application of the protective functions. Figures 1, 2, and 3 illustrate various generator interface connections with the Transmission system, and Figure 4 illustrates examples of Elements utilized in the aggregation of dispersed power resources that are in scope of the standard.

Figure 1

Figure 1 is a single (or set) of generators connected to the Transmission system through a radial line that is used exclusively to export energy directly from a BES generating unit or generating plant to the network. The protective relay R1 located on the high-side of the GSU transformer breaker CB100 is generally applied to provide backup protection to the relaying located at Bus A and in some cases Bus B. Under this application, relay R1 would apply the loadability requirement in PRC-025-2 using an appropriate option for the application from Table 1 (e.g., Options 14 through 19) for Elements that connect a GSU transformer to the Transmission system that are used exclusively to export energy directly from a BES generating unit or generating plant.

The protective relay R2 located on the incoming source breaker CB102 to the generating plant applies relaying that primarily protects the line by using line differential relaying from Bus A to B and also provides backup protection to the transmission relaying at Bus B. In this case, the relay function that provides line protection would apply the loadability requirement in PRC-025-2 and an appropriate option for the application from Table 1 (e.g., 15a, 15b, 16a, 16b, 18, and 19) for phase overcurrent supervisory elements (i.e., phase fault detectors) associated with current-based, communication-assisted schemes (i.e., pilot wire, phase comparison, and line current differential) where the scheme is capable of tripping for loss of communications. The backup protective function would apply the requirement in the PRC-025-2 standard using an appropriate option for the application from Table 1 (e.g., Options 14 through 19) for Elements that connect a GSU transformer to the Transmission system that are used exclusively to export energy directly from a BES generating unit or generating plant.

Since Elements that connect the GSU transformer(s) to the Transmission system that are used exclusively to export energy directly from a BES generating unit or generating plant are applicable to the standard, the loadability for relays applied on these Elements as shown in the shaded area of Figure 1 (i.e., CB102 and CB103) must be considered. If relay R2 or R3 is set with an element directional toward the transmission system (e.g., Buses B, C and D) or are non-directional, the relay would be affected by increased generator output in response to system disturbances and must meet the loadability setting criteria described in the standard. If relay R2 or R3 is set with an element directional toward the generator (e.g., Bus A), the relay would not be affected by increased generator output in response to system disturbances; therefore, the entity would not be required to apply the loadability setting criteria described in this standard.

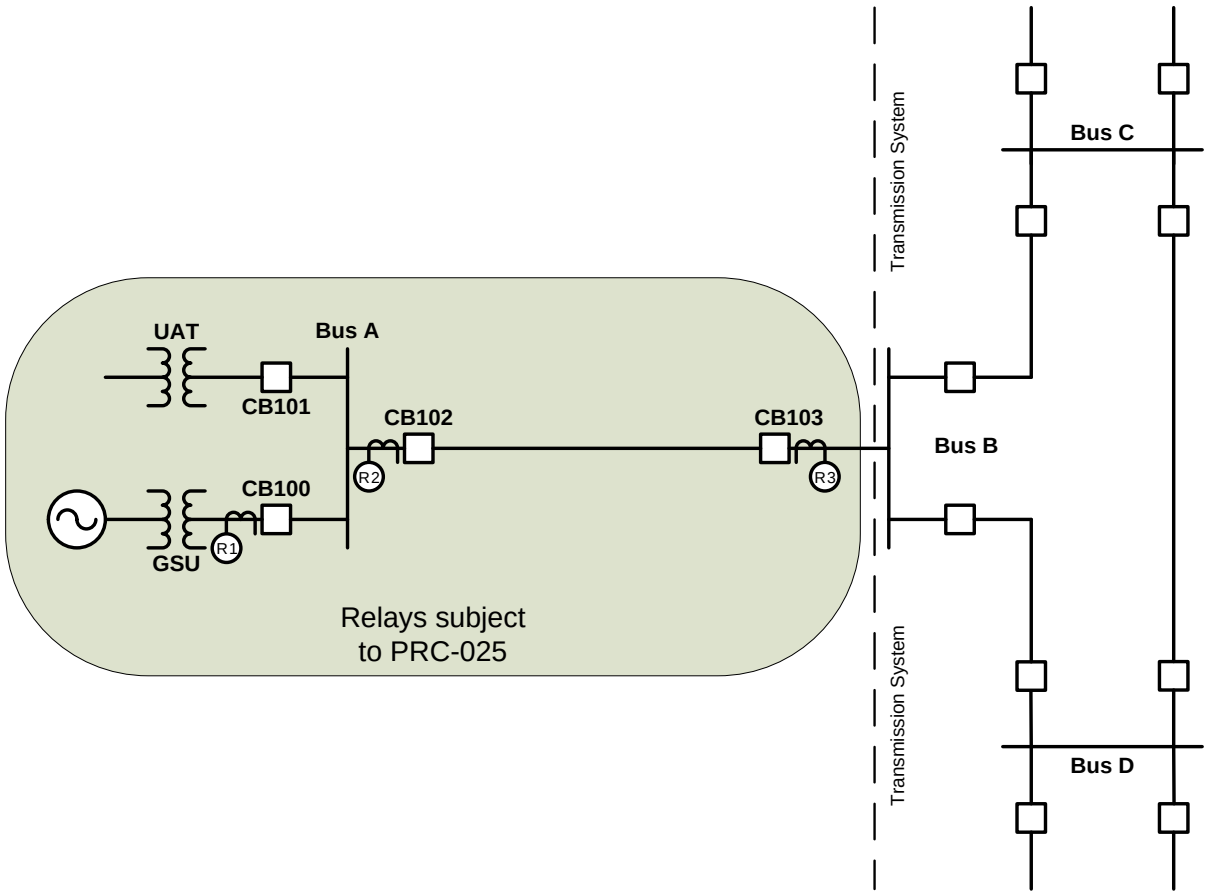


Figure 1: Generation exported through a single radial line

Figure 2

Figure 2 is an example of a single (or set) of generators connected to the Transmission system through multiple lines that are used exclusively to export energy directly from a BES generating unit or generating plant to the network. The protective relay R1 on the high-side of the GSU transformer breaker CB100 is generally applied to provide backup protection to the Transmission relaying located at Bus A and in some cases Bus B. Under this application, relay R1 would apply the loadability requirement in PRC-025-2 using an appropriate option for the application from Table 1 (e.g., Options 14 through 19) for Elements that connect a GSU transformer to the Transmission system that are used exclusively to export energy directly from a BES generating unit or generating plant.

The protective relays R2 and R3 located on the incoming source breakers CB102 and CB103 to the generating plant applies relaying that primarily protects the line from Bus A to B and also provides backup protection to the transmission relaying at Bus B. In this case, the relay function that provides line protection would apply the loadability requirement in PRC-025-2 and an appropriate option for the application from Table 1 (e.g., Options 15a, 15b, 16a, 16b, 18, and 19) for phase overcurrent supervisory elements (i.e., phase fault detectors) associated with current-based, communication-assisted schemes (i.e., pilot wire, phase comparison, and line current

differential) where the scheme is capable of tripping for loss of communications. The backup protective function would apply the requirement in the PRC-025-2 standard using an appropriate option for the application from Table 1 (e.g., Options 14 through 19) for Elements that connect a GSU transformer to the Transmission system that are used exclusively to export energy directly from a BES generating unit or generating plant.

Since Elements that connect the GSU transformer(s) to the Transmission system that are used exclusively to export energy directly from a BES generating unit or generating plant are applicable to the standard, the loadability for relays applied on these Elements as shown in the shaded area of Figure 2 (i.e., CB102, CB103, CB104, and CB105) must be considered. If relay R2, R3, R4, or R5 is set with an element directional toward the transmission system (e.g., Buses B, C and D) or are non-directional, the relay would be affected by increased generator output in response to system disturbances and must meet the loadability setting criteria described in the standard. If relay R2, R3, R4, or R5 is set with an element directional toward the generator (e.g., Bus A), the relay would not be affected by increased generator output in response to system disturbances; therefore, the entity would not be required to apply the loadability setting criteria described in this standard.

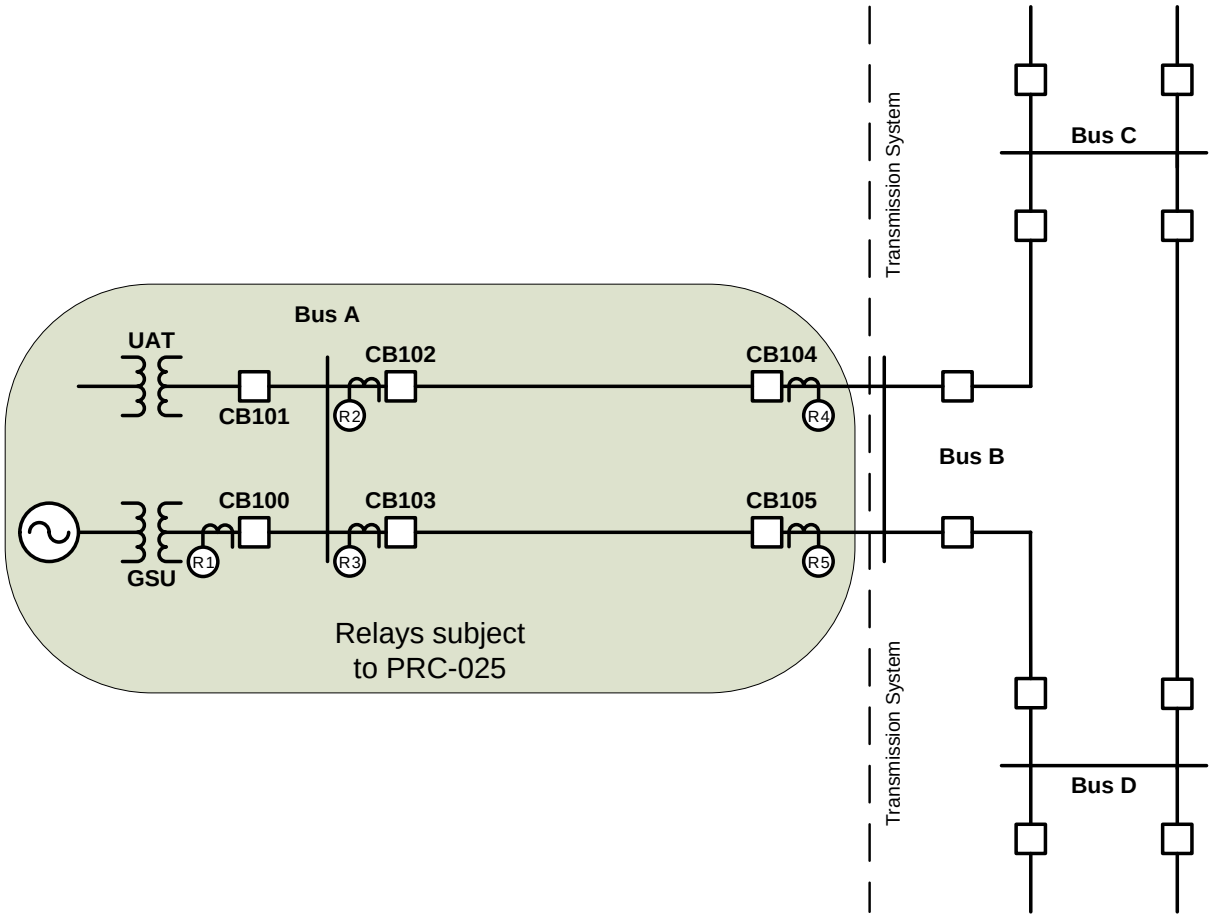


Figure 2: Generation exported through multiple radial lines

Figure 3

Figure 3 is example a single (or set) of generators exporting power dispersed through multiple lines to the Transmission system through a network. The protective relay R1 on the high-side of the GSU transformer breaker CB100 is generally applied to provide backup protection to the Transmission relaying located at Bus A and in some cases Bus C or Bus D. Under this application, relay R1 would apply the applicable loadability requirement in PRC-025-2 using an appropriate option for the application from Table 1 (e.g., Options 14 through 19) for Elements that connect a GSU transformer to the Transmission system that are used exclusively to export energy directly from a BES generating unit or generating plant.

Since the lines from Bus A to Bus C and from Bus A to Bus D are part of the transmission network, these lines would not be considered as Elements that connect a GSU transformer to the Transmission system that are used exclusively to export energy directly from a BES generating unit or generating plant. Therefore, the applicable responsible entity would be responsible for the load-responsive protective relays R2 and R3 under the PRC-023 standard. The applicable responsible entity's loadability relays R4 and R5 located on the breakers CB104 and CB105 at Bus C and D are also subject to the requirements of the PRC-023 standard.

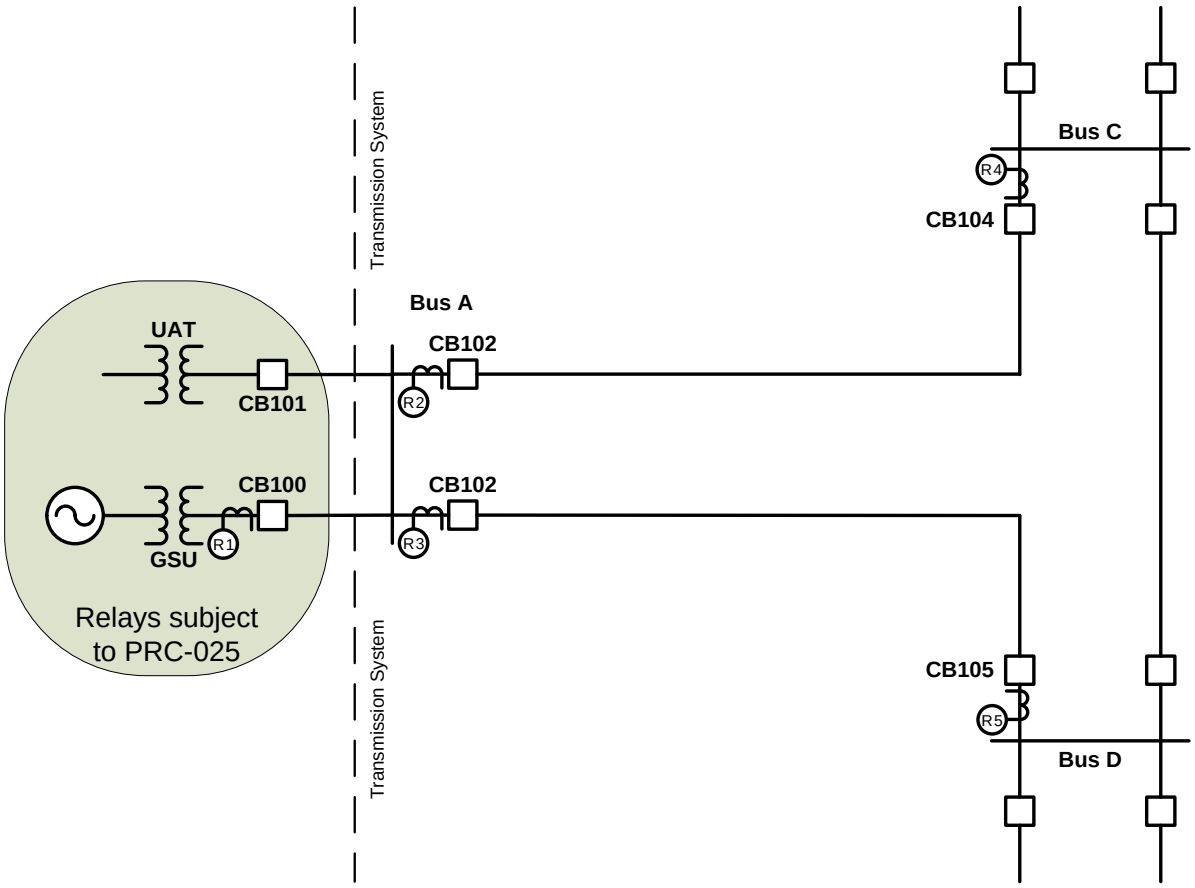


Figure 3: Generation exported through a network

This standard is also applicable to the UATs that supply station service power to support the on-line operation of generating units or generating plants. These transformers are variably referred to as station power, unit auxiliary transformer(s), or station service transformer(s) used to provide overall auxiliary power to the generator station when the generator is running. Inclusion of these transformers satisfies a directive in FERC Order No. 733, paragraph 104, which directs NERC to include in this standard a loadability requirement for relays used for overload protection of the UAT(s) that supply normal station service for a generating unit. The NERC System Protection and Control Subcommittee addressed low-side UAT protection in the document called *Unit Auxiliary Transformer Overcurrent Relay Loadability During a Transmission Depressed Voltage Condition*,[19] March 2016.

Figure 4

Elements utilized in the aggregation of dispersed power producing resources (in some cases referred to as a "collector system" or "feeders") consist of the Elements between individual generating units and the common point of interconnection to the Transmission system.

[19] http://www.nerc.com/comm/PC/System%20Protection%20and%20Control%20Subcommittee%20SPCS%2020/NERC%20-%20SPCS%20UAT%20-%20FEB_2016_final.pdf.

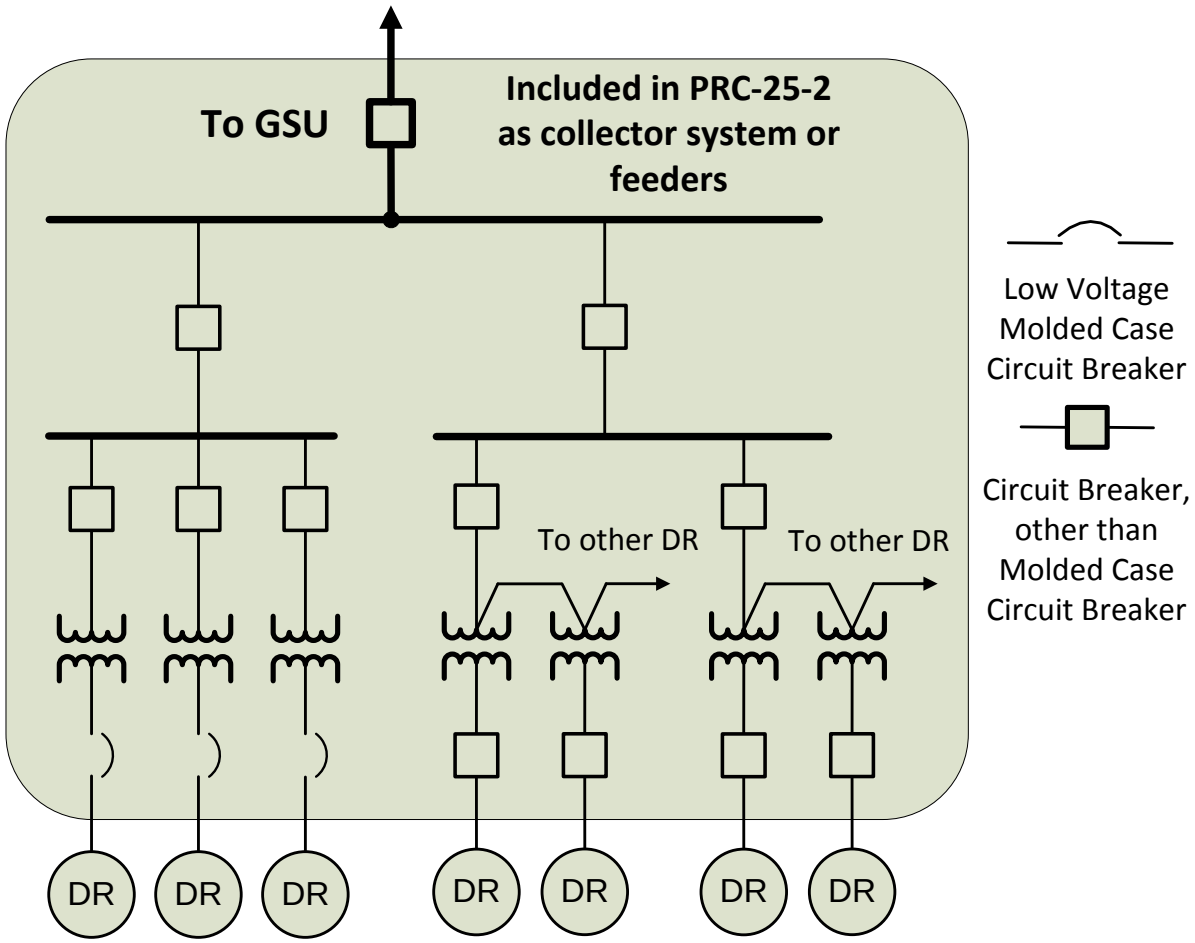


Figure-4: Elements utilized in the aggregation of dispersed power producing resources (DR)

Synchronous Generator Performance

When a synchronous generator experiences a depressed voltage, the generator will respond by increasing its Reactive Power output to support the generator terminal voltage. This operating condition, known as "field-forcing," results in the Reactive Power output exceeding the steady-state capability of the generator and may result in operation of generation system load-responsive protective relays if they are not set to consider this operating condition. The ability of the generating unit to withstand the increased Reactive Power output during field-forcing is limited by the field winding thermal withstand capability. The excitation limiter will respond to begin reducing the level of field-forcing in as little as one second, but may take much longer, depending on the level of field-forcing given the characteristics and application of the excitation system. Since this time may be longer than the time-delay of the generator load-responsive protective relay, it is important to evaluate the loadability to prevent its operation for this condition.

The generator bus voltage during field-forcing will be higher than the high-side voltage due to the voltage drop across the GSU transformer. When the relay voltage is supplied from the generator bus, it is necessary to assess loadability using the generator bus voltage. The criteria established within Table 1 are based on 0.85 per unit of the line nominal voltage. This voltage was widely observed during the events of August 14, 2003, and was determined during the analysis of the events to represent a condition from which the System may have recovered, had other undesired behavior not occurred.

The dynamic load levels specified in Table 1 under column "Setting Criteria" are representative of the maximum expected apparent power during field-forcing with the Transmission system voltage at 0.85 per unit, for example, at the high-side of the GSU transformer. These values are based on records from the events leading to the August 14, 2003 blackout, other subsequent System events, and simulations of generating unit responses to similar conditions. Based on these observations, the specified criteria represent conservative but achievable levels of Reactive Power output of the generator with a 0.85 per unit high-side voltage at the point of interconnection.

The dynamic load levels were validated by simulating the response of synchronous generating units to depressed Transmission system voltages for 67 different generating units. The generating units selected for the simulations represented a broad range of generating unit and excitation system characteristics as well as a range of Transmission system interconnection characteristics. The simulations confirmed, for units operating at or near the maximum Real Power output, that it is possible to achieve a Reactive Power output of 1.5 times the rated Real Power output when the Transmission system voltage is depressed to 0.85 per unit. While the simulations demonstrated that all generating units may not be capable of this level of Reactive Power output, the simulations confirmed that approximately 20 percent of the units modeled in the simulations could achieve these levels. On the basis of these levels, Table 1, Options 1a (i.e., 0.95 per unit) and 1b (i.e., 0.85 per unit), for example, are based on relatively simple, but conservative calculations of the high-side nominal voltage. In recognition that not all units are capable of achieving this level of output Option 1c (i.e., simulation) was developed to allow the Generator Owner, Transmission Owner, or Distribution Provider to simulate the output of a generating unit when the simple calculation is not adequate to achieve the desired protective relay setting.

Dispersed Generation

This standard is applicable to dispersed generation such as wind farms and solar arrays. The intent of this standard is to ensure the aggregate facility as defined above will remain on-line during a system disturbance; therefore, all output load-responsive protective relays associated with the facility are included in PRC-025.

Dispersed power producing resources with aggregate capacity greater than 75 MVA (gross aggregate nameplate rating) utilizing a system designed primarily for aggregating capacity, connected at a common point at a voltage of 100 kV or above are included in PRC-025-2. Load-responsive protective relays that are applied on Elements that connect these individual generating units through the point of interconnection with the Transmission system are within

the scope of PRC-025-2. For example, feeder overcurrent relays and feeder step-up transformer overcurrent relays (see Figure 6) are included because these relays are challenged by generator loadability.

In the case of solar arrays where there are multiple voltages utilized in converting the solar panel DC output to a 60Hz AC waveform, the "terminal" is defined at the 60Hz AC output of the inverter-solar panel combination.

Asynchronous Generator Performance

Asynchronous generators will not respond to a disturbance with the same magnitude of apparent power that a synchronous generator will respond. Asynchronous generators, though, will support the system during a disturbance. Inverter-based generators will provide Real Power and Reactive Power (depending on the installed capability and regional grid code requirements) and may even provide a faster Reactive Power response than a synchronous generator. The magnitude of this response may slightly exceed the steady-state capability of the inverter but only for a short duration before limiter functions will activate. Although induction generators will not inherently supply Reactive Power, induction generator installations may include static and/or dynamic reactive devices, depending on regional grid code requirements. These devices also may provide Real Power during a voltage disturbance. Thus, tripping asynchronous generators may exacerbate a disturbance.

Inverters, including wind turbines (i.e., Types 3 and 4) and photovoltaic solar, are commonly available with 0.90 power factor capability. This calculates to an apparent power magnitude of 1.11 per unit of rated MW.

Similarly, induction generator installations, including Type 1 and Type 2 wind turbines, often include static and/or dynamic reactive devices to meet grid code requirements and may have apparent power output similar to inverter-based installations; therefore, it is appropriate to use the criteria established in the Table 1 (i.e., Options 4, 5, 6, 10, 11, 12, 17, 18, and 19) for asynchronous generator installations.

Synchronous Generator Simulation Criteria

The Generator Owner, Transmission Owner, or Distribution Provider who elects a simulation option to determine the synchronous generator performance on which to base relay settings may simulate the response of a generator by lowering the Transmission system voltage at the remote end of the line or at the high-side of the GSU transformer (as prescribed by the Table 1 criteria). This can be simulated by means such as modeling the connection of a shunt reactor at the remote end of the line or at the GSU transformer high-side to lower the voltage to 0.85 per unit prior to field-forcing. The resulting step change in voltage is similar to the sudden voltage depression observed in parts of the Transmission system on August 14, 2003. The initial condition for the simulation should represent the generator at 100 percent of the maximum gross Real Power capability in MW as reported to the Transmission Planner. The simulation is used to determine the Reactive Power and voltage at the relay location to calculate relay setting limits. The Reactive Power value obtained by simulation is the highest simulated level of Reactive Power

achieved during field-forcing. The voltage value obtained by simulation is the simulated voltage coincident with the highest Reactive Power achieved during field-forcing. These values of Reactive Power and voltage correspond to the minimum apparent impedance and maximum current observed during field-forcing.

Phase Distance Relay – Directional Toward Transmission System (e.g., 21)

Generator phase distance relays that are directional toward the Transmission system, whether applied for the purpose of primary or backup GSU transformer protection, external system backup protection, or both, were noted during analysis of the August 14, 2003 disturbance event to have unnecessarily or prematurely tripped a number of generating units or generating plants, which contributed to the scope of that disturbance. Specifically, eight generators are known to have been tripped by this protection function. These options establish criteria for phase distance relays that are directional toward the Transmission system to help assure that generators, to the degree possible, will provide System support during disturbances in an effort to minimize the scope of those disturbances.

The phase distance relay that is directional toward the Transmission system measures impedance derived from the quotient of generator terminal voltage divided by generator stator current.

Section 4.6.1.1 of IEEE C37.102-2006, "Guide for AC Generator Protection," describes the purpose of this protection as follows (emphasis added):

> *"The distance relay applied for this function is intended to isolate the generator from the power system for a fault* ***that is not cleared by the transmission line breakers.*** *In some cases this relay is set with a very long reach. A condition that causes the generator voltage regulator to boost generator excitation for a sustained period may result in the system apparent impedance, as monitored at the generator terminals, to fall within the operating characteristics of the distance relay. Generally, a distance relay setting of 150% to 200% of the generator MVA rating at its rated power factor has been shown to provide good coordination for stable swings, system faults involving in-feed, and* ***normal loading conditions.*** *However, this setting may also result in failure of the relay to operate for some line faults where the line relays fail to clear. It is recommended that the setting of these relays be evaluated between the generator protection engineers and the system protection engineers* ***to optimize coordination while still protecting the turbine generator****. Stability studies may be needed to help determine a set point to optimize protection and coordination. Modern excitation control systems include overexcitation limiting and protection devices to protect the generator field, but the time delay before they reduce excitation is several seconds. In distance relay applications for which the voltage*

> *regulator action could cause an incorrect trip, consideration should be given to reducing the reach of the relay and/or coordinating the tripping time delay with the time delays of the protective devices in the voltage regulator. Digital multifunction relays equipped with load encroachment binders [sic] can prevent misoperation for these conditions.* ***Within its operating zone, the tripping time for this relay must coordinate with the longest time delay for the phase distance relays on the transmission lines connected to the generating substation bus.*** *With the advent of multifunction generator protection relays, it is becoming more common to use two-phase distance zones. In this case, the second zone would be set as previously described. When two zones are applied for backup protection, the first zone is typically set to see the substation bus (120% of the GSU transformer). This setting should be checked for coordination with the zone-1 element on the shortest line off of the bus. The normal zone-2 time-delay criteria would be used to set the delay for this element. Alternatively, zone-1 can be used to provide high-speed protection for phase faults, in addition to the normal differential protection, in the generator and iso-phase bus with partial coverage of the GSU transformer. For this application, the element would typically be set to 50% of the transformer impedance with little or no intentional time delay. It should be noted that it is possible that this element can operate on an out-of-step power swing condition and provide misleading targeting."*

If a mho phase distance relay that is directional toward the Transmission system cannot be set to maintain reliable fault protection and also meet the criteria in accordance with Table 1, there may be other methods available to do both, such as application of blinders to the existing relays, implementation of lenticular characteristic relays, application of offset mho relays, or implementation of load encroachment characteristics. Some methods are better suited to improving loadability around a specific operating point, while others improve loadability for a wider area of potential operating points in the R-X plane. The operating point for a stressed System condition can vary due to the pre-event system conditions, severity of the initiating event, and generator characteristics such as Reactive Power capability.

For this reason, it is important to consider the potential implications of revising the shape of the relay characteristic to obtain a longer relay reach, as this practice may result in a relay characteristic that overlaps the capability of the generating unit when operating at a Real Power output level other than 100 percent of the maximum Real Power capability. Overlap of the relay characteristic and generator capability could result in tripping the generating unit for a loading condition within the generating unit capability. The examples in Appendix E of the Considerations for Power Plant and Transmission System Protection Coordination technical reference document illustrate the potential for, and need to avoid, encroaching on the generating unit capability.

Phase Instantaneous Overcurrent Relay (e.g., 50)

The 50 element is a non-directional overcurrent element that typically has no intentional time delay. The primary application is for close-in high current faults where high speed operation is required or preferred. The instantaneous overcurrent elements are subject to the same loadability issues as the time overcurrent elements referenced in this standard.

Phase Time Overcurrent Relay (e.g., 51)

See Chapter 2 of the Considerations for Power Plant and Transmission System Protection Coordination technical reference document for a detailed discussion of this protection function. Note that the setting criteria established within the Table 1 options differ from the Considerations for Power Plant and Transmission System Protection Coordination technical reference document. Rather than establishing a uniform setting threshold of 200 percent of the generator MVA rating at rated power factor for all applications, the Table 1 setting criteria are based on the maximum expected generator Real Power output based on whether the generator is a synchronous or asynchronous unit.

Phase Time Overcurrent Relay – Voltage-Restrained (e.g., 51V-R)

Phase time overcurrent voltage-restrained relays (e.g., 51V-R), which change their sensitivity as a function of voltage, whether applied for the purpose of primary or backup GSU transformer protection, for external system phase backup protection, or both, were noted, during analysis of the August 14, 2003 disturbance event to have unnecessarily or prematurely tripped a number of generating units or generating plants, contributing to the scope of that disturbance. Specifically, 20 generators are known to have been tripped by voltage-restrained and voltage-controlled protection functions together. These protective functions are variably referred to by IEEE function numbers 51V, 51R, 51VR, 51V/R, 51V-R, or other terms. See Chapter 2 of the Considerations for Power Plant and Transmission System Protection Coordination technical reference document for a detailed discussion of this protection function.

Phase Time Overcurrent Relay – Voltage Controlled (e.g., 51V-C)

Phase time overcurrent voltage-controlled relays (e.g., 51V-C), enabled as a function of voltage, are variably referred to by IEEE function numbers 51V, 51C, 51VC, 51V/C, 51V-C, or other terms. See Chapter 2 of the Considerations for Power Plant and Transmission System Protection Coordination technical reference document for a detailed discussion of this protection function.

Phase Directional Overcurrent Relay – Directional Toward Transmission System (e.g., 67)

See Chapter 2 of the Considerations for Power Plant and Transmission System Protection Coordination technical reference document for a detailed discussion of the phase time overcurrent protection function. The basis for setting directional and non-directional overcurrent relays is similar. Note that the setting criteria established within the Table 1 options differ from of the Considerations for Power Plant and Transmission System Protection Coordination technical reference document. Rather than establishing a uniform setting threshold of 200 percent of the generator MVA rating at rated power factor for all applications, the Table 1 setting

criteria are based on the maximum expected generator Real Power output based on whether the generator is a synchronous or asynchronous unit.

Table 1, Options

Introduction

The margins in the Table 1 options are based on guidance found in the Considerations for Power Plant and Transmission System Protection Coordination technical reference document. The generator bus voltage during field-forcing will be higher than the high-side voltage due to the voltage drop across the GSU transformer. When the relay voltage is supplied from the generator bus, it is necessary to assess loadability using the generator bus voltage.

Relay Connections

Figures 5 and 6 below illustrate the connections for each of the Table 1 options provided in PRC-025-2, Attachment 1: Relay Settings, Table 1: Relay Loadability Evaluation Criteria.

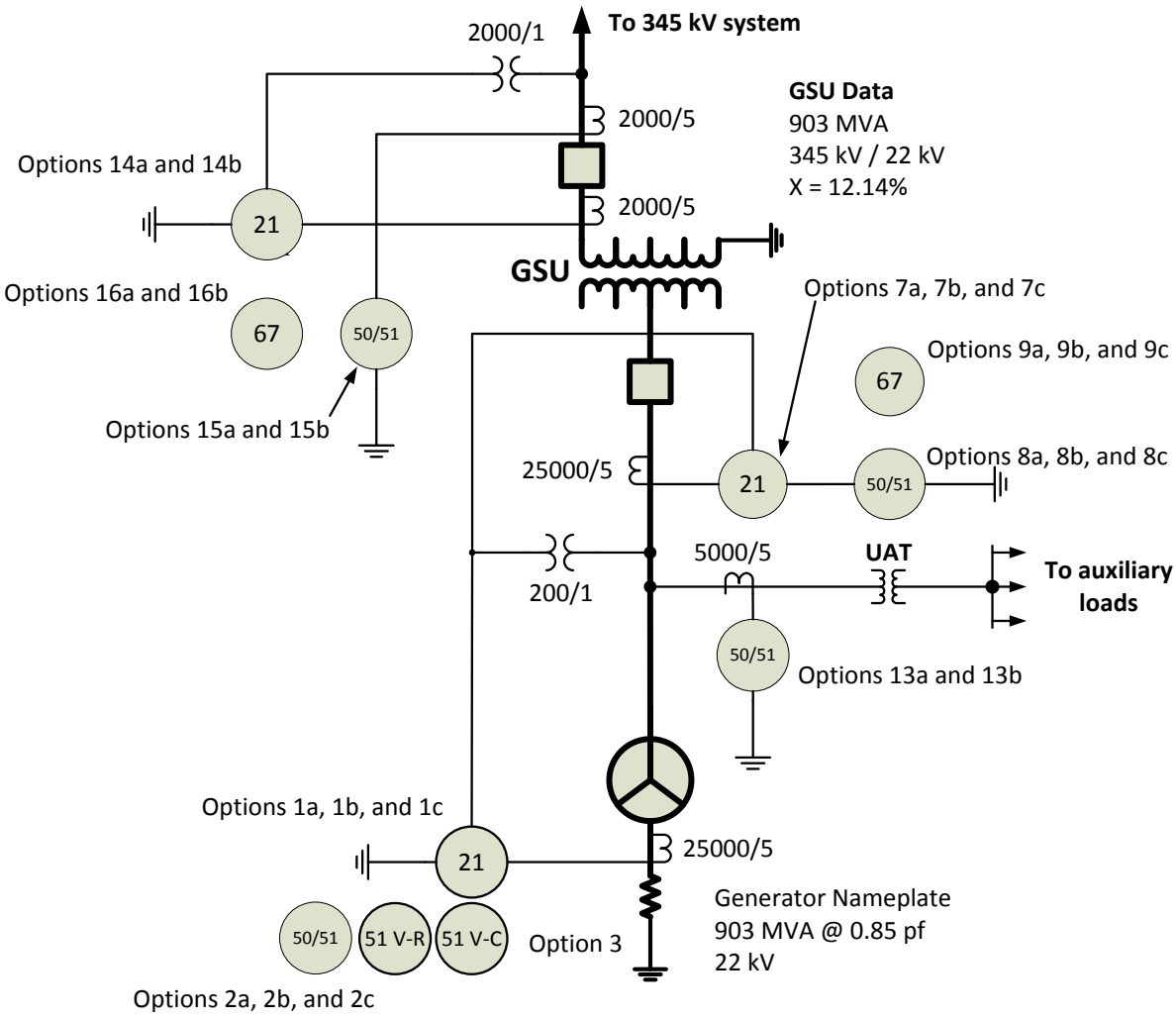


Figure 5: Relay Connection for corresponding synchronous options

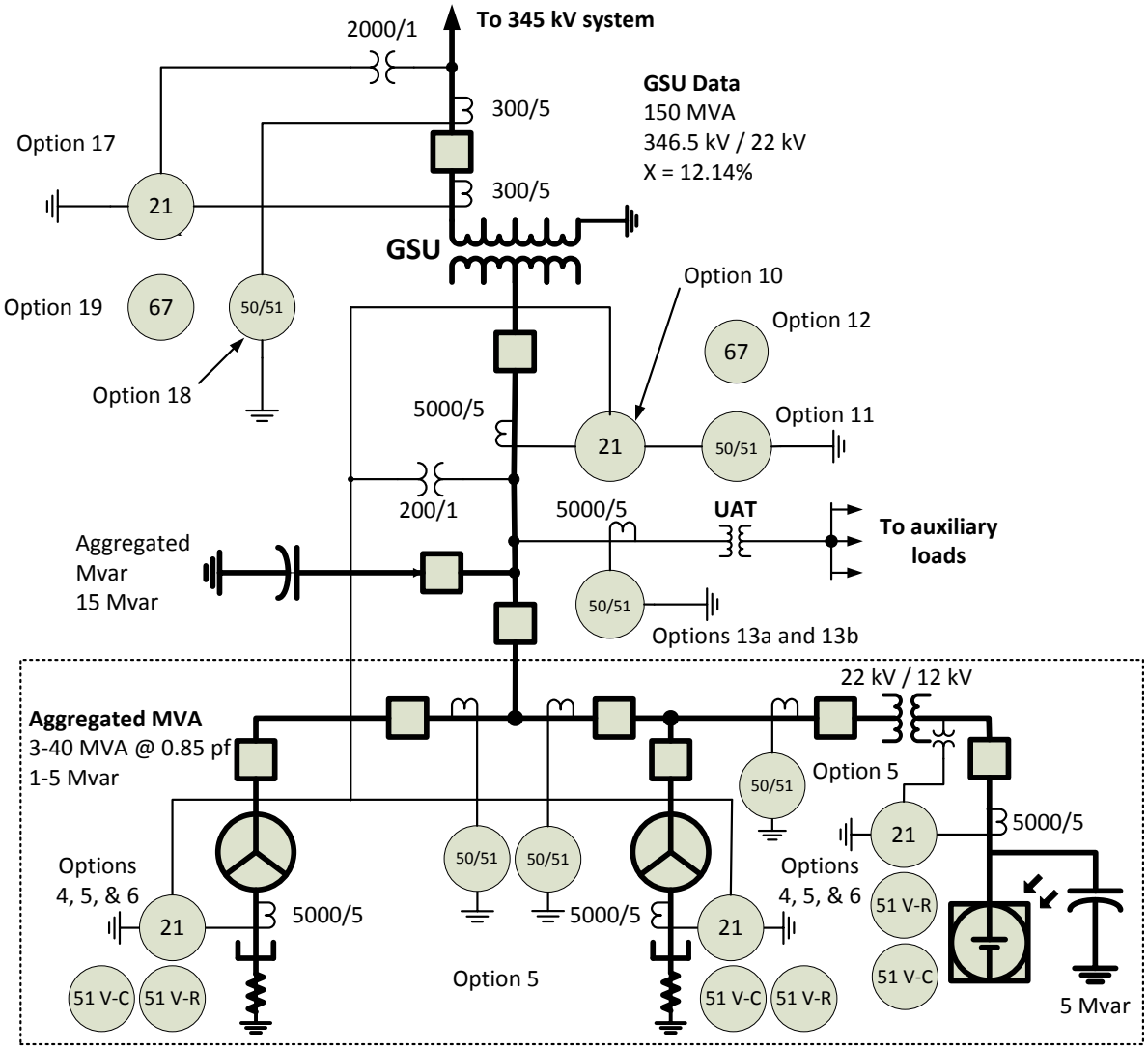


Figure 6: Relay Connection for corresponding asynchronous options including inverter-based installations

Synchronous Generators Phase Distance Relay – Directional Toward Transmission System (e.g., 21) (Options 1a, 1b, and 1c)

Table 1, Options 1a, 1b, and 1c, are provided for assessing loadability for synchronous generators applying phase distance relays that are directional toward the Transmission system. These margins are based on guidance found in Chapter 2 of the Considerations for Power Plant and Transmission System Protection Coordination technical reference document.

Option 1a calculates a generator bus voltage corresponding to 0.95 per unit nominal voltage on the high-side terminals of the GSU transformer. The generator bus voltage is calculated by multiplying the 0.95 per unit nominal voltage, at the high-side terminals of the GSU transformer, by the GSU transformer turns ratio (excluding the impedance). This calculation is a straightforward way to approximate the stressed system conditions.

Option 1b calculates the generator bus voltage corresponding to 0.85 per unit nominal voltage on the high-side terminals of the GSU transformer. The voltage drop across the GSU transformer is calculated based on a 0.85 per unit nominal voltage at the high-side terminals of the GSU transformer as well as the turns ratio and impedance. The actual generator bus voltage may be higher depending on the GSU transformer impedance and the actual Reactive Power achieved. This calculation is a more in-depth and precise method for setting of the impedance element than Option 1a.

Option 1c simulates the generator bus voltage coincident with the highest Reactive Power output achieved during field-forcing. This output is in response to a 0.85 per unit nominal voltage on the high-side terminals of the GSU transformer prior to field-forcing. Using simulation is a more involved, more precise setting of the impedance element overall.

For Options 1a and 1b, the impedance element shall be set less than the calculated impedance derived from 115 percent of both: the Real Power output of 100 percent of the maximum gross MW capability reported to the Transmission Planner, and the Reactive Power output that equates to 150 percent of the MW value, derived from the generator nameplate MVA rating at rated power factor.

For Option 1c, the impedance element shall be set less than the calculated impedance derived from 115 percent of both: the Real Power output of 100 percent of the maximum gross MW capability reported to the Transmission Planner, and the Reactive Power output that equates to 100 percent of the maximum gross Mvar output during field-forcing as determined by simulation.

Synchronous Generators Phase Overcurrent Relay – (e.g., 50, 51, or 51V-R – Voltage Restrained) (Options 2a, 2b, and 2c)

Table 1, Options 2a, 2b, and 2c, are provided for assessing loadability for synchronous generators applying phase overcurrent relays (e.g., 50, 51, or 51V-R – voltage-restrained). These margins are based on guidance found in Chapter 2 of the Considerations for Power Plant and Transmission System Protection Coordination technical reference document.

Option 2a calculates a generator bus voltage corresponding to 0.95 per unit nominal voltage on the high-side terminals of the GSU transformer. The generator bus voltage is calculated by multiplying the 0.95 per unit nominal voltage, at the high-side terminals of the GSU transformer, by the GSU transformer turns ratio (excluding the impedance). This calculation is a straightforward way to approximate the stressed system conditions.

Option 2b calculates the generator bus voltage corresponding to 0.85 per unit nominal voltage on the high-side terminals of the GSU transformer. The voltage drop across the GSU transformer is calculated based on a 0.85 per unit nominal voltage at the high-side terminals of the GSU transformer as well as for the turns ratio and impedance. The actual generator bus voltage may be higher depending on the GSU transformer impedance and the actual Reactive Power achieved. This calculation is a more in-depth and precise method for setting of the overcurrent element than Option 2a.

Option 2c simulates the generator bus voltage coincident with the highest Reactive Power output achieved during field-forcing. This output is in response to a 0.85 per unit nominal voltage on the high-side terminals of the GSU transformer prior to field-forcing. Using simulation is a more involved, more precise setting of the overcurrent element overall.

For Options 2a and 2b, the overcurrent element shall be set greater than 115 percent of the calculated current derived from both: the Real Power output of 100 percent of the maximum gross MW capability reported to the Transmission Planner, and the Reactive Power output that equates to 150 percent of the MW value, derived from the generator nameplate MVA rating at rated power factor.

For Option 2c, the overcurrent element shall be set greater than the calculated current derived from 115 percent of both: the Real Power output of 100 percent of the maximum gross MW capability reported to the Transmission Planner, and the Reactive Power output that equates to 100 percent of the maximum gross Mvar output during field-forcing as determined by simulation.

Synchronous Generators Phase Time Overcurrent Relay – Voltage Controlled (e.g., 51V-C) (Option 3)

Table 1, Option 3, is provided for assessing loadability for synchronous generators applying phase time overcurrent relays which are enabled as a function of voltage ("voltage-controlled"). These margins are based on guidance found in Chapter 2 of the Considerations for Power Plant and Transmission System Protection Coordination technical reference document.

Option 3 calculates the generator bus voltage corresponding to 1.0 per unit nominal voltage on the high-side terminals of the GSU transformer. The generator bus voltage is calculated by multiplying the 1.0 per unit nominal voltage, at the high-side terminals of the GSU transformer, by the GSU transformer turns ratio (excluding the impedance). This is a simple calculation that approximates the stressed system conditions.

For Option 3, the voltage control setting shall be set less than 75 percent of the calculated generator bus voltage. The voltage setting must be set such that the function (e.g., 51V-C) will not trip under extreme emergency conditions as the time overcurrent function will be set less than generator full load current. Relays enabled as a function of voltage are indifferent as to the current setting, and this option simply requires that the relays not respond for the depressed voltage.

Asynchronous Generators Phase Distance Relay – Directional Toward Transmission System (e.g., 21) (Option 4)

Table 1, Option 4 is provided for assessing loadability for asynchronous generators applying phase distance relays that are directional toward the Transmission system. These margins are based on guidance found in Chapter 2 of the Considerations for Power Plant and Transmission System Protection Coordination technical reference document.

Option 4 calculates the generator bus voltage corresponding to 1.0 per unit nominal voltage on the high-side terminals of the GSU transformer. The generator bus voltage is calculated by multiplying the 1.0 per unit nominal voltage, at the high-side terminals of the GSU transformer, by the GSU transformer turns ratio (excluding the impedance). This is a simple calculation that approximates the stressed system conditions.

Since the relay voltage is supplied from the generator bus, it is necessary to assess loadability using the generator-side voltage. Asynchronous generators do not produce as much Reactive Power as synchronous generators; the voltage drop due to Reactive Power flow through the GSU transformer is not as significant. Therefore, the generator bus voltage can be conservatively estimated by reflecting the high-side nominal voltage to the generator-side based on the GSU transformer's turns ratio.

For Option 4, the impedance element shall be set less than the calculated impedance derived from 130 percent of the maximum aggregate nameplate MVA output at rated power factor including the Mvar output of any static or dynamic Reactive Power devices. This is determined by summing the total MW and Mvar capability of the generation equipment behind the relay and any static or dynamic Reactive Power devices that contribute to the power flow through the relay.

Asynchronous Generators Phase Overcurrent Relay – (e.g., 50, 51, or 51V-R – Voltage Restrained) (Options 5a and 5b)

Table 1, Option 5a is provided for assessing loadability for asynchronous generators applying phase overcurrent relays (e.g., 50, 51, or 51V-R – voltage-restrained). These margins are based on guidance found in Chapter 2 of the Considerations for Power Plant and Transmission System Protection Coordination technical reference document.

Option 5a calculates the generator bus voltage corresponding to 1.0 per unit nominal voltage on the high-side terminals of the GSU transformer. The generator bus voltage is calculated by multiplying the 1.0 per unit nominal voltage, at the high-side terminals of the GSU transformer, by the GSU transformer turns ratio (excluding the impedance). This is a simple calculation that approximates the stressed system conditions.

Since the relay voltage is supplied from the generator bus, it is necessary to assess loadability using the generator-side voltage. Asynchronous generators do not produce as much Reactive Power as synchronous generators; the voltage drop due to Reactive Power flow through the GSU transformer is not as significant. Therefore, the generator bus voltage can be conservatively estimated by reflecting the high-side nominal voltage to the generator-side based on the GSU transformer's turns ratio.

For Option 5a, the overcurrent element shall be set greater than 130 percent of the calculated current derived from the maximum aggregate nameplate MVA output at rated power factor including the Mvar output of any static or dynamic Reactive Power devices. This is determined by summing the total MW and Mvar capability of the generation equipment behind the relay and

any static or dynamic Reactive Power devices that contribute to the power flow through the relay.

For Option 5b, the overcurrent element shall be set to exceed the maximum capability of the asynchronous resource and applicable equipment (e.g., windings, power electronics, cables, or bus). This is determined by summing the total current capability of the generation equipment behind the overcurrent element and any static or dynamic Reactive Power devices that contribute to the power flow through the overcurrent element. The lower tolerance of the overcurrent element tripping characteristic shall be set to not infringe upon the resource capability (including the Mvar output of the resource and any static or dynamic reactive power devices). Figure A of PRC-025-2 illustrates that the overcurrent element does not infringe upon the asynchronous resource capability. The upper hashed area of Figure A represents Exclusion 7.

Asynchronous Generator Phase Time Overcurrent Relays – Voltage Controlled (e.g., 51V-C) (Option 6)

Table 1, Option 6, is provided for assessing loadability for asynchronous generators applying phase time overcurrent relays which are enabled as a function of voltage ("voltage-controlled"). These margins are based on guidance found in Chapter 2 of the Considerations for Power Plant and Transmission System Protection Coordination technical reference document.

Option 6 calculates the generator bus voltage corresponding to 1.0 per unit nominal voltage on the high-side terminals of the GSU transformer. The generator bus voltage is calculated by multiplying the 1.0 per unit nominal voltage, at the high-side terminals of the GSU transformer, by the GSU transformer turns ratio (excluding the impedance). This is a simple calculation that approximates the stressed system conditions.

For Option 6, the voltage control setting shall be set less than 75 percent of the calculated generator bus voltage. The voltage setting must be set such that the function (e.g., 51V-C) will not trip under extreme emergency conditions as the time overcurrent function will be set less than generator full load current. Relays enabled as a function of voltage are indifferent as to the current setting, and this option simply requires that the relays not respond for the depressed voltage.

Generator Step-up Transformer (Synchronous Generators) Phase Distance Relays – Directional Toward Transmission System (e.g., 21) (Options 7a, 7b, and 7c)

The Federal Energy Regulatory Commission, in FERC Order No. 733, paragraph 104, directs that NERC address relay loadability for protective relays applied on GSU transformers. These margins are based on guidance found in Chapter 2 of the Considerations for Power Plant and Transmission System Protection Coordination technical reference document.

Table 1, Options 7a, 7b, and 7c, are provided for assessing loadability of phase distance relays that are directional toward the Transmission system and connected to the generator-side of the GSU transformer of a synchronous generator. For applications where the relay is connected on the high-side of the GSU transformer, use Option 14.

Option 7a calculates a generator bus voltage corresponding to 0.95 per unit nominal voltage on the high-side terminals of the GSU transformer. The generator bus voltage is calculated by multiplying the 0.95 per unit nominal voltage, at the high-side terminals of the GSU transformer, by the GSU transformer turns ratio (excluding the impedance). This calculation is a straightforward way to approximate the stressed system conditions.

Option 7b calculates the generator bus voltage corresponding to 0.85 per unit nominal voltage on the high-side terminals of the GSU transformer. The voltage drop across the GSU transformer is calculated based on the 0.85 per unit nominal voltage, at the high-side terminals of the GSU transformer, as well as the turns ratio and impedance. The actual generator bus voltage may be higher depending on the GSU transformer impedance and the actual Reactive Power achieved. This calculation is a more in-depth and precise method for setting the impedance element than Option 7a.

Option 7c simulates the generator bus voltage coincident with the highest Reactive Power output achieved during field-forcing. This output is in response to a 0.85 per unit nominal voltage on the high-side terminals of the GSU transformer prior to field-forcing. Using simulation is a more in-depth and precise method for setting the impedance element than Options 7a or 7b.

For Options 7a and 7b, the impedance element shall be set less than the calculated impedance derived from 115 percent of both: the Real Power output of 100 percent of the aggregate generation MW capability reported to the Transmission Planner, and the Reactive Power output that equates to 150 percent of the aggregate generation MW value (derived from the generator nameplate MVA rating at rated power factor).

For Option 7c, the impedance element shall be set less than the calculated impedance derived from 115 percent of both: the Real Power output of 100 percent of the aggregate generation MW capability reported to the Transmission Planner, and the Reactive Power output that equates to 100 percent of the maximum gross Mvar output during field-forcing as determined by simulation.

Generator Step-up Transformer (Synchronous Generators) Phase Overcurrent Relay (e.g., 50 or 51) (Options 8a, 8b and 8c)

The Federal Energy Regulatory Commission, in FERC Order No. 733, paragraph 104, directs that NERC address relay loadability for protective relays applied on GSU transformers. Note that the setting criteria established within the Table 1 options differ from Chapter 2 of the Considerations for Power Plant and Transmission System Protection Coordination technical reference document. Rather than establishing a uniform loadability threshold of 200 percent of the generator nameplate MVA rating at rated power factor for all applications, the setting criteria are based on the maximum expected generator output.

Table 1, Options 8a, 8b, and 8c, are provided for assessing loadability of phase overcurrent relays that are connected to the generator-side of the GSU transformer of a synchronous generator.

For applications where the relay is connected on the high-side of the GSU transformer, use Option 15.

Option 8a calculates a generator bus voltage corresponding to 0.95 per unit nominal voltage on the high-side terminals of the GSU transformer. The generator bus voltage is calculated by multiplying the 0.95 per unit nominal voltage, at the high-side terminals of the GSU transformer, by the GSU transformer turns ratio (excluding the impedance). This calculation is a straightforward way to approximate the stressed system conditions.

Option 8b calculates the generator bus voltage corresponding to 0.85 per unit nominal voltage on the high-side terminals of the GSU transformer. The voltage drop across the GSU transformer is calculated based on the 0.85 per unit nominal voltage, at the high-side terminals of the GSU transformer, as well as the turns ratio and impedance. The actual generator bus voltage may be higher depending on the GSU transformer impedance and the actual Reactive Power achieved. This calculation is a more in-depth and precise method for setting the overcurrent element than Option 8a.

Option 8c simulates the generator bus voltage coincident with the highest Reactive Power output achieved during field-forcing. This output is in response to a 0.85 per unit nominal voltage on the high-side terminals of the GSU transformer prior to field-forcing. Using simulation is a more in-depth and precise method for setting the overcurrent element than Options 8a or 8b.

For Options 8a and 8b, the overcurrent element shall be set greater than 115 percent of the calculated current derived from both: the Real Power output of 100 percent of the aggregate generation MW capability reported to the Transmission Planner, and the Reactive Power output that equates to 150 percent of the aggregate generation MW value (derived from the generator nameplate MVA rating at rated power factor).

For Option 8c, the overcurrent element shall be set greater than 115 percent of the calculated current derived from both: the Real Power output of 100 percent of the aggregate generation MW capability reported to the Transmission Planner, and the Reactive Power output that equates to 100 percent of the maximum gross Mvar output during field-forcing as determined by simulation.

Generator Step-up Transformer (Synchronous Generators) Phase Directional Overcurrent Relay – Directional Toward Transmission System (e.g., 67) (Options 9a, 9b and 9c)

The Federal Energy Regulatory Commission, in FERC Order No. 733, paragraph 104, directs that NERC address relay loadability for protective relays applied on GSU transformers. Note that the setting criteria established within the Table 1 options differ from Chapter 2 of the Considerations for Power Plant and Transmission System Protection Coordination technical reference document. Rather than establishing a uniform loadability threshold of 200 percent of the generator nameplate MVA rating at rated power factor for all applications, the setting criteria are based on the maximum expected generator output.

Table 1, Options 9a, 9b, and 9c, are provided for assessing loadability of phase directional overcurrent relays directional toward the Transmission System that are connected to the generator-side of the GSU transformer of a synchronous generator. For applications where the relay is connected on the high-side of the GSU transformer, use Option 16.

Option 9a calculates a generator bus voltage corresponding to 0.95 per unit nominal voltage on the high-side terminals of the GSU transformer. The generator bus voltage is calculated by multiplying the 0.95 per unit nominal voltage, at the high-side terminals of the GSU transformer, by the GSU transformer turns ratio (excluding the impedance). This calculation is a straightforward way to approximate the stressed system conditions.

Option 9b calculates the generator bus voltage corresponding to 0.85 per unit nominal voltage on the high-side terminals of the GSU transformer. The voltage drop across the GSU transformer is calculated based on the 0.85 per unit nominal voltage, at the high-side terminals of the GSU transformer, as well as the turns ratio and impedance. The actual generator bus voltage may be higher depending on the GSU transformer impedance and the actual Reactive Power achieved. This calculation is a more in-depth and precise method for setting the overcurrent element than Option 9a.

Option 9c simulates the generator bus voltage coincident with the highest Reactive Power output achieved during field-forcing. This output is in response to a 0.85 per unit nominal voltage on the high-side terminals of the GSU transformer prior to field-forcing. Using simulation is a more in-depth and precise method for setting the overcurrent element than Options 9a or 9b.

For Options 9a and 9b, the overcurrent element shall be set greater than 115 percent of the calculated current derived from both: the Real Power output of 100 percent of the aggregate generation MW capability reported to the Transmission Planner, and the Reactive Power output that equates to 150 percent of the aggregate generation MW value (derived from the generator nameplate MVA rating at rated power factor).

For Option 9c, the overcurrent element shall be set greater than 115 percent of the calculated current derived from both: the Real Power output of 100 percent of the aggregate generation MW capability reported to the Transmission Planner, and the Reactive Power output that equates to 100 percent of the maximum gross Mvar output during field-forcing as determined by simulation.

Generator Step-up Transformer (Asynchronous Generators) Phase Distance Relay – Directional Toward Transmission System (e.g., 21) (Option 10)

The Federal Energy Regulatory Commission, in FERC Order No. 733, paragraph 104, directs that NERC address relay loadability for protective relays applied on GSU transformers. Table 1, Option 10 is provided for assessing loadability for GSU transformers applying phase distance relays that are directional toward the Transmission System that are connected to the generator-side of the GSU transformer of an asynchronous generator. These margins are based on guidance found in Chapter 2 of the Considerations for Power Plant and Transmission System Protection

Coordination technical reference document. For applications where the relay is connected on the high-side of the GSU transformer, use Option 17.

Option 10 calculates the generator bus voltage corresponding to 1.0 per unit nominal voltage on the high-side terminals of the GSU transformer. The generator bus voltage is calculated by multiplying the 1.0 per unit nominal voltage, at the high-side terminals of the GSU transformer, by the GSU transformer turns ratio (excluding the impedance). This calculation is a straightforward way to approximate the stressed system conditions.

Since the relay voltage is supplied from the generator bus, it is necessary to assess loadability using the generator-side voltage. Asynchronous generators do not produce as much Reactive Power as synchronous generators; hence the voltage drop due to Reactive Power flow through the GSU transformer is not as significant. Therefore, the generator bus voltage can be conservatively estimated by reflecting the high-side nominal voltage to the generator-side based on the GSU transformer's turns ratio.

For Option 10, the impedance element shall be set less than the calculated impedance, derived from 130 percent of the maximum aggregate nameplate MVA output at rated power factor, including the Mvar output of any static or dynamic Reactive Power devices. This is determined by summing the total MW and Mvar capability of the generation equipment behind the relay and any static or dynamic Reactive Power devices that contribute to the power flow through the relay.

Generator Step-up Transformer (Asynchronous Generators) Phase Overcurrent Relay (e.g., 50 or 51) (Option 11)

The Federal Energy Regulatory Commission, in FERC Order No. 733, paragraph 104, directs that NERC address relay loadability for protective relays applied on GSU transformers. Note that the setting criteria established within the Table 1 options differ from Chapter 2 of the Considerations for Power Plant and Transmission System Protection Coordination technical reference document. Rather than establishing a uniform loadability threshold of 200 percent of the generator nameplate MVA rating at rated power factor for all applications, the setting criteria are based on the maximum expected generator output.

Table 1, Option 11 is provided for assessing loadability of phase overcurrent relays that are connected to the generator-side of the GSU transformer of an asynchronous generator. For applications where the relay is connected on the high-side of the GSU transformer, use Option 18.

Option 11 calculates the generator bus voltage corresponding to 1.0 per unit nominal voltage on the high-side terminals of the GSU transformer. The generator bus voltage is calculated by multiplying the 1.0 per unit nominal voltage, at the high-side terminals of the GSU transformer, by the GSU transformer turns ratio (excluding the impedance). This calculation is a straightforward way to approximate the stressed system conditions.

Since the relay current is supplied from the generator bus, it is necessary to assess loadability using the generator-side voltage. Asynchronous generators do not produce as much Reactive Power as synchronous generators; hence the voltage drop due to Reactive Power flow through the GSU transformer is not as significant. Therefore, the generator bus voltage can be conservatively estimated by reflecting the high-side nominal voltage to the generator-side based on the GSU transformer's turns ratio.

For Option 11, the overcurrent element shall be set greater than 130 percent of the calculated current derived from the maximum aggregate nameplate MVA output at rated power factor, including the Mvar output of any static or dynamic Reactive Power devices. This is determined by summing the total MW and Mvar capability of the generation equipment behind the relay and any static or dynamic Reactive Power devices that contribute to the power flow through the relay.

Generator Step-up Transformer (Asynchronous Generators) Phase Directional Overcurrent Relay – Directional Toward Transmission System (e.g., 67) (Option 12)

The Federal Energy Regulatory Commission, in FERC Order No. 733, paragraph 104, directs that NERC address relay loadability for protective relays applied on GSU transformers. Note that the setting criteria established within the Table 1 options differ from Chapter 2 of the Considerations for Power Plant and Transmission System Protection Coordination technical reference document. Rather than establishing a uniform loadability threshold of 200 percent of the generator nameplate MVA rating at rated power factor for all applications, the setting criteria are based on the maximum expected generator output.

Table 1, Option 12 is provided for assessing loadability of phase directional overcurrent relays directional toward the Transmission System that are connected to the generator-side of the GSU transformer of an asynchronous generator. For applications where the relay is connected on the high-side of the GSU transformer, use Option 19.

Option 12 calculates the generator bus voltage corresponding to 1.0 per unit nominal voltage on the high-side terminals of the GSU transformer. The generator bus voltage is calculated by multiplying the 1.0 per unit nominal voltage, at the high-side terminals of the GSU transformer, by the GSU transformer turns ratio (excluding the impedance). This calculation is a straightforward way to approximate the stressed system conditions.

Since the relay current is supplied from the generator bus, it is necessary to assess loadability using the generator-side voltage. Asynchronous generators do not produce as much Reactive Power as synchronous generators; hence the voltage drop due to Reactive Power flow through the GSU transformer is not as significant. Therefore, the generator bus voltage can be conservatively estimated by reflecting the high-side nominal voltage to the generator-side based on the GSU transformer's turns ratio.

For Option 12, the overcurrent element shall be set greater than 130 percent of the calculated current derived from the maximum aggregate nameplate MVA output at rated power factor,

including the Mvar output of any static or dynamic Reactive Power devices. This is determined by summing the total MW and Mvar capability of the generation equipment behind the relay and any static or dynamic Reactive Power devices that contribute to the power flow through the relay.

Unit Auxiliary Transformers Phase Overcurrent Relay (e.g., 50 or 51) (Options 13a and 13b)

In FERC Order No. 733, paragraph 104, directs NERC to include in this standard a loadability requirement for relays used for overload protection of the UAT that supply normal station service for a generating unit. For the purposes of this standard, UATs provide the overall station power to support the unit at its maximum gross operation.

Table 1, Options 13a and 13b provide two options for addressing phase overcurrent relaying applied at the high-side of UATs. The transformer high-side winding may be directly connected to the transmission grid or at the generator isolated phase bus (IPB) or iso-phase bus. Phase overcurrent relays applied at the high-side of the UAT that remove the transformer from service resulting in an immediate (e.g., via lockout or auxiliary tripping relay operation) or consequential trip of the associated generator are to be compliant with the relay setting criteria in this standard. Due to the complexity of the application of low-side overload relays for single or multi-winding transformers, phase overcurrent relaying applied at the low-side of the UAT are not addressed in this standard. The NERC System Protection and Control Subcommittee addressed low-side UAT protection in the document called “Unit Auxiliary Transformer Overcurrent Relay Loadability During a Transmission Depressed Voltage Condition, March 2016.” These relays include, but are not limited to, a relay used for arc flash protection, feeder protection relays, breaker failure, and relays whose operation may result in a generator runback.

Refer to the Figures 7 and 8 below for example configurations:

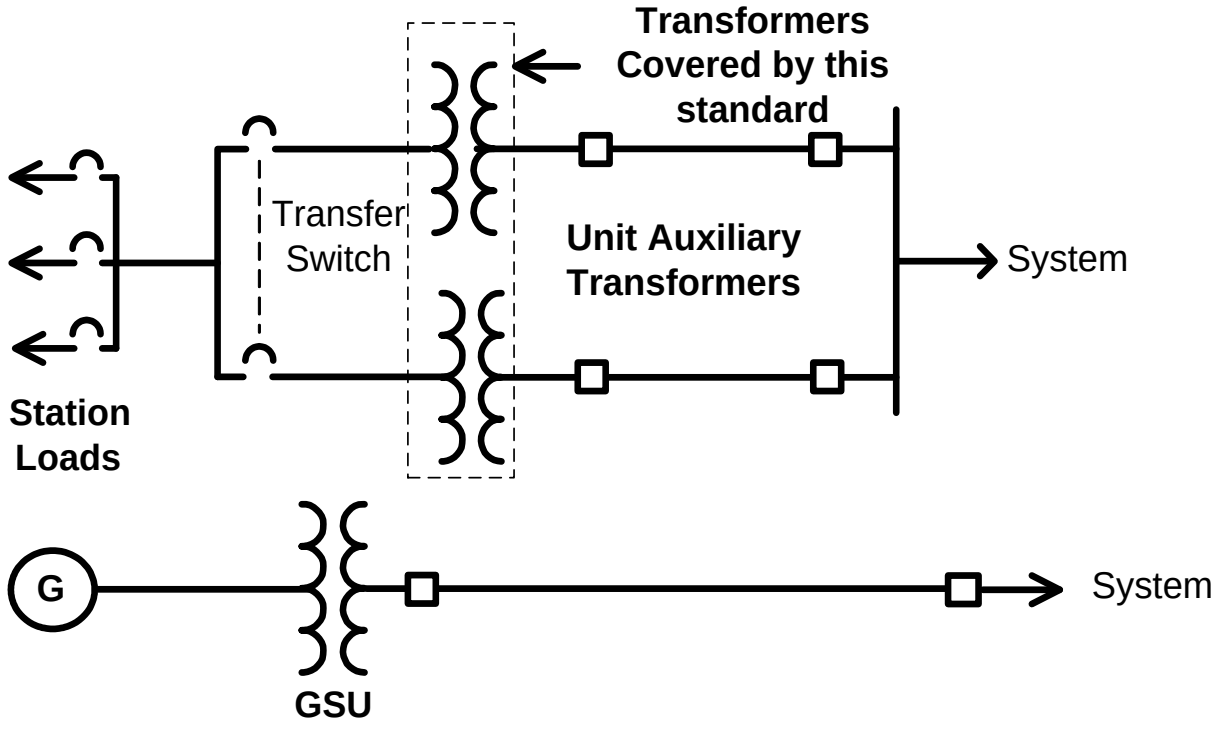


Figure 7: Auxiliary Power System (independent from generator)

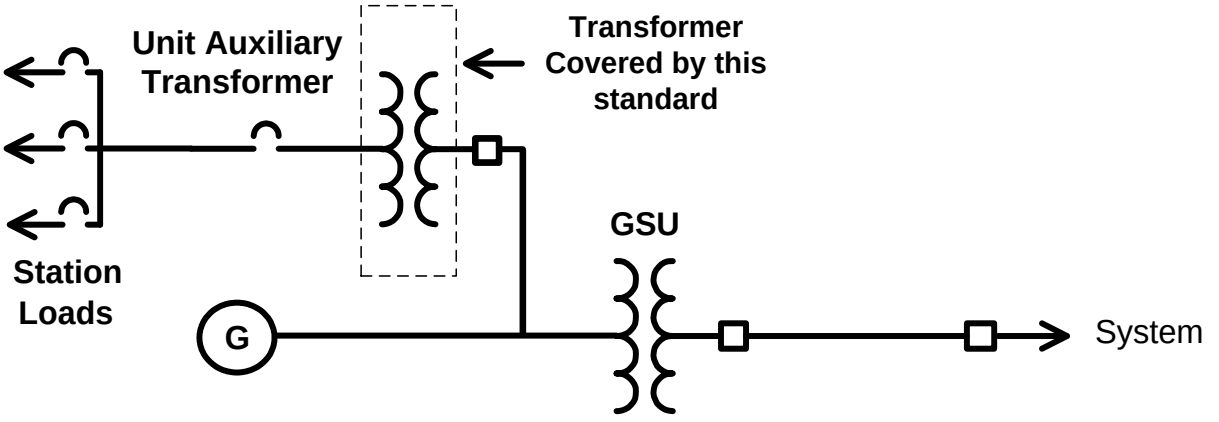


Figure 8: Typical auxiliary power system for generation units or plants

The UATs supplying power to the unit or plant electrical auxiliaries are sized to accommodate the maximum expected overall UAT load demand at the highest generator output. Although the transformer nameplate MVA size normally includes capacity for future loads as well as capacity

for starting of large induction motors on the original unit or plant design, the nameplate MVA capacity of the transformer may be near full load.

Because of the various design and loading characteristics of UATs, two options (i.e., 13a and 13b) are provided to accommodate an entity's protection philosophy while preventing the UAT transformer phase overcurrent relays from operating during the dynamic conditions anticipated by this standard.

Options 13a and 13b are based on the transformer bus voltage corresponding to 1.0 per unit nominal voltage on the high-side winding of the UAT.

For Option 13a, the overcurrent element shall be set greater than 150 percent of the calculated current derived from the UAT maximum nameplate MVA rating. This is a simple calculation that approximates the stressed system conditions.

For Option 13b, the overcurrent element shall be set greater than 150 percent of the UAT measured current at the generator maximum gross MW capability reported to the Transmission Planner. This allows for a reduced setting compared to Option 13a and the relay setting philosophy of the applicable entity. This is a more involved calculation that approximates the stressed system conditions by allowing the entity to consider the actual load placed on the UAT based on the generator's maximum gross MW capability reported to the Transmission Planner.

The performance of the UAT loads during stressed system conditions (i.e., depressed voltages) is very difficult to determine. Rather than requiring responsible entities to determine the response of UAT loads to depressed voltage, the technical experts writing the standard elected to increase the margin to 150 percent from that used elsewhere in this standard (e.g., 115 percent) and use a generator bus voltage of 1.0 per unit. A minimum setting current based on 150 percent of maximum transformer nameplate MVA rating at 1.0 per unit generator bus voltage will provide adequate transformer protection based on IEEE C37.91 at full load conditions while providing sufficient relay loadability to prevent a trip of the UAT, and subsequent unit trip, due to increased UAT load current during stressed system voltage conditions. Even if the UAT is equipped with an automatic tap changer, the tap changer may not respond quickly enough for the conditions anticipated within this standard, and thus shall not be used to reduce this margin.

Elements that connect a GSU transformer to the Transmission system that are used exclusively to export energy directly from a BES generating unit or generating plant (Synchronous Generators) Phase Distance Relays – Directional Toward Transmission System (e.g., 21) (Options 14a and 14b)

Relays applied on Elements that connect a GSU transformer to the Transmission system that are used exclusively to export energy directly from a BES generating unit or generating plant are challenged by loading conditions similar to relays applied on generators and GSU transformers. These margins are based on guidance found in Chapter 2 of the Considerations for Power Plant and Transmission System Protection Coordination technical reference document. Relays applied on the high-side of the GSU transformer respond to the same quantities as the relays applied at

the remote end of the line for Elements that connect a GSU transformer to the Transmission system that are used exclusively to export energy directly from a BES generating unit or generating plant, thus Option 14 is used for these relays as well.

Table 1, Options 14a and 14b, establish criteria for phase distance relays directional toward the Transmission system to prevent Elements that connect a GSU transformer to the Transmission system that are used exclusively to export energy directly from a BES generating unit or generating plant from tripping during the dynamic conditions anticipated by this standard. The stressed system conditions, anticipated by Option 14a reflects a 0.85 per unit of the line nominal voltage; therefore, establishing that the impedance value used for applying the Elements that connect a GSU transformer to the Transmission system that are used exclusively to export energy directly from a BES generating unit or generating plant phase distance relays that are directional toward the Transmission system be calculated from the apparent power addressed within the criteria, with application of a 0.85 per unit of the line nominal voltage at the relay location. Consideration of the voltage drop across the GSU transformer is not necessary. Option 14b simulates the line voltage coincident with the highest Reactive Power output achieved during field-forcing in response to a 0.85 per unit line nominal voltage at the remote end of the line prior to field-forcing. Using a 0.85 per unit line nominal voltage at the remote end of the line is representative of the lowest voltage expected during a depressed voltage condition on Elements that are used exclusively to export energy directly from a BES generating unit or generating plant to the Transmission system. Using simulation is a more involved, more precise setting of the overcurrent element overall.

For Option 14a, the impedance element shall be set less than the calculated impedance derived from 115 percent of both: the Real Power output of 100 percent of the aggregate generation MW capability reported to the Transmission Planner, and the Reactive Power output that equates to 120 percent of the aggregate generation MW value, derived from the generator nameplate MVA rating at rated power factor. This Reactive Power value differs from the 150 percent multiplier used in other applications to account for the Reactive Power losses in the GSU transformer. This is a simple calculation that approximates the stressed system conditions.

For Option 14b, the impedance element shall be set less than the calculated impedance derived from 115 percent of both: the Real Power output of 100 percent of the aggregate generation MW capability reported to the Transmission Planner, and the Reactive Power output that equates to 100 percent of the maximum gross Mvar output during field-forcing as determined by simulation. Option 14b uses the simulated line voltage at the relay location coincident with the highest Reactive Power output achieved during field-forcing in response to a 0.85 per unit of the line nominal voltage at the remote end of the line prior to field-forcing. Using simulation is a more involved, more precise setting of the impedance element overall.

Elements that connect a GSU transformer to the Transmission system that are used exclusively to export energy directly from a BES generating unit or generating plant (Synchronous Generators) Phase Time Overcurrent Relay (e.g., 50 or 51) (Options 15a and 15b)

Relays applied on Elements that connect a GSU transformer to the Transmission system that are used exclusively to export energy directly from a BES generating unit or generating plant are challenged by loading conditions similar to relays applied on generators and GSU transformers. Note that the setting criteria established within the Table 1 options differ from Chapter 2 of the Considerations for Power Plant and Transmission System Protection Coordination technical reference document. Rather than establishing a uniform setting threshold of 200 percent of the generator nameplate MVA rating at rated power factor for all applications, the setting criteria are based on the maximum expected generator output. Relays applied on the high-side of the GSU transformer respond to the same quantities as the relays applied at the remote end of the line for Elements that connect a GSU transformer to the Transmission system that are used exclusively to export energy directly from a BES generating unit or generating plant, thus Option 15 is used for these relays as well.

Table 1, Options 15a and 15b, establish criteria for phase instantaneous and/or time overcurrent relays to prevent Elements that connect a GSU transformer to the Transmission system that are used exclusively to export energy directly from a BES generating unit or generating plant from tripping during the dynamic conditions anticipated by this standard. The stressed system conditions, anticipated by Option 15a reflects a 0.85 per unit of the line nominal voltage at the relay location; therefore, establishing that the current value used for applying the Elements that connect a GSU transformer to the Transmission system that are used exclusively to export energy directly from a BES generating unit or generating plant phase instantaneous and/or time overcurrent relays be calculated from the apparent power addressed within the criteria, with application of a 0.85 per unit of the line nominal voltage at the relay location. Consideration of the voltage drop across the GSU transformer is not necessary. Option 15b simulates the line voltage coincident with the highest Reactive Power output achieved during field-forcing in response to a 0.85 per unit line nominal voltage at the remote end of the line prior to field-forcing. Using a 0.85 per unit line nominal voltage at the remote end of the line is representative of the lowest voltage expected during a depressed voltage condition on Elements that are used exclusively to export energy directly from a BES generating unit or generating plant to the Transmission system. Using simulation is a more involved, more precise setting of the overcurrent element overall.

For Option 15a, the overcurrent element shall be set greater than 115 percent of the calculated current derived from both: the Real Power output of 100 percent of the aggregate generation MW capability reported to the Transmission Planner, and the Reactive Power output that equates to 120 percent of the aggregate generation MW value, derived from the generator nameplate MVA rating at rated power factor. This Reactive Power value differs from the 150 percent multiplier used in other applications to account for the Reactive Power losses in the GSU transformer. This is a simple calculation that approximates the stressed system conditions.

For Option 15b, the overcurrent element shall be set greater than 115 percent of the calculated current derived from both: the Real Power output of 100 percent of the aggregate generation MW capability reported to the Transmission Planner, and the Reactive Power output that equates to 100 percent of the maximum gross Mvar output during field-forcing as determined by simulation. Option 15b uses the simulated line voltage at the relay location coincident with the highest Reactive Power output achieved during field-forcing in response to a 0.85 per unit of the line nominal voltage at the remote end of the line prior to field-forcing. Using simulation is a more involved, more precise setting of the overcurrent element overall.

Elements that connect a GSU transformer to the Transmission system that are used exclusively to export energy directly from a BES generating unit or generating plant (Synchronous Generators) Phase Directional Overcurrent Relay – Directional Toward Transmission System (e.g., 67) (Options 16a and 16b)

Relays applied on Elements that connect a GSU transformer to the Transmission system that are used exclusively to export energy directly from a BES generating unit or generating plant are challenged by loading conditions similar to relays applied on generators and GSU transformers. Note that the setting criteria established within the Table 1 options differ from Chapter 2 of the Considerations for Power Plant and Transmission System Protection Coordination technical reference document. Rather than establishing a uniform setting threshold of 200 percent of the generator nameplate MVA rating at rated power factor for all applications, the setting criteria are based on the maximum expected generator output. Relays applied on the high-side of the GSU transformer respond to the same quantities as the relays applied at the remote end of the line for Elements that connect a GSU transformer to the Transmission system that are used exclusively to export energy directly from a BES generating unit or generating plant, thus Option 16 is used for these relays as well.

Table 1, Options 16a and 16b, establish criteria for phase directional overcurrent relays that are directional toward the Transmission system to prevent Elements that connect a GSU transformer to the Transmission system that are used exclusively to export energy directly from a BES generating unit or generating plant from tripping during the dynamic conditions anticipated by this standard. The stressed system conditions, anticipated by Option 16a reflects a 0.85 per unit of the line nominal voltage at the relay location; therefore, establishing that the current value used for applying the interconnection Facilities phase directional overcurrent relays be calculated from the apparent power addressed within the criteria, with application of a 0.85 per unit of the line nominal voltage at the relay location. Consideration of the voltage drop across the GSU transformer is not necessary. Option 16b simulates the line voltage coincident with the highest Reactive Power output achieved during field-forcing in response to a 0.85 per unit line nominal voltage at the remote end of the line prior to field-forcing. Using a 0.85 per unit line nominal voltage at the remote end of the line is representative of the lowest voltage expected during a depressed voltage condition on Elements that are used exclusively to export energy directly from a BES generating unit or generating plant to the Transmission system. Using simulation is a more involved, more precise setting of the overcurrent element overall.

For Option 16a, the overcurrent element shall be set greater than 115 percent of the calculated current derived from both: the Real Power output of 100 percent of the aggregate generation MW capability reported to the Transmission Planner, and the Reactive Power output that equates to 120 percent of the aggregate generation MW value, derived from the generator nameplate MVA rating at rated power factor. This Reactive Power value differs from the 150 percent multiplier used in other applications to account for the Reactive Power losses in the GSU transformer. This is a simple calculation that approximates the stressed system conditions.

For Option 16b, the overcurrent element shall be set greater than 115 percent of the calculated current derived from both: the Real Power output of 100 percent of the aggregate generation MW capability reported to the Transmission Planner, and the Reactive Power output that equates to 100 percent of the maximum gross Mvar output during field-forcing as determined by simulation. Option 16b uses the simulated line voltage at the relay location coincident with the highest Reactive Power output achieved during field-forcing in response to a 0.85 per unit of the line nominal voltage at the remote end of the line prior to field-forcing. Using simulation is a more involved, more precise setting of the overcurrent element overall.

Elements that connect a GSU transformer to the Transmission system that are used exclusively to export energy directly from a BES generating unit or generating plant (Asynchronous Generators) Phase Distance Relay – Directional Toward Transmission System (e.g., 21) (Option 17)

Relays installed on the high-side of the GSU transformer, including relays installed on the remote end of the line, for Elements that connect a GSU transformer to the Transmission system that are used exclusively to export energy directly from a BES generating unit or generating plant are challenged by loading conditions similar to relays applied on generators and GSU transformers. These margins are based on guidance found in Chapter 2 of the Considerations for Power Plant and Transmission System Protection Coordination technical reference document.

Table 1, Option 17 establishes criteria for phase distance relays that are directional toward the Transmission system to prevent Elements that connect a GSU transformer to the Transmission system that are used exclusively to export energy directly from a BES generating unit or generating plant from tripping during the dynamic conditions anticipated by this standard. Option 17 applies a 1.0 per unit line nominal voltage at the relay location to calculate the impedance from the maximum aggregate nameplate MVA.

For Option 17, the impedance element shall be set less than the calculated impedance derived from 130 percent of the maximum aggregate nameplate MVA output at rated power factor including the Mvar output of any static or dynamic Reactive Power devices. This is determined by summing the total MW and Mvar capability of the generation equipment behind the relay and any static or dynamic Reactive Power devices that contribute to the power flow through the relay. This is a simple calculation that approximates the stressed system conditions.

Elements that connect a GSU transformer to the Transmission system that are used exclusively to export energy directly from a BES generating unit or generating plant (Asynchronous Generators) Phase Overcurrent Relay (e.g., 50 and 51) (Option 18)

Relays installed on the high-side of the GSU transformer, including relays installed on the remote end of the line, for Elements that connect a GSU transformer to the Transmission system that are used exclusively to export energy directly from a BES generating unit or generating plant are challenged by loading conditions similar to relays applied on generators and GSU transformers. Note that the setting criteria established within the Table 1 options differ from Chapter 2 of the Considerations for Power Plant and Transmission System Protection Coordination technical reference document. Rather than establishing a uniform setting threshold of 200 percent of the generator nameplate MVA rating at rated power factor for all applications, the setting criteria are based on the maximum expected generator output.

Table 1, Option 18 establishes criteria for phase overcurrent relays to prevent Elements that connect a GSU transformer to the Transmission system that are used exclusively to export energy directly from a BES generating unit or generating plant from tripping during the dynamic conditions anticipated by this standard. Option 18 applies a 1.0 per unit line nominal voltage at the location of the relay to calculate the current from the maximum aggregate nameplate MVA.

For Option 18, the overcurrent element shall be set greater than 130 percent of the calculated current derived from the maximum aggregate nameplate MVA output at rated power factor including the Mvar output of any static or dynamic Reactive Power devices. This is determined by summing the total MW and Mvar capability of the generation equipment behind the relay and any static or dynamic Reactive Power devices that contribute to the power flow through the relay. This is a simple calculation that approximates the stressed system conditions.

Elements that connect a GSU transformer to the Transmission system that are used exclusively to export energy directly from a BES generating unit or generating plant (Asynchronous Generators) Phase Directional Overcurrent Relay – Directional Toward Transmission System (e.g., 67) (Option 19)

Relays installed on the high-side of the GSU transformer, including relays installed on the remote end of the line, for Elements that connect a GSU transformer to the Transmission system that are used exclusively to export energy directly from a BES generating unit or generating plant are challenged by loading conditions similar to relays applied on generators and GSU transformers. Note that the setting criteria established within the Table 1 options differ from Chapter 2 of the Considerations for Power Plant and Transmission System Protection Coordination technical reference document. Rather than establishing a uniform setting threshold of 200 percent of the generator nameplate MVA rating at rated power factor for all applications, the setting criteria are based on the maximum expected generator output.

Table 1, Option 19 establishes criteria for phase directional overcurrent relays that are directional toward the Transmission system to prevent Elements that connect a GSU transformer to the Transmission system that are used exclusively to export energy directly from a BES generating unit or generating plant from tripping during the dynamic conditions anticipated by this standard.

Option 19 applies a 1.0 per unit line nominal voltage at the relay location to calculate the current from the maximum aggregate nameplate MVA.

For Option 19, the overcurrent element shall be set greater than 130 percent of the calculated current derived from the maximum aggregate nameplate MVA output at rated power factor including the Mvar output of any static or dynamic Reactive Power devices. This is determined by summing the total MW and Mvar capability of the generation equipment behind the relay and any static or dynamic Reactive Power devices that contribute to the power flow through the relay. This is a simple calculation that approximates the stressed system conditions.

Example Calculations

Introduction

Example Calculations	
Input Descriptions	**Input Values**
Synchronous Generator nameplate (MVA @ rated pf):	$GEN_{Synch_nameplate} = 903\ MVA$
	$pf = 0.85$
Generator rated voltage (Line-to-Line):	$V_{gen_nom} = 22\ kV$
Real Power output in MW as reported to the TP:	$P_{Synch_reported} = 700.0\ MW$
Generator step-up (GSU) transformer rating:	$MVA_{GSU} = 903\ MVA$
GSU transformer reactance (903 MVA base):	$X_{GSU} = 12.14\%$
GSU transformer MVA base:	$MVA_{base} = 767.6\ MVA$
GSU transformer turns ratio:	$GSU_{ratio} = \frac{22\ kV}{346.5\ kV}$
High-side nominal system voltage (Line-to-Line):	$V_{nom} = 345\ kV$
Current transformer (CT) ratio:	$CT_{ratio} = \frac{25000}{5}$
Potential transformer (PT) ratio low-side:	$PT_{ratio} = \frac{200}{1}$
PT ratio high-side:	$PT_{ratio_hv} = \frac{2000}{1}$
Unit auxiliary transformer (UAT) nameplate:	$UAT_{nameplate} = 60\ MVA$
UAT high-side voltage:	$V_{UAT} = 13.8\ kV$
UAT CT ratio:	$CT_{UAT} = \frac{5000}{5}$
CT high voltage ratio:	$CT_{ratio_hv} = \frac{2000}{5}$
Reactive Power output of static reactive device:	$MVAR_{static} = 15\ Mvar$

Example Calculations	
Reactive Power output of static reactive device generation:	$MVAR_{gen_static} = 5\ Mvar$
Asynchronous generator nameplate (MVA @ rated pf):	$GEN_{Asynch_nameplate} = 40\ MVA$
	$pf = 0.85$
Asynchronous CT ratio:	$CT_{Asynch_ratio} = \frac{5000}{5}$
Asynchronous high voltage CT ratio:	$CT_{Asynch_ratio_hv} = \frac{300}{5}$
CT remote substation bus	$CT_{ratio_remote_bus} = \frac{2000}{5}$

Example Calculations: Option 1a

Option 1a represents the simplest calculation for synchronous generators applying a phase distance relay (e.g., 21) directional toward the Transmission system.

Real Power output (P):

Eq. (1) $P = GEN_{Synch_nameplate} \times pf$

$P = 903\ MVA \times 0.85$

$P = 767.6\ MW$

Reactive Power output (Q):

Eq. (2) $Q = 150\% \times P$

$Q = 1.50 \times 767.6\ MW$

$Q = 1151.3\ Mvar$

Option 1a, Table 1 – Bus Voltage, calls for a 0.95 per unit of the high-side nominal voltage for the generator bus voltage (V_{gen}):

Eq. (3) $V_{gen} = 0.95\ p.u. \times V_{nom} \times GSU_{ratio}$

$V_{gen} = 0.95 \times 345\ kV \times \left(\frac{22\ kV}{346.5\ kV}\right)$

$V_{gen} = 20.81\ kV$

Apparent power (S):

Eq. (4) $S = P_{Synch_reported} + jQ$

$S = 700.0\ MW + j1151.3\ Mvar$

$S = 1347.4\angle 58.7°\ MVA$

Primary impedance (Z_{pri}):

Eq. (5) $Z_{pri} = \frac{V_{gen}^2}{S^*}$

$Z_{pri} = \frac{(20.81\ kV)^2}{1347.4\angle -58.7°\ MVA}$

Example Calculations: Option 1a

$$Z_{pri} = 0.321\angle 58.7° \ \Omega$$

Secondary impedance (Z_{sec}):

Eq. (6) $$Z_{sec} = Z_{pri} \times \frac{CT_{ratio}}{PT_{ratio}}$$

$$Z_{sec} = 0.321\angle 58.7° \ \Omega \times \frac{\frac{25000}{5}}{\frac{200}{1}}$$

$$Z_{sec} = 0.321\angle 58.7° \ \Omega \times 25$$

$$Z_{sec} = 8.035\angle 58.7° \ \Omega$$

To satisfy the 115% margin in Option 1a:

Eq. (7) $$Z_{\text{sec}\,limit} = \frac{Z_{sec}}{115\%}$$

$$Z_{\text{sec}\,limit} = \frac{8.035\angle 58.7° \ \Omega}{1.15}$$

$$Z_{\text{sec}\,limit} = 6.9873\angle 58.7° \ \Omega$$

$$\theta_{transient\ load\ angle} = 58.7°$$

Assume a Mho distance impedance relay with a maximum torque angle (MTA) set at 85°, then the maximum allowable impedance reach is:

Eq. (8) $$Z_{max} < \frac{|Z_{\text{sec}\,limit}|}{\cos(\theta_{MTA} - \theta_{transient\ load\ angle})}$$

$$Z_{max} < \frac{6.9873 \ \Omega}{\cos(85.0° - 58.7°)}$$

$$Z_{max} < \frac{6.9873 \ \Omega}{0.896}$$

$$Z_{max} < \ 7.793\angle 85.0° \ \Omega$$

Example Calculations: Options 1b and 7b

Option 1b represents a more complex, more precise calculation for synchronous generators applying a phase distance relay (e.g., 21) directional toward the Transmission system. This option requires calculating low-side voltage taking into account voltage drop across the GSU transformer. Similarly these calculations may be applied to Option 7b for GSU transformers applying a phase distance relay (e.g., 21) directional toward the Transmission system.

Real Power output (P):

Eq. (9) $$P = GEN_{Synch_nameplate} \times pf$$

$$P = 903\ MVA \times 0.85$$

$$P = 767.6\ MW$$

Reactive Power output (Q):

Eq. (10) $$Q = 150\% \times P$$

$$Q = 1.50 \times 767.6\ MW$$

$$Q = 1151.3\ Mvar$$

Convert Real Power, Reactive Power, and transformer reactance to per unit values on a 767.6 MVA base (MVA_{base}):

Real Power output (P):

Eq. (11) $$P_{pu} = \frac{P_{Synch_reported}}{MVA_{base}}$$

$$P_{pu} = \frac{700.0\ MW}{767.6\ MVA}$$

$$P_{pu} = 0.91\ p.u.$$

Reactive Power output (Q):

Eq. (12) $$Q_{pu} = \frac{Q}{MVA_{base}}$$

$$Q_{pu} = \frac{1151.3\ Mvar}{767.6\ MVA}$$

$$Q_{pu} = 1.5\ p.u.$$

Example Calculations: Options 1b and 7b

Transformer impedance (X_{pu}):

Eq. (13) $$X_{pu} = X_{GSU(old)} \times \left(\frac{MVA_{base}}{MVA_{GSU}}\right)$$

$$X_{pu} = 12.14\% \times \left(\frac{767.6\ MVA}{903\ MVA}\right)$$

$$X_{pu} = 0.1032\ p.u.$$

Using the formula below; calculate the low-side GSU transformer voltage ($V_{low\text{-}side}$) using 0.85 p.u. high-side voltage ($V_{high\text{-}side}$). Assume initial low-side voltage to be 0.95 p.u. and repeat the calculation as necessary until $V_{low\text{-}side}$ converges. A convergence of less than one percent (<1%) between iterations is considered sufficient:

Eq. (14) $$\theta_{low-side} = \sin^{-1}\left[\frac{\left(P_{pu} \times |X_{pu}|\right)}{\left(|V_{low-side}| \times \left[V_{high-side}\right]\right)}\right]$$

$$\theta_{low-side} = \sin^{-1}\left[\frac{(0.91 \times 0.1032)}{(0.95 \times 0.85)}\right]$$

$$\theta_{low-side} = 6.7°$$

Eq. (15)

$$|V_{low-side}| = \frac{|V_{high-side}| \times \cos(\theta_{low-side}) \pm \sqrt{|V_{high-side}|^2 \times \cos^2(\theta_{low-side}) + 4 \times Q_{pu} \times X_{pu}}}{2}$$

$$|V_{low-side}| = \frac{|0.85| \times \cos(6.7°) \pm \sqrt{|0.85|^2 \times \cos^2(6.7°) + 4 \times 1.5 \times 0.1032}}{2}$$

$$|V_{low-side}| = \frac{|0.85| \times 0.9931 \pm \sqrt{0.7225 \times 0.9864 + 0.6192}}{2}$$

$$|V_{low-side}| = \frac{0.8441 \pm 1.1541}{2}$$

$$|V_{low-side}| = 0.9991\ p.u.$$

Example Calculations: Options 1b and 7b

Use the new estimated $V_{low\text{-}side}$ value of 0.9991 per unit for the second iteration:

Eq. (16) $$\theta_{low-side} = \sin^{-1}\left[\frac{(P_{pu} \times |X_{pu}|)}{(|V_{low-side}| \times [V_{high-side}])}\right]$$

$$\theta_{low-side} = \sin^{-1}\left[\frac{(0.91 \times 0.1032)}{(0.9991 \times 0.85)}\right]$$

$$\theta_{low-side} = 6.3°$$

Eq. (17)

$$|V_{low-side}| = \frac{|V_{high-side}| \times \cos(\theta_{low-side}) \pm \sqrt{|V_{high-side}|^2 \times \cos^2(\theta_{low-side}) + 4 \times Q_{pu} \times X_{pu}}}{2}$$

$$|V_{low-side}| = \frac{|0.85| \times \cos(6.3°) \pm \sqrt{|0.85|^2 \times \cos^2(6.3°) + 4 \times 1.5 \times 0.1032}}{2}$$

$$|V_{low-side}| = \frac{|0.85| \times 0.9940 \pm \sqrt{0.7225 \times 0.9880 + 0.6192}}{2}$$

$$|V_{low-side}| = \frac{0.8449 \pm 1.1546}{2}$$

$$|V_{low-side}| = 0.9998\ p.u.$$

To account for system high-side nominal voltage and the transformer tap ratio:

Eq. (18) $$V_{bus} = |V_{low-side}| \times V_{nom} \times GSU_{ratio}$$

$$V_{bus} = 0.9998\ p.u. \times 345\ kV \times \left(\frac{22\ kV}{346.5\ kV}\right)$$

$$V_{bus} = 21.90\ kV$$

Apparent power (S):

Eq. (19) $$S = P_{Synch_reported} + jQ$$

$$S = 700.0\ MW + j1151.3\ Mvar$$

$$S = 1347.4\angle 58.7°\ MVA$$

Example Calculations: Options 1b and 7b

Primary impedance (Z_{pri}):

Eq. (20) $$Z_{pri} = \frac{V_{bus}^2}{S^*}$$

$$Z_{pri} = \frac{(21.90\ kV)^2}{1347.4\angle -58.7°\ MVA}$$

$$Z_{pri} = 0.356\angle 58.7°\ \Omega$$

Secondary impedance (Z_{sec}):

Eq. (21) $$Z_{sec} = Z_{pri} \times \frac{CT_{ratio}}{PT_{ratio}}$$

$$Z_{sec} = 0.356\angle 58.7°\ \Omega \times \frac{\frac{25000}{5}}{\frac{200}{1}}$$

$$Z_{sec} = 0.356\angle 58.7°\ \Omega \times 25$$

$$Z_{sec} = 8.900\angle 58.7°\ \Omega$$

To satisfy the 115% margin in Options 1b and 7b:

Eq. (22) $$Z_{\text{sec}\,limit} = \frac{Z_{sec}}{115\%}$$

$$Z_{\text{sec}\,limit} = \frac{8.900\angle 58.7°\ \Omega}{1.15}$$

$$Z_{\text{sec}\,limit} = 7.74\angle 58.7°\ \Omega$$

$$\theta_{transient\ load\ angle} = 58.7°$$

Assume a Mho distance impedance relay with a maximum torque angle (MTA) set at 85°, then the maximum allowable impedance reach is:

Eq. (23) $$Z_{max} < \frac{|Z_{\text{sec}\,limit}|}{\cos\left(\theta_{MTA} - \theta_{transient\ load\ angle}\right)}$$

$$Z_{max} < \frac{7.74\ \Omega}{\cos(85.0° - 58.7°)}$$

Example Calculations: Options 1b and 7b

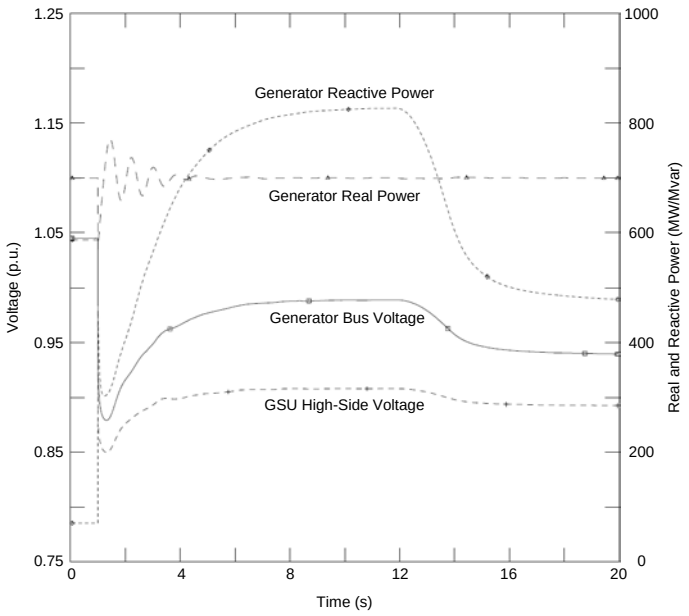
$$Z_{max} < \frac{7.74\ \Omega}{0.8965}$$

$$Z_{max} < 8.633 \angle 85.0°\ \Omega$$

Example Calculations: Options 1c and 7c

Option 1c represents a more involved, more precise setting of the impedance element. This option requires determining maximum generator Reactive Power output during field-forcing and the corresponding generator bus voltage. Once these values are determined, the remainder of the calculation is the same as Options 1a and 1b.

The generator Reactive Power and generator bus voltage are determined by simulation. The maximum Reactive Power output on the low-side of the GSU transformer during field-forcing is used as this value will correspond to the lowest apparent impedance. The corresponding generator bus voltage is also used in the calculation. Note that although the excitation limiter reduces the field, the duration of the Reactive Power output achieved for this condition is sufficient to operate a phase distance relay.



In this simulation the following values are derived:

$$Q = 827.4\ Mvar$$

$$V_{bus_simulated} = 0.989 \times V_{gen_nom} = 21.76\ k\text{V}$$

Example Calculations: Options 1c and 7c

The other value required is the Real Power output which is modeled in the simulation at 100% of the gross MW capability reported to the Transmission Planner. In this case:

$$P_{Synch_reported} = 700.0\ MW$$

Apparent power (S):

Eq. (24) $$S = P_{Synch_reported} + jQ$$

$$S = 700.0\ MW + j827.4\ Mvar$$

$$S = 1083.8\angle 49.8°\ MVA$$

Primary impedance (Z_{pri}):

Eq. (25) $$Z_{pri} = \frac{V_{bus_simulated}^2}{S^*}$$

$$Z_{pri} = \frac{(21.76\ kV)^2}{1083.8\angle -49.8°\ MVA}$$

$$Z_{pri} = 0.437\angle 49.8°\ \Omega$$

Secondary impedance (Z_{sec}):

Eq. (26) $$Z_{sec} = Z_{pri} \times \frac{CT_{ratio}}{PT_{ratio}}$$

$$Z_{sec} = 0.437\angle 49.8°\ \Omega \times \frac{\frac{25000}{5}}{\frac{200}{1}}$$

$$Z_{sec} = 0.437\angle 49.8°\ \Omega \times 25$$

$$Z_{sec} = 10.92\angle 49.8°\ \Omega$$

To satisfy the 115% margin in the requirement in Options 1c and 7c:

Eq. (27) $$Z_{\mathrm{sec}\,limit} = \frac{Z_{sec}}{115\%}$$

$$Z_{\mathrm{sec}\,limit} = \frac{10.92\angle 49.8°\ \Omega}{1.15}$$

$$Z_{\mathrm{sec}\,limit} = 9.50\angle 49.8°\ \Omega$$

Example Calculations: Options 1c and 7c

$$\theta_{transient\ load\ angle} = 49.8°$$

Assume a Mho distance impedance relay with a maximum torque angle (MTA) set at 85°, then the maximum allowable impedance reach is:

Eq. (28) $$Z_{max} < \frac{|Z_{\sec limit}|}{\cos(\theta_{MTA} - \theta_{transient\ load\ angle})}$$

$$Z_{max} < \frac{9.50\ \Omega}{\cos(85.0° - 49.8°)}$$

$$Z_{max} < \frac{9.50\ \Omega}{0.8171}$$

$$Z_{max} < 11.63\angle 85.0°\ \Omega$$

Example Calculations: Option 2a

Option 2a represents the simplest calculation for synchronous generators applying a phase overcurrent (e.g., 50, 51, or 51V-R) relay:

Real Power output (P):

Eq. (29) $$P = GEN_{Synch_nameplate} \times pf$$

$$P = 903\ MVA \times 0.85$$

$$P = 767.6\ MW$$

Reactive Power output (Q):

Eq. (30) $$Q = 150\% \times P$$

$$Q = 1.50 \times 767.6\ MW$$

$$Q = 1151.3\ Mvar$$

Option 2a, Table 1 – Bus Voltage, calls for a 0.95 per unit of the high-side nominal voltage for the generator bus voltage (V_{gen}):

Eq. (31) $$V_{gen} = 0.95\ p.u. \times V_{nom} \times GSU_{ratio}$$

Example Calculations: Option 2a

$$V_{gen} = 0.95 \times 345\ kV \times \left(\frac{22\ kV}{346.5\ kV}\right)$$

$$V_{gen} = 20.81\ kV$$

Apparent power (S):

Eq. (32) $$S = P_{Synch_reported} + jQ$$

$$S = 700.0\ MW + j1151.3\ Mvar$$

$$S = 1347.4\angle 58.7°\ MVA$$

Primary current (I_{pri}):

Eq. (33) $$I_{pri} = \frac{S}{\sqrt{3} \times V_{gen}}$$

$$I_{pri} = \frac{1347.4\ MVA}{1.73 \times 20.81\ kV}$$

$$I_{pri} = 37383\ A$$

Secondary current (I_{sec}):

Eq. (34) $$I_{sec} = \frac{I_{pri}}{CT_{ratio}}$$

$$I_{sec} = \frac{37383\ A}{\frac{25000}{5}}$$

$$I_{sec} = 7.477\ A$$

To satisfy the 115% margin in Option 2a:

Eq. (35) $$I_{\mathrm{sec}\,limit} > I_{sec} \times 115\%$$

$$I_{\mathrm{sec}\,limit} > 7.477\ A \times 1.15$$

$$I_{\mathrm{sec}\,limit} > 8.598\ A$$

Example Calculations: Option 2b

Option 2b represents a more complex calculation for synchronous generators applying a phase overcurrent (e.g., 50, 51, or 51V-R) relay:

Real Power output (P):

Eq. (36) $$P = GEN_{Synch_nameplate} \times pf$$

$$P = 903\ MVA \times 0.85$$

$$P = 767.6\ MW$$

Reactive Power output (Q):

Eq. (37) $$Q = 150\% \times P$$

$$Q = 1.50 \times 767.6\ MW$$

$$Q = 1151.3\ Mvar$$

Convert Real Power, Reactive Power, and transformer reactance to per unit values on 767.6 MVA base (MVA_{base}).

Real Power output (P):

Eq. (38) $$P_{pu} = \frac{P_{Synch_reported}}{MVA_{base}}$$

$$P_{pu} = \frac{700.0\ MW}{767.6\ MVA}$$

$$P_{pu} = 0.91\ p.u.$$

Reactive Power output (Q):

Eq. (39) $$Q_{pu} = \frac{Q}{MVA_{base}}$$

$$Q_{pu} = \frac{1151.3\ Mvar}{767.6\ MVA}$$

$$Q_{pu} = 1.5\ p.u.$$

Example Calculations: Option 2b

Transformer impedance:

Eq. (40) $$X_{pu} = X_{GSU(old)} \times \frac{MVA_{base}}{MVA_{GSU}}$$

$$X_{pu} = 12.14\% \times \left(\frac{767.6\ MVA}{903\ MVA}\right)$$

$$X_{pu} = 0.1032\ p.u.$$

Using the formula below; calculate the low-side GSU transformer voltage ($V_{low\text{-}side}$) using 0.85 p.u. high-side voltage ($V_{high\text{-}side}$). Assume initial low-side voltage to be 0.95 p.u. and repeat the calculation as necessary until $V_{low\text{-}side}$ converges. A convergence of less than one percent (<1%) between iterations is considered sufficient:

Eq. (41) $$\theta_{low-side} = \sin^{-1}\left[\frac{\left(P_{pu} \times |X_{pu}|\right)}{\left(|V_{low-side}| \times [V_{high-side}]\right)}\right]$$

$$\theta_{low-side} = \sin^{-1}\left[\frac{(0.91 \times 0.1032)}{(0.95 \times 0.85)}\right]$$

$$\theta_{low-side} = 6.7°$$

Eq. (42)

$$|V_{low-side}| = \frac{|V_{high-side}| \times \cos(\theta_{low-side}) \pm \sqrt{|V_{high-side}|^2 \times \cos^2(\theta_{low-side}) + 4 \times Q_{pu} \times X_{pu}}}{2}$$

$$|V_{low-side}| = \frac{|0.85| \times \cos(6.7°) \pm \sqrt{|0.85|^2 \times \cos^2(6.7°) + 4 \times 1.5 \times 0.1032}}{2}$$

$$|V_{low-side}| = \frac{|0.85| \times 0.9931 \pm \sqrt{0.7225 \times 0.9864 + 0.6192}}{2}$$

$$|V_{low-side}| = \frac{0.8441 \pm 1.1541}{2}$$

$$|V_{low-side}| = 0.9991\ p.u.$$

Example Calculations: Option 2b

Use the new estimated $V_{low\text{-}side}$ value of 0.9991 per unit for the second iteration:

Eq. (43) $$\theta_{low-side} = \sin^{-1}\left[\frac{(P_{pu} \times |X_{pu}|)}{(|V_{low-side}| \times [V_{high-side}])}\right]$$

$$\theta_{low-side} = \sin^{-1}\left[\frac{(0.91 \times 0.1032)}{(0.9991 \times 0.85)}\right]$$

$$\theta_{low-side} = 6.3°$$

Eq. (44)

$$|V_{low-side}| = \frac{|V_{high-side}| \times \cos(\theta_{low-side}) \pm \sqrt{|V_{high-side}|^2 \times \cos^2(\theta_{low-side}) + 4 \times Q_{pu} \times X_{pu}}}{2}$$

$$|V_{low-side}| = \frac{|0.85| \times \cos(6.3°) \pm \sqrt{|0.85|^2 \times \cos^2(6.3°) + 4 \times 1.5 \times 0.1032}}{2}$$

$$|V_{low-side}| = \frac{|0.85| \times 0.9940 \pm \sqrt{0.7225 \times 0.9880 + 0.6192}}{2}$$

$$|V_{low-side}| = \frac{0.8449 \pm 1.1546}{2}$$

$$|V_{low-side}| = 0.9998\ p.u.$$

To account for system high-side nominal voltage and the transformer tap ratio:

Eq. (45) $$V_{bus} = |V_{low-side}| \times V_{nom} \times GSU_{ratio}$$

$$V_{bus} = 0.9998\ p.u. \times 345\ kV \times \left(\frac{22\ kV}{346.5\ kV}\right)$$

$$V_{bus} = 21.90\ kV$$

Apparent power (S):

Eq. (46) $$S = P_{Synch_reported} + jQ$$

$$S = 700.0\ MW + j1151.3\ Mvar$$

$$S = 1347.4 \angle 58.7°\ MVA$$

Example Calculations: Option 2b

Primary current (I_{pri}):

Eq. (47) $$I_{pri} = \frac{S}{\sqrt{3} \times V_{bus}}$$

$$I_{pri} = \frac{1347.4\ MVA}{1.73 \times 21.90\ kV}$$

$$I_{pri} = 35553\ A$$

Secondary current (I_{sec}):

Eq. (48) $$I_{sec} = \frac{I_{pri}}{CT_{ratio}}$$

$$I_{sec} = \frac{35553\ A}{\frac{25000}{5}}$$

$$I_{sec} = 7.111\ A$$

To satisfy the 115% margin in Option 2b:

Eq. (49) $$I_{\mathrm{sec}\,limit} > I_{sec} \times 115\%$$

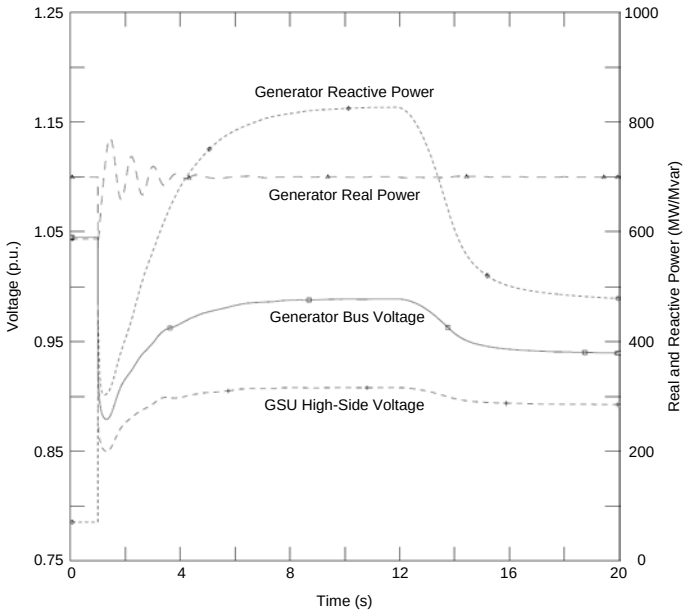
$$I_{\mathrm{sec}\,limit} > 7.111\ A \times 1.15$$

$$I_{\mathrm{sec}\,limit} > 8.178\ A$$

Example Calculations: Option 2c

Option 2c represents a more involved, more precise setting of the overcurrent element for the phase overcurrent (e.g., 50, 51, or 51V-R) relay. This option requires determining maximum generator Reactive Power output during field-forcing and the corresponding generator bus voltage. Once these values are determined, the remainder of the calculation is the same as Options 2a and 2b.

The generator Reactive Power and generator bus voltage are determined by simulation. The maximum Reactive Power output on the low-side of the GSU transformer during field-forcing is used as this value will correspond to the highest current. The corresponding generator bus voltage is also used in the calculation. Note that although the excitation limiter reduces the field, the duration of the Reactive Power output achieved for this condition is sufficient to operate a voltage-restrained phase overcurrent relay.



In this simulation the following values are derived:

$$Q = 827.4\ Mvar$$

$$V_{bus_simulated} = 0.989 \times V_{gen_nom} = 21.76\ kV$$

The other value required is the Real Power output which is modeled in the simulation at 100% of the gross MW capability reported to the Transmission Planner. In this case:

$$P_{Synch_reported} = 700.0\ MW$$

Example Calculations: Option 2c

Apparent power (S):

Eq. (50) $S = P_{Synch_reported} + jQ$

$S = 700.0\ MW + j827.4\ Mvar$

$S = 1083.8 \angle 49.8°\ MVA$

Primary current (I_{pri}):

Eq. (51) $I_{pri} = \frac{S}{\sqrt{3} \times V_{bus_simulated}}$

$I_{pri} = \frac{1083.8\ MVA}{1.73 \times 21.76\ kV}$

$I_{pri} = 28790\ A$

Secondary current (I_{sec}):

Eq. (52) $I_{sec} = \frac{I_{pri}}{CT_{ratio}}$

$I_{sec} = \frac{28790\ A}{\frac{25000}{5}}$

$I_{sec} = 5.758\ A$

To satisfy the 115% margin in Option 2c:

Eq. (53) $I_{\text{sec}\,limit} > I_{sec} \times 115\%$

$I_{\text{sec}\,limit} > 5.758\ A \times 1.15$

$I_{\text{sec}\,limit} > 6.622\ A$

Example Calculations: Options 3 and 6

Option 3 represents the only calculation for synchronous generators applying a phase time overcurrent (e.g., 51V-C) relay (Enabled to operate as a function of voltage). Similarly, Option 6 uses the same calculation for asynchronous generators.

Example Calculations: Options 3 and 6

Options 3 and 6, Table 1 – Bus Voltage, calls for a 1.0 per unit of the high-side nominal voltage for the generator bus voltage (V_{gen}):

Eq. (54) $$V_{gen} = 1.0\ p.u. \times V_{nom} \times GSU_{ratio}$$

$$V_{gen} = 1.0 \times 345\ kV \times \left(\frac{22\ kV}{346.5\ kV}\right)$$

$$V_{gen} = 21.9\ kV$$

The voltage setting shall be set less than 75% of the generator bus voltage:

Eq. (55) $$V_{setting} < V_{gen} \times 75\%$$

$$V_{setting} < 21.9\ kV\ \times 0.75$$

$$V_{setting} < 16.429\ kV$$

Example Calculations: Option 4

This represents the calculation for an asynchronous generator (including inverter-based installations) applying a phase distance relay (e.g., 21) directional toward the Transmission system.

Real Power output (P):

Eq. (56) $$P = GEN_{Asych_nameplate} \times pf$$

$$P = 40\ MVA\ \times 0.85$$

$$P = 34.0\ MW$$

Reactive Power output (Q):

Eq. (57) $$Q = GEN_{Async_nameplate} \times \sin(\cos^{-1}(pf))$$

$$Q = 40\ MVA \times \sin(\cos^{-1}(0.85))$$

$$Q = 21.1\ Mvar$$

Example Calculations: Option 4

Option 4, Table 1 – Bus Voltage, calls for a 1.0 per unit of the high-side nominal voltage for the generator bus voltage (V_{gen}):

Eq. (58) $$V_{gen} = 1.0\ p.u. \times V_{nom} \times GSU_{ratio}$$

$$V_{gen} = 1.0 \times 345\ kV \times \left(\frac{22\ kV}{346.5\ kV}\right)$$

$$V_{gen} = 21.9\ kV$$

Apparent power (S):

Eq. (59) $$S = P + jQ$$

$$S = 34.0\ MW + j21.1\ Mvar$$

$$S = 40.0 \angle 31.8°\ MVA$$

Primary impedance (Z_{pri}):

Eq. (60) $$Z_{pri} = \frac{V_{gen}^2}{S^*}$$

$$Z_{pri} = \frac{(21.9\ kV)^2}{40.0 \angle -31.8°\ MVA}$$

$$Z_{pri} = 11.99 \angle 31.8°\ \Omega$$

Secondary impedance (Z_{sec}):

Eq. (61) $$Z_{sec} = Z_{pri} \times \frac{CT_{Asynch_ratio}}{PT_{ratio}}$$

$$Z_{sec} = 11.99 \angle 31.8°\ \Omega \times \frac{\frac{5000}{5}}{\frac{200}{1}}$$

$$Z_{sec} = 11.99 \angle 31.8°\ \Omega \times 5$$

$$Z_{sec} = 59.95 \angle 31.8°\ \Omega$$

To satisfy the 130% margin in Option 4:

Eq. (62) $$Z_{\text{sec}\,limit} = \frac{Z_{sec}}{130\%}$$

Example Calculations: Option 4

$$Z_{\sec limit} = \frac{59.95\angle 31.8° \ \Omega}{1.30}$$

$$Z_{\sec limit} = 46.12\angle 31.8° \ \Omega$$

$$\theta_{transient\ load\ angle} = 31.8°$$

Assume a Mho distance impedance relay with a maximum torque angle (MTA) set at 85°, then the maximum allowable impedance reach is:

Eq. (63) $$Z_{max} < \frac{|Z_{\sec limit}|}{\cos(\theta_{MTA} - \theta_{transient\ load\ angle})}$$

$$Z_{max} < \frac{46.12 \ \Omega}{\cos(85.0° - 31.8°)}$$

$$Z_{max} < \frac{46.12 \ \Omega}{0.599}$$

$$Z_{max} < \ 77.0\angle 85.0° \ \Omega$$

Example Calculations: Option 5a

This represents the calculation for three asynchronous generators applying a phase overcurrent (e.g., 50, 51, or 51V-R) relay. In this application it was assumed that 20 Mvar of total static compensation was added.

Real Power output (P):

Eq. (64) $$P = \ 3 \times GEN_{Asynch_nameplate} \times pf$$

$$P = 3 \times 40 \ MVA \ \times 0.85$$

$$P = 102.0 \ MW$$

Reactive Power output (Q):

Eq. (65) $$Q = MVAR_{static} + MVAR_{gen_static} + \left(3 \times GEN_{Asynch_nameplate} \times \sin(\cos^{-1}(pf))\right)$$

$$Q = 15 \ Mvar + 5 \ Mvar + (3 \times 40 \ MVA \times \sin(\cos^{-1}(0.85)))$$

$$Q = 83.2 \ Mvar$$

Example Calculations: Option 5a

Option 5a, Table 1 – Bus Voltage, calls for a 1.0 per unit of the high-side nominal voltage for the generator bus voltage (V_{gen}):

Eq. (66) $$V_{gen} = 1.0\ p.u. \times V_{nom} \times GSU_{ratio}$$

$$V_{gen} = 1.0 \times 345\ kV \times \left(\frac{22\ kV}{346.5\ kV}\right)$$

$$V_{gen} = 21.9\ kV$$

Apparent power (S):

Eq. (67) $$S = P + jQ$$

$$S = 102.0\ MW + j83.2\ Mvar$$

$$S = 131.6\angle 39.2°\ MVA$$

Primary current (I_{pri}):

Eq. (68) $$I_{pri} = \frac{S^*}{\sqrt{3} \times V_{gen}}$$

$$I_{pri} = \frac{131.6\angle -39.2°\ MVA}{1.73 \times 21.9\ kV}$$

$$I_{pri} = 3473\angle -39.2°\ A$$

Secondary current (I_{sec}):

Eq. (69) $$I_{sec} = \frac{I_{pri}}{CT_{Asynch_ratio}}$$

$$I_{sec} = \frac{3473\angle -39.2°\ A}{\frac{5000}{5}}$$

$$I_{sec} = 3.473\angle -39.2°\ A$$

To satisfy the 130% margin in Option 5a:

Eq. (70) $$I_{\mathrm{sec}\,limit} > I_{sec} \times 130\%$$

$$I_{\mathrm{sec}\,limit} > 3.473\angle -39.2°\ A \times 1.30$$

Example Calculations: Option 5a

$$I_{\sec limit} > 4.52\angle -39.2° \; A$$

Example Calculations: Option 5b

Similarly to Option 5a, this example represents the calculation for three asynchronous generators applying a phase overcurrent (e.g., 50, 51, or 51V-R) relay. In this application it was assumed that 20 Mvar of total static compensation was added.

Real Power output (P):

Eq. (71) $$P = 3 \times GEN_{Asynch_nameplate} \times pf$$

$$P = 3 \times 40 \; MVA \times 0.85$$

$$P = 102.0 \; MW$$

Reactive Power output (Q):

Eq. (72) $$Q = MVAR_{static} + MVAR_{gen_static} + \left(3 \times GEN_{Asynch_nameplate} \times \sin(\cos^{-1}(pf))\right)$$

$$Q = 15 \; Mvar + 5 \; Mvar + (3 \times 40 \; MVA \times \sin(\cos^{-1}(0.85)))$$

$$Q = 83.2 \; Mvar$$

Option 5b, Table 1 – Bus Voltage, calls for a 1.0 per unit of the high-side nominal voltage for the generator bus voltage (V_{gen}):

Eq. (73) $$V_{gen} = 1.0 \; p.u. \times V_{nom} \times GSU_{ratio}$$

$$V_{gen} = 1.0 \times 345 \; kV \times \left(\frac{22 \; kV}{346.5 \; kV}\right)$$

$$V_{gen} = 21.9 \; kV$$

Apparent power (S):

Eq. (74) $$S = P + jQ$$

$$S = 102.0 \; MW + j83.2 \; Mvar$$

$$S = 131.6\angle 39.2° \; MVA$$

Example Calculations: Option 5b

Primary current (I_{pri}):

Eq. (75) $$I_{pri} = \frac{S^*}{\sqrt{3} \times V_{gen}}$$

$$I_{pri} = \frac{131.6\angle -39.2°\ MVA}{1.73 \times 21.9\ kV}$$

$$I_{pri} = 3473\angle -39.2°\ A$$

Secondary current (I_{sec}):

Eq. (76) $$I_{sec} = \frac{I_{pri}}{CT_{Asynch_ratio}}$$

$$I_{sec} = \frac{3473\angle -39.2°\ A}{\frac{5000}{5}}$$

$$I_{sec} = 3.473\angle -39.2°\ A$$

To satisfy Option 5b, the lower tolerance of the overcurrent element tripping characteristic shall not infringe upon the resource capability (including the Mvar output of the resource and any static or dynamic reactive power devices) See Figure A for more details.

Example Calculations: Options 7a and 10

These examples represent the calculation for a mixture of asynchronous (i.e., Option 10) and synchronous (i.e., Option 7a) generation (including inverter-based installations) applying a phase distance relay (e.g., 21) directional toward the Transmission system. In this application it was assumed 20 Mvar of total static compensation was added.

Synchronous Generation (Option 7a)

Real Power output (P_{sync}):

Eq. (77) $$P_{Synch} = GEN_{Synch_nameplate} \times pf$$

$$P_{Synch} = 903\ MVA \times 0.85$$

$$P_{Synch} = 767.6\ MW$$

Example Calculations: Options 7a and 10

Reactive Power output (Q_{synch}):

Eq. (78) $$Q_{Synch} = 150\% \times P_{Synch}$$

$$Q_{Synch} = 1.50 \times 767.6\ MW$$

$$Q_{Synch} = 1151.3\ MW$$

Apparent power (S_{Synch}):

Eq. (79) $$S_{Synch} = P_{Synch_reported} + jQ_{Synch}$$

$$S_{Synch} = 700.0\ MW + j1151.3\ Mvar$$

Asynchronous Generation (Option 10)

Real Power output (P_{Asynch}):

Eq. (80) $$P_{Asynch} = 3 \times GEN_{Asynch_nameplate} \times pf$$

$$P_{Asynch} = 3 \times 40\ MVA \times 0.85$$

$$P_{Asynch} = 102.0\ MW$$

Reactive Power output (Q_{Asynch}):

Eq. (81) $$Q_{Asynch} = MVAR_{static} + MVAR_{gen_static} + \left(3 \times GEN_{Asynch_nameplate} \times \sin(\cos^{-1}(pf))\right)$$

$$Q_{Asynch} = 15\ Mvar + 5\ Mvar + (3 \times 40\ MVA \times \sin(\cos^{-1}(0.85)))$$

$$Q_{Asynch} = 83.2\ Mvar$$

Apparent power (S_{Asynch}):

Eq. (82) $$S_{Asynch} = P_{Asynch} + jQ_{Asynch}$$

$$S_{Asynch} = 102.0\ MW + j83.2\ Mvar$$

Example Calculations: Options 7a and 10

Options 7a and 10, Table 1 – Bus Voltage, Option 7a specifies 0.95 per unit of the high-side nominal voltage for the generator bus voltage and Option 10 specifies 1.0 per unit of the high-side nominal voltage for generator bus voltage. Due to the presence of the synchronous generator, the 0.95 per unit bus voltage will be used as (V_{gen}) as it results in the most conservative voltage:

Eq. (83) $$V_{gen} = 0.95\ p.u. \times V_{nom} \times GSU_{ratio}$$

$$V_{gen} = 0.95 \times 345\ kV \times \left(\frac{22\ kV}{346.5\ kV}\right)$$

$$V_{gen} = 20.81\ kV$$

Apparent power (S) accounted for 115% margin requirement for a synchronous generator and 130% margin requirement for an asynchronous generator:

Eq. (84) $$S = 115\% \times \left(P_{Synch_reported} + jQ_{Synch}\right) + 130\% \times \left(P_{Asynch} + jQ_{Asynch}\right)$$

$$S = 1.15 \times (700.0\ MW + j1151.3\ Mvar) + 1.30 \times (102.0\ MW + j83.2\ Mvar)$$

$$S = 1711.8\ \angle 56.8°\ MVA$$

Primary impedance (Z_{pri}):

Eq. (85) $$Z_{pri} = \frac{V_{gen}^2}{S^*}$$

$$Z_{pri} = \frac{(20.81\ kV)^2}{1711.8\angle -56.8°\ MVA}$$

$$Z_{pri} = 0.2527\angle 56.8°\ \Omega$$

Secondary impedance (Z_{sec}):

Eq. (86) $$Z_{sec} = Z_{pri} \times \frac{CT_{ratio}}{PT_{ratio}}$$

$$Z_{sec} = 0.2527\angle 56.8°\ \Omega \times \frac{\frac{25000}{5}}{\frac{200}{1}}$$

$$Z_{sec} = 0.2527\angle 56.8°\ \Omega \times 25$$

$$Z_{sec} = 6.32\angle 56.8°\ \Omega$$

Example Calculations: Options 7a and 10

No additional margin is needed because the synchronous apparent power has been multiplied by 1.15 (115%) and the asynchronous apparent power has been multiplied by 1.30 (130%) in Equation 84 to satisfy the margin requirements in Options 7a and 10.

Eq. (87) $$Z_{\sec limit} = \frac{Z_{sec}}{100\%}$$

$$Z_{\sec limit} = \frac{6.32 \angle 56.8° \, \Omega}{1.00}$$

$$Z_{\sec limit} = 6.32 \angle 56.8° \, \Omega$$

$$\theta_{transient\ load\ angle} = 56.8°$$

Assume a Mho distance impedance relay with a maximum torque angle (MTA) set at 85°, then the maximum allowable impedance reach is:

Eq. (88) $$Z_{max} < \frac{|Z_{\sec limit}|}{\cos(\theta_{MTA} - \theta_{transient\ load\ angle})}$$

$$Z_{max} < \frac{6.32 \, \Omega}{\cos(85.0° - 56.8°)}$$

$$Z_{max} < \frac{6.32 \, \Omega}{0.881}$$

$$Z_{max} < \ 7.17 \angle 85.0° \, \Omega$$

Example Calculations: Options 8a and 9a

Options 8a and 9a represent the simplest calculation for synchronous generators applying a phase overcurrent (e.g., 50, 51, or 67) relay. The following uses the $GEN_{Synch_nameplate}$ value to represent an "aggregate" value to illustrate the option:

Real Power output (P):

Eq. (89) $$P = \ GEN_{Synch_nameplate} \times pf$$

$$P = 903 \ MVA \ \times 0.85$$

$$P = 767.6 \ MW$$

Example Calculations: Options 8a and 9a

Reactive Power output (Q):

Eq. (90) $Q = 150\% \times P$

$$Q = 1.50 \times 767.6\ MW$$

$$Q = 1151.3\ Mvar$$

Options 8a and 9a, Table 1 – Bus Voltage, calls for a generator bus voltage corresponding to 0.95 per unit of the high-side nominal voltage times the turns ratio of the generator step-up transformer generator bus voltage (V_{gen}):

Eq. (91) $V_{gen} = 0.95\ p.u. \times V_{nom} \times GSU_{ratio}$

$$V_{gen} = 0.95 \times 345\ kV \times \left(\frac{22\ kV}{346.5\ kV}\right)$$

$$V_{gen} = 20.81\ kV$$

Apparent power (S):

Eq. (92) $S = P_{Synch_reported} + jQ$

$$S = 700.0\ MW + j1151.3\ Mvar$$

$$S = 1347.4 \angle 58.7°\ MVA$$

Primary current (I_{pri}):

Eq. (93) $I_{pri} = \frac{S}{\sqrt{3} \times V_{gen}}$

$$I_{pri} = \frac{1347.4\ MVA}{1.73 \times 20.81\ kV}$$

$$I_{pri} = 37383\ A$$

Secondary current (I_{sec}):

Eq. (94) $I_{sec} = \frac{I_{pri}}{CT_{ratio}}$

$$I_{sec} = \frac{37383\ A}{\frac{25000}{5}}$$

Example Calculations: Options 8a and 9a

$$I_{sec} = 7.477\ A$$

To satisfy the 115% margin in Options 8a and 9a:

Eq. (95) $$I_{\text{sec}\,limit} > I_{sec} \times 115\%$$

$$I_{\text{sec}\,limit} > 7.477\ A \times 1.15$$

$$I_{\text{sec}\,limit} > 8.598\ A$$

Example Calculations: Options 8b and 9b

Options 8b and 9b represent a more precise calculation for synchronous generators applying a phase overcurrent (e.g., 50, 51, or 67) relay. The following uses the $GEN_{Synch_nameplate}$ value to represent an "aggregate" value to illustrate the option:

Real Power output (P):

Eq. (96) $$P = GEN_{Synch_nameplate} \times pf$$

$$P = 903\ MVA \times 0.85$$

$$P = 767.6\ MW$$

Reactive Power output (Q):

Eq. (97) $$Q = 150\% \times P$$

$$Q = 1.50 \times 767.6\ MW$$

$$Q = 1151.3\ Mvar$$

Convert Real Power, Reactive Power, and transformer reactance to per unit values on 767.6 MVA base (GSU transformer MVA_{base}).

Real Power output (P):

Eq. (98) $$P_{pu} = \frac{P_{Synch_reported}}{MVA_{base}}$$

$$P_{pu} = \frac{700.0\ MW}{767.6\ MVA}$$

Example Calculations: Options 8b and 9b

$$P_{pu} = 0.91\ p.u.$$

Reactive Power output (Q):

Eq. (99) $$Q_{pu} = \frac{Q}{MVA_{base}}$$

$$Q_{pu} = \frac{1151.3\ Mvar}{767.6\ MVA}$$

$$Q_{pu} = 1.5\ p.u.$$

Transformer impedance:

Eq. (100) $$X_{pu} = X_{GSU(old)} \times \frac{MVA_{base}}{MVA_{GSU}}$$

$$X_{pu} = 12.14\% \times \left(\frac{767.6\ MVA}{903\ MVA}\right)$$

$$X_{pu} = 0.1032\ p.u.$$

Using the formula below; calculate the low-side GSU transformer voltage ($V_{low\text{-}side}$) using 0.85 p.u. high-side voltage ($V_{high\text{-}side}$). Assume initial low-side voltage to be 0.95 p.u. and repeat the calculation as necessary until $V_{low\text{-}side}$ converges. A convergence of less than one percent (<1%) between iterations is considered sufficient:

Eq. (101) $$\theta_{low-side} = \sin^{-1}\left[\frac{\left(P_{pu} \times |X_{pu}|\right)}{\left(|V_{low-side}| \times \lceil V_{high-side} \rceil\right)}\right]$$

$$\theta_{low-side} = \sin^{-1}\left[\frac{(0.91 \times 0.1032)}{(0.95 \times 0.85)}\right]$$

Eq. (102)

$$|V_{low-side}| = \frac{|V_{high-side}| \times \cos(\theta_{low-side}) \pm \sqrt{|V_{high-side}|^2 \times \cos^2(\theta_{low-side}) + 4 \times Q_{pu} \times X_{pu}}}{2}$$

$$|V_{low-side}| = \frac{|0.85| \times \cos(6.7°) \pm \sqrt{|0.85|^2 \times \cos^2(6.7°) + 4 \times 1.5 \times 0.1032}}{2}$$

$$|V_{low-side}| = \frac{|0.85| \times 0.9931 \pm \sqrt{0.7225 \times 0.9864 + 0.6192}}{2}$$

Example Calculations: Options 8b and 9b

$$|V_{low-side}| = \frac{0.8441 \pm 1.1541}{2}$$

$$|V_{low-side}| = 0.9991\ p.u.$$

Use the new estimated $V_{low\text{-}side}$ value of 0.9991 per unit for the second iteration:

Eq. (103) $$\theta_{low-side} = \sin^{-1}\left[\frac{(P_{pu} \times |X_{pu}|)}{(|V_{low-side}| \times \lceil V_{high-side} \rceil)}\right]$$

$$\theta_{low-side} = \sin^{-1}\left[\frac{(0.91 \times 0.1032)}{(0.9991 \times 0.85)}\right]$$

$$\theta_{low-side} = 6.3°$$

Eq. (104)

$$|V_{low-side}| = \frac{|V_{high-side}| \times \cos(\theta_{low-side}) \pm \sqrt{|V_{high-side}|^2 \times \cos^2(\theta_{low-side}) + 4 \times Q_{pu} \times X_{pu}}}{2}$$

$$|V_{low-side}| = \frac{|0.85| \times \cos(6.3°) \pm \sqrt{|0.85|^2 \times \cos^2(6.3°) + 4 \times 1.5 \times 0.1032}}{2}$$

$$|V_{low-side}| = \frac{|0.85| \times 0.9940 \pm \sqrt{0.7225 \times 0.9880 + 0.6192}}{2}$$

$$|V_{low-side}| = \frac{0.8449 \pm 1.1546}{2}$$

$$|V_{low-side}| = 0.9998\ p.u.$$

To account for system high-side nominal voltage and the transformer tap ratio:

Eq. (105) $$V_{bus} = |V_{low-side}| \times V_{nom} \times GSU_{ratio}$$

$$V_{bus} = 0.9998\ p.u. \times 345\ kV \times \left(\frac{22\ kV}{346.5\ kV}\right)$$

$$V_{bus} = 21.90\ kV$$

Apparent power (S):

Eq. (106) $$S = P_{Synch_reported} + jQ$$

Example Calculations: Options 8b and 9b

$$S = 700.0\ MW + j1151.3\ Mvar$$

$$S = 1347.4\angle 58.7°\ MVA$$

Primary current (I_{pri}):

Eq. (107) $$I_{pri} = \frac{S}{\sqrt{3} \times V_{bus}}$$

$$I_{pri} = \frac{1347.4\ MVA}{1.73 \times 21.90\ kV}$$

$$I_{pri} = 35553\ A$$

Secondary current (I_{sec}):

Eq. (108) $$I_{sec} = \frac{I_{pri}}{CT_{ratio}}$$

$$I_{sec} = \frac{35553\ A}{\frac{25000}{5}}$$

$$I_{sec} = 7.111\ A$$

To satisfy the 115% margin in Options 8b and 9b:

Eq. (109) $$I_{\text{sec}\,limit} > I_{sec} \times 115\%$$

$$I_{\text{sec}\,limit} > 7.111\ A \times 1.15$$

$$I_{\text{sec}\,limit} > 8.178\ A$$

Example Calculations: Options 8a, 9a, 11, and 12

This example represents the calculation for a mixture of asynchronous and synchronous generators applying a phase overcurrent (e.g., 50, 51, or 67) relays. In this application it was assumed 20 Mvar of total static compensation was added. The current transformers (CT) are located on the low-side of the GSU transformer.

Example Calculations: Options 8a, 9a, 11, and 12

Synchronous Generation (Options 8a and 9a)

Real Power output (P_{Synch}):

Eq. (110) $$P_{Synch} = GEN_{Synch_nameplate} \times pf$$

$$P_{Synch} = 903\ MVA \times .85$$

$$P_{Synch} = 767.6\ MW$$

Reactive Power output (Q_{Synch}):

Eq. (111) $$Q_{Synch} = 150\% \times P_{Synch}$$

$$Q_{Synch} = 1.50 \times 767.6\ MW$$

$$Q_{Synch} = 1151.3\ Mvar$$

Apparent power (S_{Synch}):

Eq. (112) $$S_{Synch} = P_{Synch_reported} + jQ_{Synch}$$

$$S_{Synch} = 700.0\ MW + j1151.3\ Mvar$$

$$S_{Synch} = 1347.4 \angle 58.7°\ MVA$$

Option 8a, Table 1 – Bus Voltage calls for a 0.95 per unit of the high-side nominal voltage as a basis for generator bus voltage (V_{gen}):

Eq. (113) $$V_{gen} = 0.95\ p.u. \times V_{nom} \times GSU_{ratio}$$

$$V_{gen} = 0.95 \times 345\ kV \times \left(\frac{22\ kV}{346.5\ kV}\right)$$

$$V_{gen} = 20.81\ kV$$

Primary current ($I_{pri\text{-}sync}$):

Eq. (114) $$I_{pri-sync} = \frac{115\% \times S^*_{Synch}}{\sqrt{3} \times V_{gen}}$$

$$I_{pri-sync} = \frac{1.15 \times (1347.4 \angle -58.7°\ MVA)}{1.73 \times 20.81\ kV}$$

Example Calculations: Options 8a, 9a, 11, and 12

$$I_{pri-sync} = 43061 \angle -58.7° \; A$$

Asynchronous Generation (Options 11 and 12)

Real Power output (P_{Asynch}):

Eq. (115) $$P_{Asynch} = 3 \times GEN_{Asynch_nameplate} \times pf$$

$$P_{Asynch} = 3 \times 40 \; MVA \times 0.85$$

$$P_{Asynch} = 102.0 \; MW$$

Reactive Power output (Q_{Asynch}):

Eq. (116) $$Q_{Asynch} = MVAR_{static} + MVAR_{gen_static} + GEN_{Asynch_nameplate} \times \sin(\cos^{-1}(pf))$$

$$Q_{Asynch} = 15 \; Mvar + 5 \; Mvar + (3 \times 40 \; MVA \times \sin(\cos^{-1}(0.85)))$$

$$Q_{Asynch} = 83.2 \; Mvar$$

Option 11, Table 1 – Bus Voltage, calls for a 1.0 per unit of the high-side nominal voltage for the generator bus voltage (V_{gen}), however due to the presence of synchronous generator 0.95 per unit bus voltage will be used:

Eq. (117) $$V_{gen} = 0.95 \; p.u. \times V_{nom} \times GSU_{ratio}$$

$$V_{gen} = 0.95 \times 345 \; kV \times \left(\frac{22 \; kV}{346.5 \; kV}\right)$$

$$V_{gen} = 20.81 \; kV$$

Apparent power (S_{Asynch}):

Eq. (118) $$S_{Asynch} = 130\% \times (P_{Asynch} + jQ_{Asynch})$$

$$S_{Asynch} = 1.30 \times (102.0 \; MW + j83.2 \; Mvar)$$

$$S_{Asynch} = 171.1 \angle 39.2° \; MVA$$

Primary current ($I_{pri\text{-}async}$):

Eq. (119) $$I_{pri-async} = \frac{S_{Asych}}{\sqrt{3} \times V_{gen}}$$

Example Calculations: Options 8a, 9a, 11, and 12

$$I_{pri-async} = \frac{171.1 \angle -39.2° \; MVA}{1.73 \; \times 20.81 \; kV}$$

$$I_{pri-async} = 4755 \angle -39.2° \; A$$

Secondary current (I_{sec}):

Eq. (120) $$I_{sec} = \frac{I_{pri-sync}}{CT_{ratio}} + \frac{I_{pri-async}}{CT_{ratio}}$$

$$I_{sec} = \frac{43061 \angle -58.7° \; A}{\frac{25000}{5}} + \frac{4755 \angle -39.2° \; A}{\frac{25000}{5}}$$

$$I_{sec} = 9.514 \angle -56.8° \; A$$

No additional margin is needed because the synchronous apparent power has been multiplied by 1.15 (115%) in Equation 114 and the asynchronous apparent power has been multiplied by 1.30 (130%) in Equation 118.

Eq. (121) $$I_{\text{sec}\,limit} > I_{sec} \times 100\%$$

$$I_{\text{sec}\,limit} > 9.514 \angle -56.8° \; A \times 1.00$$

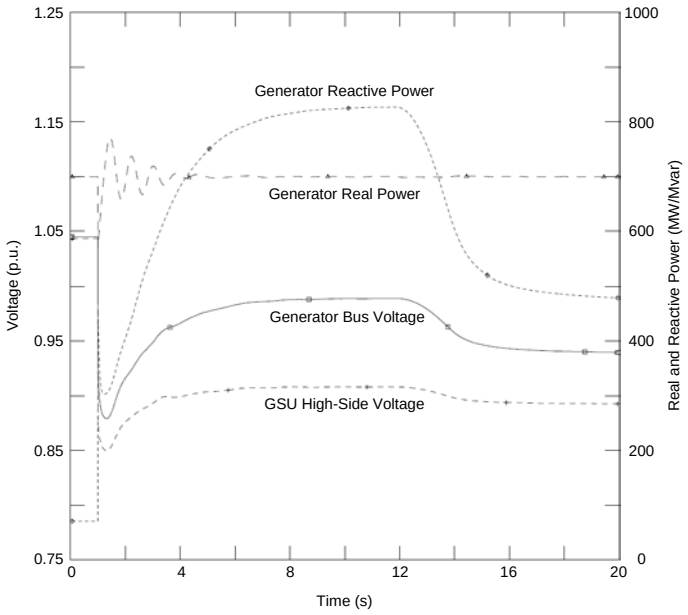
$$I_{\text{sec}\,limit} > 9.514 \angle -56.8° \; A$$

Example Calculations: Options 8c and 9c

This example uses Option 15b as a simulation example for a synchronous generator applying a phase overcurrent relay (e.g., 50, 51, or 67). In this application the same synchronous generator is modeled as for Options 1c, 2c, and 7c. The CTs are located on the low-side of the GSU transformer.

The generator Reactive Power and generator bus voltage are determined by simulation. The maximum Reactive Power output on the low-side of the GSU transformer, during field-forcing, is used since this value will correspond to the highest current. The corresponding generator bus voltage is also used in the calculation. Note that although the excitation limiter reduces the field, the duration of the Reactive Power output achieved for this condition is sufficient to operate a phase overcurrent relay.

Example Calculations: Options 8c and 9c



In this simulation the following values are derived:

$$Q = 827.4\ Mvar$$

$$V_{bus_simulated} = 0.989 \times V_{gen} = 21.76\ kV$$

The other value required is the Real Power output which is modeled in the simulation at 100% of the gross MW capability reported to the Transmission Planner. In this case:

$$P_{reported} = 700.0\ MW$$

Apparent power (S):

Eq. (122) $$S = P_{Synch_reported} + jQ$$

$$S = 700.0\ MW + j827.4\ Mvar$$

$$S = 1083.8\angle 49.8°$$

Primary current (I_{pri}):

Eq. (123) $$I_{pri} = \frac{S}{\sqrt{3} \times V_{bus_simulated}}$$

$$I_{pri} = \frac{1083.8\ MVA}{1.73 \times 21.76\ kV}$$

Example Calculations: Options 8c and 9c

$$I_{pri} = 28790\ A$$

Secondary current (I_{sec}):

Eq. (124) $$I_{sec} = \frac{I_{pri}}{CT_{ratio}}$$

$$I_{sec} = \frac{28790\ A}{\frac{25000}{5}}$$

$$I_{sec} = 5.758\ A$$

To satisfy the 115% margin in Options 8c and 9c:

Eq. (125) $$I_{\text{sec}\,limit} > I_{sec} \times 115\%$$

$$I_{\text{sec}\,limit} > 5.758\ A \times 1.15$$

$$I_{\text{sec}\,limit} > 6.622\ A$$

Example Calculations: Option 10

This example represents the calculation for three asynchronous generators (including inverter-based installations) applying a phase distance relay (e.g., 21) directional toward the Transmission system. In this application it was assumed 20 Mvar of total static compensation was added.

Real Power output (P):

Eq. (126) $$P = 3 \times GEN_{Asych_nameplate} \times pf$$

$$P = 3 \times 40\ MVA \times 0.85$$

$$P = 102.0\ MW$$

Reactive Power output (Q):

Eq. (127) $$Q = MVAR_{static} + MVAR_{gen_static} + \left(3 \times GEN_{Asynch_nameplate} \times \sin(\cos^{-1}(pf))\right)$$

$$Q = 15\ Mvar + 5\ Mvar + (3 \times 40\ MVA \times \sin(\cos^{-1}(0.85)))$$

$$Q = 83.2\ Mvar$$

Example Calculations: Option 10

Option 10, Table 1 – Bus Voltage, calls for a 1.0 per unit of the high-side nominal voltage for the generator bus voltage (V_{gen}):

Eq. (128) $$V_{gen} = 1.0\ p.u. \times V_{nom} \times GSU_{ratio}$$

$$V_{gen} = 1.0 \times 345\ kV \times \left(\frac{22\ kV}{346.5\ kV}\right)$$

$$V_{gen} = 21.9\ kV$$

Apparent power (S):

Eq. (129) $$S = P + jQ$$

$$S = 102.0\ MW + j83.2\ Mvar$$

$$S = 131.6\angle 39.2°\ MVA$$

Primary impedance (Z_{pri}):

Eq. (130) $$Z_{pri} = \frac{V_{gen}^2}{S^*}$$

$$Z_{pri} = \frac{(21.9\ kV)^2}{131.6\angle -39.2°\ MVA}$$

$$Z_{pri} = 3.644\ \angle 39.2°\ \Omega$$

Secondary impedance (Z_{sec}):

Eq. (131) $$Z_{sec} = Z_{pri} \times \frac{CT_{Asynch_ratio}}{PT_{ratio}}$$

$$Z_{sec} = 3.644\ \angle 39.2°\ \Omega \times \frac{\frac{5000}{5}}{\frac{200}{1}}$$

$$Z_{sec} = 3.644\ \angle 39.2°\ \Omega \times 5$$

$$Z_{sec} = 18.22\ \angle 39.2°\ \Omega$$

To satisfy the 130% margin in Option 10:

Eq. (132) $$Z_{\mathrm{sec}\,limit} = \frac{Z_{sec}}{130\%}$$

Example Calculations: Option 10

$$Z_{\sec limit} = \frac{18.22\angle 39.2°\ \Omega}{1.30}$$

$$Z_{\sec limit} = 14.02\angle 39.2°\ \Omega$$

$$\theta_{transient\ load\ angle} = 39.2°$$

Assume a Mho distance impedance relay with a maximum torque angle (MTA) set at 85°, then the maximum allowable impedance reach is:

Eq. (133) $$Z_{max} < \frac{|Z_{\sec limit}|}{\cos\left(\theta_{MTA} - \theta_{transient\ load\ angle}\right)}$$

$$Z_{max} < \frac{14.02\ \Omega}{\cos(85.0° - 39.2°)}$$

$$Z_{max} < \frac{14.02\ \Omega}{0.6972}$$

$$Z_{max} < 20.11\angle 85.0°\ \Omega$$

Example Calculations: Options 11 and 12

Option 11 represents the calculation for a GSU transformer applying a phase overcurrent (e.g., 50 or 51) relay connected to three asynchronous generators. Similarly, these calculations can be applied to Option 12 for a phase directional overcurrent relay (e.g., 67) directional toward the Transmission system. In this application it was assumed 20 Mvar of total static compensation was added.

Real Power output (P):

Eq. (134) $$P = 3 \times GEN_{Asynch_nameplate} \times pf$$

$$P = 3 \times 40\ MVA \times 0.85$$

$$P = 102.0\ MW$$

Reactive Power output (Q):

Eq. (135) $$Q = MVAR_{static} + MVAR_{gen_static} + \left(3 \times GEN_{Asynch_nameplate} \times \sin(\cos^{-1}(pf))\right)$$

$$Q = 15\ Mvar + 5\ Mvar + (3 \times 40\ MVA \times \sin(\cos^{-1}(0.85)))$$

Example Calculations: Options 11 and 12

$$Q = 83.2\ Mvar$$

Options 11 and 12, Table 1 – Bus Voltage, calls for a 1.0 per unit of the high-side nominal voltage for the generator bus voltage (V_{gen}):

Eq. (136) $$V_{gen} = 1.0\ p.u. \times V_{nom} \times GSU_{ratio}$$

$$V_{gen} = 1.0 \times 345\ kV \times \left(\frac{22\ kV}{346.5\ kV}\right)$$

$$V_{gen} = 21.9\ kV$$

Apparent power (S):

Eq. (137) $$S = P + jQ$$

$$S = 102.0\ MW + j83.2\ Mvar$$

$$S = 131.6\ \angle 39.2°\ MVA$$

Primary current (I_{pri}):

Eq. (138) $$I_{pri} = \frac{S^*}{\sqrt{3} \times V_{gen}}$$

$$I_{pri} = \frac{131.6\ \angle -39.2°\ MVA}{1.73 \times 21.9\ kV}$$

$$I_{pri} = 3473 \angle -39.2°\ A$$

Secondary current (I_{sec}):

Eq. (139) $$I_{sec} = \frac{I_{pri}}{CT_{Asynch_ratio}}$$

$$I_{sec} = \frac{3473 \angle -39.2°\ A}{\frac{5000}{5}}$$

$$I_{sec} = 3.473 \angle -39.2°\ A$$

To satisfy the 130% margin in Options 11 and12:

Eq. (140) $$I_{\mathrm{sec}\,limit} > I_{sec} \times 130\%$$

Example Calculations: Options 11 and 12

$$I_{\text{sec}\,limit} > 3.473\angle -39.2°\ A \times 1.30$$

$$I_{\text{sec}\,limit} > 4.515\angle -39.2°\ A$$

Example Calculations: Options 13a and 13b

Option 13a for the UAT assumes the maximum nameplate rating of the winding is utilized for the purposes of the calculations and the appropriate voltage. Similarly, Option 13b uses the measured current while operating at the maximum gross MW capability reported to the Transmission Planner.

Primary current (I_{pri}):

Eq. (141) $$I_{pri} = \frac{UAT_{nameplate}}{\sqrt{3} \times V_{UAT}}$$

$$I_{pri} = \frac{60\ MVA}{1.73 \times 13.8\ kV}$$

$$I_{pri} = 2510.2\ A$$

Secondary current (I_{sec}):

Eq. (142) $$I_{sec} = \frac{I_{pri}}{CT_{UAT}}$$

$$I_{sec} = \frac{2510.2\ A}{\frac{5000}{5}}$$

$$I_{sec} = 2.51\ \text{A}$$

To satisfy the 150% margin in Options 13a:

Eq. (143) $$I_{\text{sec}\,limit} > I_{sec} \times 150\%$$

$$I_{\text{sec}\,limit} > 2.51\ A \times 1.50$$

$$I_{\text{sec}\,limit} > 3.77\ A$$

Example Calculations: Option 14a

Option 14a represents the calculation for relays installed on the high-side of the GSU transformer, including relays installed on the remote end of line, for Elements that connect a GSU transformer to the Transmission system that are used exclusively to export energy directly from a BES generating unit or generating plant that connected to synchronous generation. In this example, the Element is protected by a phase distance (e.g., 21) relay directional toward the Transmission system. The CTs are located on the high-side of the GSU transformer.

Real Power output (P):

Eq. (144) $$P = GEN_{Synch_nameplate} \times pf$$

$$P = 903\ MVA \times 0.85$$

$$P = 767.6\ MW$$

Reactive Power output (Q):

Eq. (145) $$Q = 120\% \times P$$

$$Q = 1.20 \times 767.6\ MW$$

$$Q = 921.1\ Mvar$$

Option 14a, Table 1 – Bus Voltage, calls for a 0.85 per unit of the line nominal voltage for the GSU transformer voltage (V_{nom}):

Eq. (146) $$V_{bus} = 0.85\ p.u. \times V_{nom}$$

$$V_{gen} = 0.85 \times 345\ kV$$

$$V_{gen} = 293.25\ kV$$

Apparent power (S):

Eq. (147) $$S = P_{Synch_reported} + jQ$$

$$S = 700.0\ MW + j921.1\ Mvar$$

$$S = 1157.0 \angle 52.77°\ MVA$$

$$\theta_{transient\ load\ angle} = 52.77°$$

Example Calculations: Option 14a

Primary impedance (Z_{pri}):

Eq. (148) $$Z_{pri} = \frac{V_{bus}^2}{S^*}$$

$$Z_{pri} = \frac{(293.25\ kV)^2}{1157.0\angle -52.77°\ MVA}$$

$$Z_{pri} = 74.335\angle 52.77°\ \Omega$$

Secondary impedance (Z_{sec}):

Eq. (149) $$Z_{sec} = Z_{pri} \times \frac{CT_{ratio_hv}}{PT_{ratio_hv}}$$

$$Z_{sec} = 74.335\angle 52.77°\ \Omega \times \frac{\frac{2000}{5}}{\frac{2000}{1}}$$

$$Z_{sec} = 74.335\angle 52.77°\ \Omega \times 0.2$$

$$Z_{sec} = 14.867\angle 52.77°\ \Omega$$

To satisfy the 115% margin in Option 14a:

Eq. (150) $$Z_{\text{sec}\,limit} = \frac{Z_{sec}}{115\%}$$

$$Z_{\text{sec}\,limit} = \frac{14.867\angle 52.77°\ \Omega}{1.15}$$

$$Z_{\text{sec}\,limit} = 12.928\angle 52.77°\ \Omega$$

$$\theta_{transient\ load\ angle} = 52.77°$$

Assume a Mho distance impedance relay with a maximum torque angle (MTA) set at 85°, then the maximum allowable impedance reach is:

Eq. (151) $$Z_{max} < \frac{|Z_{\text{sec}\,limit}|}{\cos\left(\theta_{MTA} - \theta_{transient\ load\ angle}\right)}$$

$$Z_{max} < \frac{12.928\ \Omega}{\cos(85.0° - 52.77°)}$$

Example Calculations: Option 14a

$$Z_{max} < \frac{12.928\ \Omega}{0.846}$$

$$Z_{max} < \ 15.283\angle 85.0°\ \Omega$$

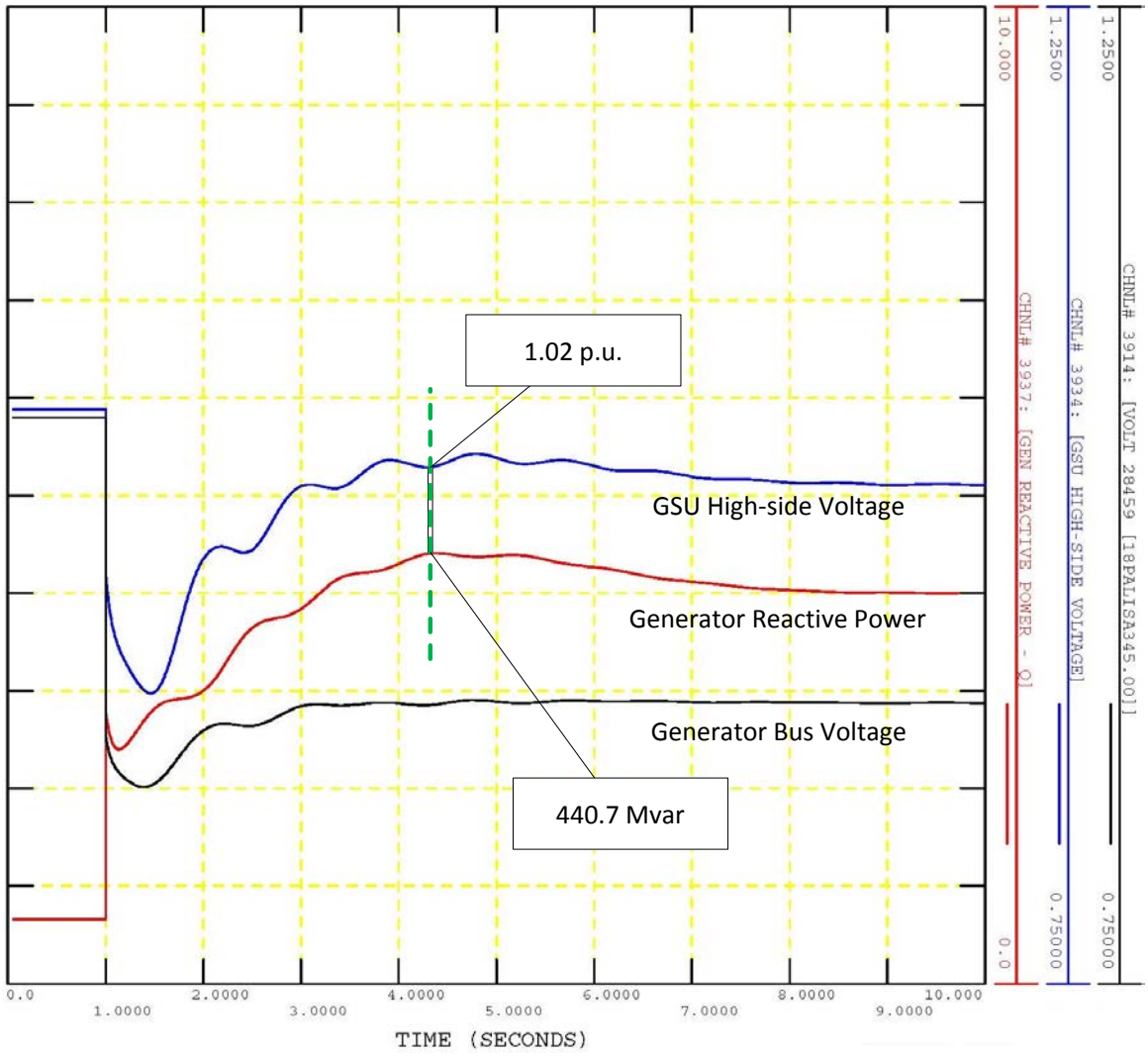
Example Calculations: Option 14b

Option 14b represents the simulation for relays installed on the high-side of the GSU transformer, including relays installed on the remote end of line, for Elements that connect a GSU transformer to the Transmission system that are used exclusively to export energy directly from a BES generating unit or generating plant connected to synchronous generation. In this example, the Element is protected by a phase distance (e.g., 21) relay directional toward the Transmission system. The CTs are located on the high-side of the GSU transformer.

Relays installed on the high-side of the GSU transformer, including relays installed on the remote end of line, simulation is used to determine the simulated line voltage at the relay location coincident with the highest Reactive Power output achieved during field-forcing in response to a 0.85 per unit of the line nominal voltage at the remote end of the line prior to field-forcing. This is achieved by modeling a shunt at the remote end (i.e., at the Transmission system) of the line during simulation.

The maximum Reactive Power flow and coincident voltage for both the high-side of the GSU transformer and remote end of the line are determined by simulation. The maximum Reactive Power output on the high-side of the GSU transformer and remote end of the line during field-forcing is used as these values will correspond to the lowest apparent impedance at the relay location. The corresponding simulated voltage is also used in the calculation. Note that although the excitation limiter reduces the field, the duration of the Reactive Power output achieved for this condition is sufficient to operate a phase distance relay.

Example Calculations: Option 14b



In this simulation the following values are derived:

$$Q = 440.7\ Mvar$$

$$V_{bus_simulated} = 1.02 \times V_{nom} = 351.9\ kV$$

The other value required is the Real Power output which is modeled in the simulation at 100% of the gross MW capability reported to the Transmission Planner. In this case:

$$P_{reported} = 700.0\ MW$$

Apparent power (S):

Eq. (152) $S = P_{Synch_reported} + jQ$

Example Calculations: Option 14b

$$S = 700.0\ MW + j440.7\ Mvar$$

$$S = 827.2\angle 32.2°\ MVA$$

$$\theta_{transient\ load\ angle} = 32.2°$$

Primary impedance (Z_{pri}):

Eq. (153) $$Z_{pri} = \frac{V_{bus_simulated}^2}{S^*}$$

$$Z_{pri} = \frac{(351.9\ kV)^2}{827.2\angle -32.2°\ MVA}$$

$$Z_{pri} = 149.7\angle 32.2°\ \Omega$$

Secondary impedance (Z_{sec}):

Eq. (154) $$Z_{sec} = Z_{pri} \times \frac{CT_{ratio_hv}}{PT_{ratio_hv}}$$

$$Z_{sec} = 149.7\angle 32.2°\ \Omega \times \frac{\frac{2000}{5}}{\frac{2000}{1}}$$

$$Z_{sec} = 149.7\angle 32.2°\ \Omega \times 0.2$$

$$Z_{sec} = 29.9\angle 32.2°\ \Omega$$

To satisfy the 115% margin in Option 14b:

Eq. (155) $$Z_{\mathrm{sec}\,limit} = \frac{Z_{sec}}{115\%}$$

$$Z_{\mathrm{sec}\,limit} = \frac{29.9\angle 32.2°\ \Omega}{1.15}$$

$$Z_{\mathrm{sec}\,limit} = 26.0\angle 32.2°\ \Omega$$

$$\theta_{transient\ load\ angle} = 32.2°$$

Example Calculations: Option 14b

Assume a Mho distance impedance relay with a maximum torque angle (MTA) set at 85°, then the maximum allowable impedance reach is:

Eq. (156) $$Z_{max} < \frac{|Z_{\sec limit}|}{\cos\left(\theta_{MTA} - \theta_{transient\ load\ angle}\right)}$$

$$Z_{max} < \frac{26.0\ \Omega}{\cos(85.0° - 32.2°)}$$

$$Z_{max} < \frac{26.0\ \Omega}{0.61}$$

$$Z_{max} < 43.0 \angle 85.0°\ \Omega$$

Example Calculations: Options 15a and 16a

Options 15a and 16a represent the calculation for relay installed on the high-side of the GSU transformer, including relays installed at the remote end of the line, for Elements that connect a GSU transformer to the Transmission system that are used exclusively to export energy directly from a BES generating unit or generating plant connected to synchronous generation.

Option 15a represents applying a phase time overcurrent relay (e.g., 51) and/or phase instantaneous overcurrent supervisory elements (e.g., 50) associated with current-based, communication-assisted schemes where the scheme is capable of tripping for loss of communications installed on the high-side of the GSU transformer, including relays installed at the remote end of the line.

Option 16a represents applying a phase directional instantaneous overcurrent supervisory element (e.g., 67) associated with current-based, communication-assisted schemes where the scheme is capable of tripping for loss of communications directional toward the Transmission system installed on the high-side of the GSU and at the remote end of the line and/or a phase time directional overcurrent relay (e.g., 67) directional toward the Transmission system installed on the high-side of the GSU transformer, including relays installed at the remote end of the line.

Example calculations are provided for the case, where potential transformers (PT) and current transformers (CT) are located at the high-side of the GSU transformer and the 0.85 per unit of the line nominal voltage at the high-side of the GSU transformer. Example calculations are also provided for the case where PTs and CTs are located at the remote end

Example Calculations: Options 15a and 16a

of the line and the 0.85 per unit of the line nominal voltage will be at the remote bus location.

Calculations at the high-side of the GSU transformer.

Real Power output (P):

Eq. (157) $$P = GEN_{Synch_nameplate} \times pf$$

$$P = 903\ MVA \times 0.85$$

$$P = 767.6\ MW$$

Reactive Power output (Q):

Eq. (158) $$Q = 120\% \times P$$

$$Q = 1.20 \times 767.6\ MW$$

$$Q = 921.12\ Mvar$$

Option 15a, Table 1 – Bus Voltage, calls for a 0.85 per unit of the line nominal voltage:

Eq. (159) $$V_{bus} = 0.85\ p.u. \times V_{nom}$$

$$V_{bus} = 0.85 \times 345\ kV$$

$$V_{bus} = 293.25\ kV$$

Apparent power (S):

Eq. (160) $$S = P_{Synch_reported} + jQ$$

$$S = 700.0\ MW + j921.12\ Mvar$$

$$S = 1157\angle 52.8°\ MVA$$

Primary current (I_{pri}):

Eq. (161) $$I_{pri} = \frac{S^*}{\sqrt{3} \times V_{bus}}$$

$$I_{pri} = \frac{1157\angle -52.8°\ MVA}{1.73 \times 293.25\ kV}$$

Example Calculations: Options 15a and 16a

$$I_{pri} = 2280.6\angle -52.8° \, A$$

Secondary current (I_{sec}):

Eq. (162) $$I_{sec} = \frac{I_{pri}}{CT_{ratio_hv}}$$

$$I_{sec} = \frac{2280.6\angle -52.8° \, A}{\frac{2000}{5}}$$

$$I_{sec} = 5.701 \angle -52.8° \, A$$

To satisfy the 115% margin in Options 15a and 16a:

Eq. (163) $$I_{\text{sec}\,limit} > I_{sec} \times 115\%$$

$$I_{\text{sec}\,limit} > 5.701 \angle -52.8° \, A \times 1.15$$

$$I_{\text{sec}\,limit} > 6.56 \angle -52.8° \, A$$

Calculations at the remote end of the line from the plant.

Real Power output (P):

Eq. (164) $$P = GEN_{Synch_nameplate} \times pf$$

$$P = 903 \, MVA \times 0.85$$

$$P = 767.6 \, MW$$

Reactive Power output (Q):

Eq. (165) $$Q = 120\% \times P$$

$$Q = 1.20 \times 767.6 \, MW$$

$$Q = 921.12 \, Mvar$$

Option 15a and 16a, Table 1 – Bus Voltage, calls for a 0.85 per unit of the line nominal voltage at the relay location, in this example the relay location is at the remote substation bus.

Eq. (166) $$V_{bus_remote_substation} = 0.85 \, p.u. \times V_{nom}$$

$$V_{bus_remote_substation} = 0.85 \times 345 \, kV$$

Example Calculations: Options 15a and 16a

$$V_{bus_remote_substation} = 293.25\ kV$$

Apparent power (S):

Eq. (167) $$S = P_{Synch_reported} + jQ$$

$$S = 700.0\ MW + j921.12\ Mvar$$

$$S = 1157\angle 52.8°\ MVA$$

Primary current (I_{pri}):

Eq. (168) $$I_{pri} = \frac{S^*}{\sqrt{3} \times V_{bus_remote_substation}}$$

$$I_{pri} = \frac{1157\angle -52.8°\ MVA}{1.73 \times 293.25\ kV}$$

$$I_{pri} = 2280.6\angle -52.8°\ A$$

Secondary current (I_{sec}):

Eq. (169) $$I_{sec} = \frac{I_{pri}}{CT_{CT_{ratio_remote_bus}}}$$

$$I_{sec} = \frac{2280.6\angle -52.8°\ A}{\frac{2000}{5}}$$

$$I_{sec} = 5.701 \angle -52.8°\ A$$

To satisfy the 115% margin in Options 15a and 16a:

Eq. (170) $$I_{\text{sec}\,limit} > I_{sec} \times 115\%$$

$$I_{\text{sec}\,limit} > 5.701 \angle -52.8°\ A \times 1.15$$

$$I_{\text{sec}\,limit} > 6.56 \angle -52.8°\ A$$

Example Calculations: Options 15b and 16b

Options 15b and 16b represent the calculation for relays installed on the high-side of the GSU transformer, including relays installed at the remote end of the line, for Elements that connect a GSU transformer to the Transmission system that are used exclusively to export energy directly from a BES generating unit or generating plant connected to synchronous generation.

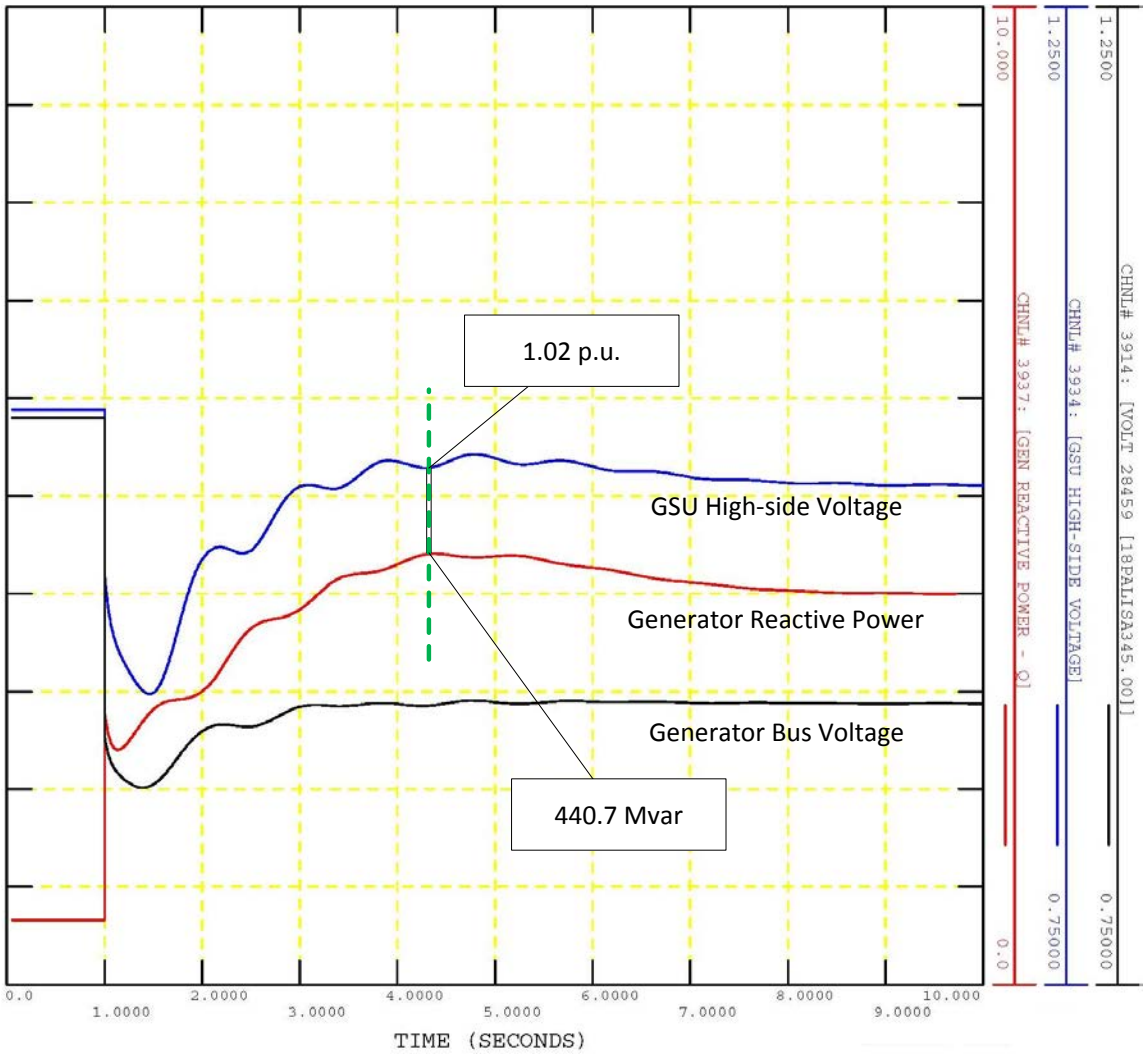
Option 15b represents applying a phase time overcurrent relay (e.g., 51) and/or phase instantaneous overcurrent supervisory elements (e.g., 50) associated with current-based, communication-assisted schemes where the scheme is capable of tripping for loss of communications installed on the high-side of the GSU transformer, including relays at the remote end of the line.

Option 16b represents applying a phase directional instantaneous overcurrent supervisory element (e.g., 67) associated with current-based, communication-assisted schemes where the scheme is capable of tripping for loss of communications directional toward the Transmission system and/or a phase directional time overcurrent relay (e.g., 67) directional toward the Transmission system installed on the high-side of the GSU, including relays at the remote end of the line.

Example calculations are provided for the case where relays are installed on the high-side of the GSU transformer, including relays installed on the remote end of line. Simulation is used to determine the line voltage at the relay location coincident with the highest Reactive Power output achieved during field-forcing in response to a 0.85 per unit of the line nominal voltage at the remote end of the line prior to field-forcing. This is achieved by modeling a shunt at the remote end (i.e., at the Transmission system) of the line during simulation.

The maximum Reactive Power flow and coincident voltage for both the high-side of the GSU transformer and remote end of the line are determined by simulation. The maximum Reactive Power output on the high-side of the GSU transformer and remote end of the line during field-forcing is used as these values will correspond to the lowest apparent impedance at the relay location. The corresponding simulated voltage is also used in the calculation. Note that although the excitation limiter reduces the field, the duration of the Reactive Power output achieved for this condition is sufficient to operate a phase overcurrent relay.

Example Calculations: Options 15b and 16b



In this simulation the following values are derived:

$$Q = 440.7\ Mvar$$

$$V_{bus_simulated} = 1.02 \times V_{nom} = 351.9\ kV$$

The other value required is the Real Power output which is modeled in the simulation at 100% of the gross MW capability reported to the Transmission Planner. In this case:

$$P_{reported} = 700.0\ MW$$

Apparent power (S):

Eq. (171) $S = P_{Synch_reported} + jQ$

Example Calculations: Options 15b and 16b

$$S = 700.0\ MW + j440.7\ Mvar$$

$$S = 827.2\angle 32.2°\ MVA$$

Primary current (I_{pri}):

Eq. (172) $$I_{pri} = \frac{S^*}{\sqrt{3} \times V_{bus_simulated}}$$

$$I_{pri} = \frac{827.2\angle -32.2°\ MVA}{1.73 \times 351.9\ kV}$$

$$I_{pri} = 1357.1\angle -32.2°\ A$$

Secondary current (I_{sec}):

Eq. (173) $$I_{sec} = \frac{I_{pri}}{CT_{ratio_hv}}$$

$$I_{sec} = \frac{1357.1\angle -32.2°\ A}{\frac{2000}{5}}$$

$$I_{sec} = 3.39\angle -32.2°\ A$$

To satisfy the 115% margin in Options 15b and 16b:

Eq. (174) $$I_{\text{sec}\,limit} > I_{sec} \times 115\%$$

$$I_{\text{sec}\,limit} > 3.39\angle -32.2°\ A \times 1.15$$

$$I_{\text{sec}\,limit} > 3.90\angle -32.2°\ A$$

Example Calculations: Option 17

Option 17 represents the calculation for relays installed on the high-side of the GSU transformer, including relays installed on the remote end of line, for Elements that connect a GSU transformer for three asynchronous generators to the Transmission system that are used exclusively to export energy directly from a BES generating unit or generating plant that is applying a phase distance relay (e.g., 21) directional toward the Transmission system. In this application it was assumed 20 Mvar of total static compensation was added.

Example Calculations: Option 17

Real Power output (P):

Eq. (175) $$P_{Asynch} = 3 \times GEN_{Asynch_nameplate} \times pf$$

$$P_{Asynch} = 3 \times 40\ MVA \times 0.85$$

$$P_{Asynch} = 102.0\ MW$$

Reactive Power output (Q):

Eq. (176) $$Q_{Asynch} = MVAR_{static} + MVAR_{gen_static} + \left(3 \times GEN_{Asynch_nameplate} \times \sin(\cos^{-1}(pf))\right)$$

$$Q_{Asynch} = 15\ Mvar + 5\ Mvar + (3 \times 40\ MVA \times \sin(\cos^{-1}(0.85)))$$

$$Q_{Asynch} = 83.2\ Mvar$$

Option 17, Table 1 – Bus Voltage, calls for a 1.0 per unit of the line nominal voltage for the bus voltage (V_{bus}):

Eq. (177) $$V_{bus} = 1.0\ p.u. \times V_{nom}$$

$$V_{gen} = 1.0 \times 345\ kV$$

$$V_{gen} = 345.0\ kV$$

Apparent power (S):

Eq. (178) $$S = P + jQ$$

$$S = 102.0\ MW + j83.2\ Mvar$$

$$S = 131.6\angle 39.2°\ MVA$$

Primary impedance (Z_{pri}):

Eq. (179) $$Z_{pri} = \frac{V_{bus}^2}{S^*}$$

$$Z_{pri} = \frac{(345.0\ kV)^2}{131.6\angle -39.2°\ MVA}$$

$$Z_{pri} = 904.4\angle 39.2°\ \Omega$$

Example Calculations: Option 17

Secondary impedance (Z_{sec}):

Eq. (180) $$Z_{sec} = Z_{pri} \times \frac{CT_{Asynch_ratio_hv}}{PT_{ratio_hv}}$$

$$Z_{sec} = 904.4\angle 39.2° \ \Omega \times \frac{\frac{300}{5}}{\frac{2000}{1}}$$

$$Z_{sec} = 904.4\angle 39.2° \ \Omega \times 0.03$$

$$Z_{sec} = 27.13\angle 39.2° \ \Omega$$

To satisfy the 130% margin in Option 17:

Eq. (181) $$Z_{\text{sec}\,limit} = \frac{Z_{sec}}{130\%}$$

$$Z_{\text{sec}\,limit} = \frac{27.13\angle 39.2° \ \Omega}{1.30}$$

$$Z_{\text{sec}\,limit} = 20.869\angle 39.2° \ \Omega$$

$$\theta_{transient\ load\ angle} = 39.2°$$

Assume a Mho distance impedance relay with a maximum torque angle (MTA) set at 85°, and then the maximum allowable impedance reach is:

Eq. (182) $$Z_{max} < \frac{|Z_{\text{sec}\,limit}|}{\cos\left(\theta_{MTA} - \theta_{transient\ load\ angle}\right)}$$

$$Z_{max} < \frac{20.869 \ \Omega}{\cos(85.0° - 39.2°)}$$

$$Z_{max} < \frac{20.869 \ \Omega}{0.697}$$

$$Z_{max} < \ 29.941\angle 85.0° \ \Omega$$

Example Calculations: Options 18 and 19

Option 18 represents the calculation for relays on relays installed on the high-side of the GSU transformer, including relays installed on the remote end of line, for Elements that connect a

Example Calculations: Options 18 and 19

GSU transformer for three asynchronous generators to the Transmission system that are used exclusively to export energy directly from a BES generating unit or generating plant.

Option 18 represents applying a phase time overcurrent (e.g., 51) and/or phase instantaneous overcurrent supervisory elements (e.g., 50) associated with current-based, communication-assisted schemes where the scheme is capable of tripping for loss of communications installed on the high-side of the GSU transformer, including relays at the remote end of the line.

Similarly, Option 19 may also be applied here for the phase directional overcurrent relays (e.g., 67) directional toward the Transmission system for Elements that connect a GSU transformer, including relays at the remote end of the line to the Transmission system that are used exclusively to export energy directly from a BES generating unit or generating plant. In this application it was assumed 20 Mvar of total static compensation was added.

Real Power output (P):

Eq. (183) $$P = 3 \times GEN_{Asych_nameplate} \times pf$$

$$P = 3 \times 40\ MVA \times 0.85$$

$$P = 102.0\ MW$$

Reactive Power output (Q):

Eq. (184) $$Q = MVAR_{static} + MVAR_{gen_static} + \left(3 \times GEN_{Asynch_nameplate} \times \sin(\cos^{-1}(pf))\right)$$

$$Q = 15\ Mvar + 5\ Mvar + (3 \times 40\ MVA \times \sin(\cos^{-1}(0.85)))$$

$$Q = 83.2\ Mvar$$

Options 18 and 19, Table 1 – Bus Voltage, calls for a 1.0 per unit of the line nominal voltage (V_{bus}):

Eq. (185) $$V_{nom} = 1.0\ p.u. \times V_{nom}$$

$$V_{bus} = 1.0 \times 345\ kV$$

$$V_{bus} = 345\ kV$$

Apparent power (S):

Eq. (186) $$S = P + jQ$$

Example Calculations: Options 18 and 19

$$S = 102.0\ MW + j83.2\ Mvar$$

$$S = 131.6\angle 39.2°\ MVA$$

Primary current (I_{pri}):

Eq. (187) $$I_{pri} = \frac{S^*}{\sqrt{3} \times V_{bus}}$$

$$I_{pri} = \frac{131.6\angle -39.2°\ MVA}{1.73 \times 345\ kV}$$

$$I_{pri} = 220.5 \angle -39.2° A$$

Secondary current (I_{sec}):

Eq. (188) $$I_{sec} = \frac{I_{pri}}{CT_{Asynch_ratio_hv}}$$

$$I_{sec} = \frac{220.5\angle -39.2°\ A}{\frac{300}{5}}$$

$$I_{sec} = 3.675\angle -39.2°\ A$$

To satisfy the 130% margin in Options 18 and 19:

Eq. (189) $$I_{\text{sec}\,limit} > I_{sec} \times 130\%$$

$$I_{\text{sec}\,limit} > 3.675\angle -39.2°\ A \times 1.30$$

$$I_{\text{sec}\,limit} > 4.778\angle -39.2°\ A$$

End of calculations

Rationale

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for R1

Requirement R1 is a risk-based requirement that requires the responsible entity to be aware of each protective relay subject to the standard and applies an appropriate setting based on its calculations or simulation for the conditions established in Attachment 1.

The criteria established in Attachment 1 represent short-duration conditions during which generation Facilities are capable of providing system reactive resources, and for which generation Facilities have been historically recorded to disconnect, causing events to become more severe.

The term, “while maintaining reliable fault protection” in Requirement R1 describes that the responsible entity is to comply with this standard while achieving their desired protection goals. Refer to the Guidelines and Technical Basis, Introduction, for more information.

Appendix PRC-025-2-QC-1
Specific provisions applicable in Québec for standard
PRC-025-2 – Generator Relay Loadability

This appendix establishes specific provisions for the application of the standard in Québec. Provisions of the standard and of this appendix must be read jointly for comprehension and interpretation purposes. Where the standard and appendix differ, the appendix shall prevail.

A. Introduction

1. Title: No specific provisions.

2. Number: No specific provisions.

3. Purpose: No specific provisions.

4. Applicability:

4.1. Functional Entities

No specific provisions.

4.2. Facilities: The following Elements associated with Main Transmission System (RTP) generating units and generating plants, including those generating units and generating plants identified as Blackstart Resources in the Transmission Operator's system restoration plan:

4.2.1 No specific provisions.

4.2.2 No specific provisions.

4.2.3 No specific provisions.

4.2.4 Elements that connect the GSU transformer(s) to the Transmission system that are used exclusively to export energy directly from a RTP generating unit or generating plant, except that Elements may also supply generating plant loads.

4.2.5 No specific provisions.

4.3. Exemptions: The generating facilities that are not connected to the RTP are exempted from the application of this standard.

In the application of this standard, all references to the terms "Bulk Electric System" or "BES" shall be replaced by the terms "Main Transmission System" or "RTP" respectively.

5. Effective dates for Québec:

5.1. Adoption of the standard by the Régie de l'énergie: September 1st, 2022

5.2. Adoption of the appendix by the Régie de l'énergie: September 1st, 2022

5.3. Effective date of the standard and appendix for Québec: October 1st , 2022

IMPLEMENTATION PLAN OF THE PRC-025-2 STANDARD

Table 1

Load responsive protective relays subject to the PRC-025-2 and that were subject to the PRC-025-1 standard

Requirement	Applicability	Date of enforcement in Québec
E1	For entities affective by the standard in which replacement or removal is not necessary, except as noted in the Table 3 listed below.	October 1st, 2022
	For entities affective by the standard in which replacement or removal is necessary, except as noted in the Table 3 listed below.	October 1st, 2023

Table 2

Load responsive protective relays newly subject to the PRC-025-2 standard

Requirement	Applicability	Implementation timeline in Québec	Date of enforcement in Québec
E1	For entities affective by the standard in which replacement or removal is not necessary, except as noted in the Table 3 listed below.	60 months	October 1st, 2027
	For entities affective by the standard in which replacement or removal is necessary, except as noted in the Table 3 listed below.	84 months	October 1st, 2029

Table 3

Phased-In Implementation of specific PRC-025-2 Table 1 Relay Loadability Evaluation Criteria Options

Option	Applicability	Implementation timeline in Québec	Date of enforcement in Québec
5b	For entities affective by the standard in which replacement or	24 months	October 1st, 2024

Table 3

Phased-In Implementation of specific PRC-025-2 Table 1 Relay Loadability Evaluation Criteria Options

Option	Applicability	Implementation timeline in Québec	Date of enforcement in Québec
Asynchronous generating unit(s) (including inverter-based installations,) including Element utilized in the aggregation of dispersed power producing resources applying any phase overcurrent relay (e.g., 51, or 51V-R – voltage restrained)	removal is not necessary		
	For entities affective by the standard in which replacement or removal is necessary	48 months	October 1st, 2026
2a, 2b and 2c (element 50 only) Synchronous generating units(s) (including inverter-based installations), including Elements utilized in the aggregation of dispersed power producing resources applying specifically the phase overcurrent relay 50 element.	For entities affective by the standard in which replacement or removal is not necessary	60 months	October 1st, 2027
	For entities affective by the standard in which replacement or removal is necessary	84 months	October 1st, 2029
5a and 5b (element 50 only) Asynchronous generating unit(s), including Elements utilized in the aggregation of dispersed power producing resources applying specifically the phase overcurrent relay 50 element.	For entities affective by the standard in which replacement or removal is not necessary	60 months	October 1st, 2027
	For entities affective by the standard in which replacement or removal is necessary	84 months	October 1st, 2029
Options 8a, 8b, and 8c (50 element only) Generator step-up transformer(s) connected to synchronous generators	For entities affective by the standard in which replacement or removal is not necessary	60 months	October 1st, 2027

Table 3 **Phased-In Implementation of specific PRC-025-2 Table 1 Relay Loadability Evaluation Criteria Options**			
Option	**Applicability**	**Implementation timeline in Québec**	**Date of enforcement in Québec**
applying, specifically the phase overcurrent relay 50 element installed on generator-side of the GSU transformer.	For entities affective by the standard in which replacement or removal is necessary	84 months	October 1st, 2029
11 (50 element only) Generator step-up transformer(s) connected to asynchronous generators only (including inverter-based installations) apply, specifically the phase overcurrent 50 element installed on the generator side of the GSU transformer	For entities affective by the standard in which replacement or removal is not necessary	60 months	October 1st, 2027
	For entities affective by the standard in which replacement or removal is necessary	84 months	October 1st, 2029
13a and 13b (50 element only) Unit auxiliary transformer(s) (UAT) applying, specifically the phase overcurrent 50 element applied at the high-side terminals of the UAT, for which operation of the relay will cause the associated generator to trip.	For entities affective by the standard in which replacement or removal is not necessary	60 months	October 1st, 2027
	For entities affective by the standard in which replacement or removal is necessary	84 months	October 1st, 2029
14b Relays installed on the high-side of the GSU transformer, including relays installed on the remote end of line, for Elements that connect the GSU transformer(s) to the Transmission system that are used exclusively to export energy directly from	For entities affective by the standard in which replacement or removal is not necessary	24 months	October 1st, 2024
	For entities affective by the standard in which replacement or removal is necessary	48 months	October 1st, 2026

Table 3 **Phased-In Implementation of specific PRC-025-2 Table 1 Relay Loadability Evaluation Criteria Options**			
Option	**Applicability**	**Implementation timeline in Québec**	**Date of enforcement in Québec**
a RTP generating unit or generating plant (except that Elements may also supply generating plant loads) – connected to synchronous generators applying a phase distance relay (e.g., 21) – directional toward the Transmission system			
15b Relays installed on the high-side of the GSU transformer, including relays installed at the remote end of the line, for Elements that connect the GSU transformer(s) to the Transmission system that are used exclusively to export energy directly from a RTP generating unit or generating plant (except that Elements may also supply generating plant loads) –connected to synchronous generators applying a phase instantaneous overcurrent supervisory element (e.g., 50) – associated with current-based, communication-assisted schemes where the scheme is capable of tripping for loss of communications and/or phase time overcurrent relay (e.g., 51)	For entities affective by the standard in which replacement or removal is not necessary	24 months	October 1st, 2024
	For entities affective by the standard in which replacement or removal is necessary	48 months	October 1st, 2026

Table 3

Phased-In Implementation of specific PRC-025-2 Table 1 Relay Loadability Evaluation Criteria Options

Option	Applicability	Implementation timeline in Québec	Date of enforcement in Québec
16b Relays installed on the high-side of the GSU transformer, including relays installed at the remote end of the line, for Elements that connect the GSU transformer(s) to the Transmission system that are used exclusively to export energy directly from a RTP generating unit or generating plant (except that Elements may also supply generating plant load.) – connected to synchronous generators applying Phase directional instantaneous overcurrent supervisory element (e.g., 67) – associated with current-based, communication assisted schemes where the scheme is capable of tripping for loss of communications directional toward the Transmission system and/or phase directional time overcurrent relay (e.g., 67) –directional toward the Transmission system	For entities affective by the standard in which replacement or removal is not necessary	24 months	October 1st , 2024
	For entities affective by the standard in which replacement or removal is necessary	48 months	October 1st, 2026

6. **Background:** No specific provisions.

7. **Standard Only Definition:** No specific provisions.

B. Requirements and measures

No specific provisions.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

In Québec, "Compliance Enforcement Authority" means the Régie de l'énergie in its roles of monitoring and enforcing compliance with respect to the Reliability Standard and to this appendix.

1.2. Evidence Retention

No specific provisions.

Violation Severity Levels

No specific provisions.

D. Regional Variances

No specific provisions.

E. Associated Documents

No specific provisions.

PRC-025-2 Attachment 1: Relay Settings

In the application of this standard, all references to the terms "Bulk Electric System" or "BES" shall be replaced by the terms "Main Transmission System" or "RTP" respectively.

PRC-025-2 Guidelines and Technical Basis

In the application of this standard, all references to the terms "Bulk Electric System" or "BES" shall be replaced by the terms "Main Transmission System" or "RTP" respectively.

Table 1 – Options

In the application of this standard, all references to the terms "Bulk Electric System" or "BES" shall be replaced by the terms "Main Transmission System" or "RTP" respectively.

Rationale

No specific provisions.

Version history

Version	Date	Action	Change tracking
1	September 1st, 2022	New appendix as per decision D-2022-108.	New

A. Introduction

1. **Title:** **Relay Performance During Stable Power Swings**

2. **Number:** **PRC-026-1**

3. **Purpose:** To ensure that load-responsive protective relays are expected to not trip in response to stable power swings during non-Fault conditions.

4. **Applicability:**

   4.1. Functional Entities:

   4.1.1 Generator Owner that applies load-responsive protective relays as described in PRC-026-1 – Attachment A at the terminals of the Elements listed in Section 4.2, Facilities.

   4.1.2 Planning Coordinator.

   4.1.3 Transmission Owner that applies load-responsive protective relays as described in PRC-026-1 – Attachment A at the terminals of the Elements listed in Section 4.2, Facilities.

   4.2. Facilities: The following Elements that are part of the Bulk Electric System (BES):

   4.2.1 Generators.

   4.2.2 Transformers.

   4.2.3 Transmission lines.

5. **Background:**

   This is the third phase of a three-phased standard development project that focused on developing this new Reliability Standard to address protective relay operations due to stable power swings. The March 18, 2010, Federal Energy Regulatory Commission (FERC) Order No. 733 approved Reliability Standard PRC-023-1 – Transmission Relay Loadability. In that Order, FERC directed NERC to address three areas of relay loadability that include modifications to the approved PRC-023-1, development of a new Reliability Standard to address generator protective relay loadability, and a new Reliability Standard to address the operation of protective relays due to stable power swings. This project's SAR addresses these directives with a three-phased approach to standard development.

   Phase 1 focused on making the specific modifications from FERC Order No. 733 to PRC-023-1. Reliability Standard PRC-023-2, which incorporated these modifications, became mandatory on July 1, 2012.

   Phase 2 focused on developing a new Reliability Standard, PRC-025-1 – Generator Relay Loadability, to address generator protective relay loadability. PRC-025-1 became mandatory on October 1, 2014, along with PRC-023-3, which was modified to harmonize PRC-023-2 with PRC-025-1.

   Phase 3 focuses on preventing protective relays from tripping unnecessarily due to stable power swings by requiring identification of Elements on which a stable or unstable power swing may affect Protection System operation, assessment of the security of load-

responsive protective relays to tripping in response to only a stable power swing, and implementation of Corrective Action Plans (CAP), where necessary. Phase 3 improves security of load-responsive protective relays for stable power swings so they are expected to not trip in response to stable power swings during non-Fault conditions while maintaining dependable fault detection and dependable out-of-step tripping.

6. Effective Dates:

Requirement R1

First day of the first full calendar year that is 12 months after the date that the standard is approved by an applicable governmental authority or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective on the first day of the first full calendar year that is 12 months after the date the standard is adopted by the NERC Board of Trustees or as otherwise provided for in that jurisdiction.

Requirements R2, R3, and R4

First day of the first full calendar year that is 36 months after the date that the standard is approved by an applicable governmental authority or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective on the first day of the first full calendar year that is 36 months after the date the standard is adopted by the NERC Board of Trustees or as otherwise provided for in that jurisdiction.

B. Requirements and Measures

R1. Each Planning Coordinator shall, at least once each calendar year, provide notification of each generator, transformer, and transmission line BES Element in its area that meets one or more of the following criteria, if any, to the respective Generator Owner and Transmission Owner: *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

Criteria:

1. Generator(s) where an angular stability constraint exists that is addressed by a System Operating Limit (SOL) or a Remedial Action Scheme (RAS) and those Elements terminating at the Transmission station associated with the generator(s).
2. An Element that is monitored as part of an SOL identified by the Planning Coordinator's methodology[1] based on an angular stability constraint.
3. An Element that forms the boundary of an island in the most recent underfrequency load shedding (UFLS) design assessment based on application of the Planning Coordinator's criteria for identifying islands, only if the island is formed by tripping the Element due to angular instability.
4. An Element identified in the most recent annual Planning Assessment where relay tripping occurs due to a stable or unstable[2] power swing during a simulated disturbance.

M1. Each Planning Coordinator shall have dated evidence that demonstrates notification of the generator, transformer, and transmission line BES Element(s) that meet one or more of the criteria in Requirement R1, if any, to the respective Generator Owner and Transmission Owner. Evidence may include, but is not limited to, the following documentation: emails, facsimiles, records, reports, transmittals, lists, or spreadsheets.

[1] NERC Reliability Standard FAC-014-2 – Establish and Communicate System Operating Limits, Requirement R3.

[2] An example of an unstable power swing is provided in the Guidelines and Technical Basis section, "Justification for Including Unstable Power Swings in the Requirements section of the Guidelines and Technical Basis."

R2. Each Generator Owner and Transmission Owner shall: [Violation Risk Factor: High] [Time Horizon: Operations Planning]

2.1 Within 12 full calendar months of notification of a BES Element pursuant to Requirement R1, determine whether its load-responsive protective relay(s) applied to that BES Element meets the criteria in PRC-026-1 – Attachment B where an evaluation of that Element's load-responsive protective relay(s) based on PRC-026-1 – Attachment B criteria has not been performed in the last five calendar years.

2.2 Within 12 full calendar months of becoming aware[3] of a generator, transformer, or transmission line BES Element that tripped in response to a stable or unstable[4] power swing due to the operation of its protective relay(s), determine whether its load-responsive protective relay(s) applied to that BES Element meets the criteria in PRC-026-1 – Attachment B.

M2. Each Generator Owner and Transmission Owner shall have dated evidence that demonstrates the evaluation was performed according to Requirement R2. Evidence may include, but is not limited to, the following documentation: apparent impedance characteristic plots, email, design drawings, facsimiles, R-X plots, software output, records, reports, transmittals, lists, settings sheets, or spreadsheets.

R3. Each Generator Owner and Transmission Owner shall, within six full calendar months of determining a load-responsive protective relay does not meet the PRC-026-1 – Attachment B criteria pursuant to Requirement R2, develop a Corrective Action Plan (CAP) to meet one of the following: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

- The Protection System meets the PRC-026-1 – Attachment B criteria, while maintaining dependable fault detection and dependable out-of-step tripping (if out-of-step tripping is applied at the terminal of the BES Element); or
- The Protection System is excluded under the PRC-026-1 – Attachment A criteria (e.g., modifying the Protection System so that relay functions are supervised by power swing blocking or using relay systems that are immune to power swings), while maintaining dependable fault detection and dependable out-of-step tripping (if out-of-step tripping is applied at the terminal of the BES Element).

M3. The Generator Owner and Transmission Owner shall have dated evidence that demonstrates the development of a CAP in accordance with Requirement R3. Evidence may include, but is not limited to, the following documentation: corrective action plans, maintenance records, settings sheets, project or work management program records, or work orders.

R4. Each Generator Owner and Transmission Owner shall implement each CAP developed pursuant to Requirement R3 and update each CAP if actions or timetables change until all actions are complete. *[Violation Risk Factor: Medium][Time Horizon: Long-Term Planning]*

M4. The Generator Owner and Transmission Owner shall have dated evidence that demonstrates implementation of each CAP according to Requirement R4, including updates to the CAP when actions or timetables change. Evidence may include, but is not limited to, the following documentation: corrective action plans, maintenance records, settings sheets, project or work management program records, or work orders.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Generator Owner, Planning Coordinator, and Transmission Owner shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation.

- The Planning Coordinator shall retain evidence of Requirement R1 for a minimum of one calendar year following the completion of the Requirement.
- The Generator Owner and Transmission Owner shall retain evidence of Requirement R2 evaluation for a minimum of 12 calendar months following completion of each evaluation where a CAP is not developed.
- The Generator Owner and Transmission Owner shall retain evidence of Requirements R2, R3, and R4 for a minimum of 12 calendar months following completion of each CAP.

If a Generator Owner, Planning Coordinator, or Transmission Owner is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved, or for the time specified above, whichever is longer.

---

[3] Some examples of the ways an entity may become aware of a power swing are provided in the Guidelines and Technical Basis section, "Becoming Aware of an Element That Tripped in Response to a Power Swing."

[4] An example of an unstable power swing is provided in the Guidelines and Technical Basis section, "Justification for Including Unstable Power Swings in the Requirements section of the Guidelines and Technical Basis."

The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

As defined in the NERC Rules of Procedure; "Compliance Monitoring and Assessment Processes" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated reliability standard.

1.4. Additional Compliance Information

None.

Table of Compliance Elements

R#	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	Long-term Planning	Medium	The Planning Coordinator provided notification of the BES Element(s) in accordance with Requirement R1, but was less than or equal to 30 calendar days late.	The Planning Coordinator provided notification of the BES Element(s) in accordance with Requirement R1, but was more than 30 calendar days and less than or equal to 60 calendar days late.	The Planning Coordinator provided notification of the BES Element(s) in accordance with Requirement R1, but was more than 60 calendar days and less than or equal to 90 calendar days late.	The Planning Coordinator provided notification of the BES Element(s) in accordance with Requirement R1, but was more than 90 calendar days late. OR The Planning Coordinator failed to provide notification of the BES Element(s) in accordance with Requirement R1.

R#	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R2	Operations Planning	High	The Generator Owner or Transmission Owner evaluated its load-responsive protective relay(s) in accordance with Requirement R2, but was less than or equal to 30 calendar days late.	The Generator Owner or Transmission Owner evaluated its load-responsive protective relay(s) in accordance with Requirement R2, but was more than 30 calendar days and less than or equal to 60 calendar days late.	The Generator Owner or Transmission Owner evaluated its load-responsive protective relay(s) in accordance with Requirement R2, but was more than 60 calendar days and less than or equal to 90 calendar days late.	The Generator Owner or Transmission Owner evaluated its load-responsive protective relay(s) in accordance with Requirement R2, but was more than 90 calendar days late. OR The Generator Owner or Transmission Owner failed to evaluate its load-responsive protective relay(s) in accordance with Requirement R2.

R#	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R3	Long-term Planning	Medium	The Generator Owner or Transmission Owner developed a Corrective Action Plan (CAP) in accordance with Requirement R3, but in more than six calendar months and less than or equal to seven calendar months.	The Generator Owner or Transmission Owner developed a Corrective Action Plan (CAP) in accordance with Requirement R3, but in more than seven calendar months and less than or equal to eight calendar months.	The Generator Owner or Transmission Owner developed a Corrective Action Plan (CAP) in accordance with Requirement R3, but in more than eight calendar months and less than or equal to nine calendar months.	The Generator Owner or Transmission Owner developed a Corrective Action Plan (CAP) in accordance with Requirement R3, but in more than nine calendar months. OR The Generator Owner or Transmission Owner failed to develop a CAP in accordance with Requirement R3.
R4	Long-term Planning	Medium	The Generator Owner or Transmission Owner implemented a Corrective Action Plan (CAP), but failed to update a CAP when actions or timetables changed, in accordance with Requirement R4.	N/A	N/A	The Generator Owner or Transmission Owner failed to implement a Corrective Action Plan (CAP) in accordance with Requirement R4.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

Applied Protective Relaying, Westinghouse Electric Corporation, 1979.

Burdy, John, *Loss-of-excitation Protection for Synchronous Generators GER-3183*, General Electric Company.

IEEE Power System Relaying Committee WG D6, *Power Swing and Out-of-Step Considerations on Transmission Lines*, July 2005: http://www.pes-psrc.org/Reports/Power%20Swing%20and%20OOS%20Considerations%20on%20Transmission%20Lines%20F..pdf.

Kimbark Edward Wilson, *Power System Stability, Volume II: Power Circuit Breakers and Protective Relays*, Published by John Wiley and Sons, 1950.

Kundur, Prabha, *Power System Stability and Control*, 1994, Palo Alto: EPRI, McGraw Hill, Inc.

NERC System Protection and Control Subcommittee, *Protection System Response to Power Swings*, August 2013: http://www.nerc.com/comm/PC/System%20Protection%20and%20Control%20Subcommittee%20SPCS%2020/SPCS%20Power%20Swing%20Report_Final_20131015.pdf.

Reimert, Donald, *Protective Relaying for Power Generation Systems*, 2006, Boca Raton: CRC Press.

Version History

Version	Date	Action	Change Tracking
1	November 13, 2014	Adopted by NERC Board of Trustees	New
1	March 17, 2016	FERC Order issued approving PRC-026-1. Docket No. RM15-8-000.	

PRC-026-1 – Attachment A

This standard applies to any protective functions which could trip instantaneously or with a time delay of less than 15 cycles on load current (i.e., "load-responsive") including, but not limited to:

- Phase distance
- Phase overcurrent
- Out-of-step tripping
- Loss-of-field

The following protection functions are excluded from Requirements of this standard:

- Relay elements supervised by power swing blocking
- Relay elements that are only enabled when other relays or associated systems fail. For example:
    - Overcurrent elements that are only enabled during loss of potential conditions.
    - Relay elements that are only enabled during a loss of communications
- Thermal emulation relays which are used in conjunction with dynamic Facility Ratings
- Relay elements associated with direct current (dc) lines
- Relay elements associated with dc converter transformers
- Phase fault detector relay elements employed to supervise other load-responsive phase distance elements (i.e., in order to prevent false operation in the event of a loss of potential)
- Relay elements associated with switch-onto-fault schemes
- Reverse power relay on the generator
- Generator relay elements that are armed only when the generator is disconnected from the system, (e.g., non-directional overcurrent elements used in conjunction with inadvertent energization schemes, and open breaker flashover schemes)
- Current differential relay, pilot wire relay, and phase comparison relay
- Voltage-restrained or voltage-controlled overcurrent relays

PRC-026-1 – Attachment B

Criterion A:

An impedance-based relay used for tripping is expected to not trip for a stable power swing, when the relay characteristic is completely contained within the unstable power swing region.[5] The unstable power swing region is formed by the union of three shapes in the impedance (R-X) plane; (1) a lower loss-of-synchronism circle based on a ratio of the sending-end to receiving-end voltages of 0.7; (2) an upper loss-of-synchronism circle based on a ratio of the sending-end to receiving-end voltages of 1.43; (3) a lens that connects the endpoints of the total system impedance (with the parallel transfer impedance removed) bounded by varying the sending-end and receiving-end voltages from 0.0 to 1.0 per unit, while maintaining a constant system separation angle across the total system impedance where:

1. The system separation angle is:
   - At least 120 degrees, or
   - An angle less than 120 degrees where a documented transient stability analysis demonstrates that the expected maximum stable separation angle is less than 120 degrees.
2. All generation is in service and all transmission BES Elements are in their normal operating state when calculating the system impedance.
3. Saturated (transient or sub-transient) reactance is used for all machines.

[5] Guidelines and Technical Basis, Figures 1 and 2.

PRC-026-1 – Attachment B

Criterion B:

The pickup of an overcurrent relay element used for tripping, that is above the calculated current value (with the parallel transfer impedance removed) for the conditions below:

1. The system separation angle is:
   - At least 120 degrees, or
   - An angle less than 120 degrees where a documented transient stability analysis demonstrates that the expected maximum stable separation angle is less than 120 degrees.
2. All generation is in service and all transmission BES Elements are in their normal operating state when calculating the system impedance.
3. Saturated (transient or sub-transient) reactance is used for all machines.
4. Both the sending-end and receiving-end voltages at 1.05 per unit.

Guidelines and Technical Basis

Introduction

The NERC System Protection and Control Subcommittee technical document, *Protection System Response to Power Swings*, August 2013,[6] ("PSRPS Report" or "report") was specifically prepared to support the development of this NERC Reliability Standard. The report provided a historical perspective on power swings as early as 1965 up through the approval of the report by the NERC Planning Committee. The report also addresses reliability issues regarding trade-offs between security and dependability of Protection Systems, considerations for this NERC Reliability Standard, and a collection of technical information about power swing characteristics and varying issues with practical applications and approaches to power swings. Of these topics, the report suggests an approach for this NERC Reliability Standard ("standard" or "PRC-026-1") which is consistent with addressing three regulatory directives in the FERC Order No. 733. The first directive concerns the need for "…protective relay systems that differentiate between faults and stable power swings and, when necessary, phases out protective relay systems that cannot meet this requirement."[7] Second, is "…to develop a Reliability Standard addressing undesirable relay operation due to stable power swings."[8] The third directive "…to consider "islanding" strategies that achieve the fundamental performance for all islands in developing the new Reliability Standard addressing stable power swings"[9] was considered during development of the standard.

The development of this standard implements the majority of the approaches suggested by the report. However, it is noted that the Reliability Coordinator and Transmission Planner have not been included in the standard's Applicability section (as suggested by the PSRPS Report). This is so that a single entity, the Planning Coordinator, may be the single source for identifying Elements according to Requirement R1. A single source will insure that multiple entities will not identify Elements in duplicate, nor will one entity fail to provide an Element because it believes the Element is being provided by another entity. The Planning Coordinator has, or has access to, the wide-area model and can correctly identify the Elements that may be susceptible to a stable or unstable power swing. Additionally, not including the Reliability Coordinator and Transmission Planner is consistent with the applicability of other relay loadability NERC Reliability Standards (e.g., PRC-023 and PRC-025). It is also consistent with the NERC Functional Model.

The phrase, "while maintaining dependable fault detection and dependable out-of-step tripping" in Requirement R3, describes that the Generator Owner and Transmission Owner are to comply with this standard while achieving its desired protection goals. Load-responsive protective relays, as addressed within this standard, may be intended to provide a variety of backup protection functions, both within the generating unit or generating plant and on the transmission system, and

---

[6] NERC System Protection and Control Subcommittee, *Protection System Response to Power Swings*, August 2013: http://www.nerc.com/comm/PC/System%20Protection%20and%20Control%20Subcommittee%20SPCS%2020/SPCS%20Power%20Swing%20Report_Final_20131015.pdf)

[7] Transmission Relay Loadability Reliability Standard, Order No. 733, P.150 FERC ¶ 61,221 (2010).

[8] Ibid. P.153.

[9] Ibid. P.162.

this standard is not intended to result in the loss of these protection functions. Instead, the Generator Owner and Transmission Owner must consider both the Requirements within this standard and its desired protection goals and perform modifications to its protective relays or protection philosophies as necessary to achieve both.

Power Swings

The IEEE Power System Relaying Committee WG D6 developed a technical document called *Power Swing and Out-of-Step Considerations on Transmission Lines* (July 2005) that provides background on power swings. The following are general definitions from that document:[10]

> Power Swing: a variation in three phase power flow which occurs when the generator rotor angles are advancing or retarding relative to each other in response to changes in load magnitude and direction, line switching, loss of generation, faults, and other system disturbances.
>
> Pole Slip: a condition whereby a generator, or group of generators, terminal voltage angles (or phases) go past 180 degrees with respect to the rest of the connected power system.
>
> Stable Power Swing: a power swing is considered stable if the generators do not slip poles and the system reaches a new state of equilibrium, i.e. an acceptable operating condition.
>
> Unstable Power Swing: a power swing that will result in a generator or group of generators experiencing pole slipping for which some corrective action must be taken.
>
> Out-of-Step Condition: Same as an unstable power swing.
>
> Electrical System Center or Voltage Zero: it is the point or points in the system where the voltage becomes zero during an unstable power swing.

Burden to Entities

The PSRPS Report provides a technical basis and approach for focusing on Protection Systems, which are susceptible to power swings, while achieving the purpose of the standard. The approach reduces the number of relays to which the PRC-026-1 Requirements would apply by first identifying the BES Element(s) on which load-responsive protective relays must be evaluated. The first step uses criteria to identify the Elements on which a Protection System is expected to be challenged by power swings. Of those Elements, the second step is to evaluate each load-responsive protective relay that is applied on each identified Element. Rather than requiring the Planning Coordinator or Transmission Planner to perform simulations to obtain information for each identified Element, the Generator Owner and Transmission Owner will reduce the need for simulation by comparing the load-responsive protective relay characteristic to specific criteria in PRC-026-1 – Attachment B.

[10] http://www.pes-psrc.org/Reports/Power%20Swing%20and%20OOS%20Considerations%20on%20Transmission%20Lines%20F..pdf.

Applicability

The standard is applicable to the Generator Owner, Planning Coordinator, and Transmission Owner entities. More specifically, the Generator Owner and Transmission Owner entities are applicable when applying load-responsive protective relays at the terminals of the applicable BES Elements. The standard is applicable to the following BES Elements: generators, transformers, and transmission lines. The Distribution Provider was considered for inclusion in the standard; however, it is not subject to the standard because this entity, by functional registration, would not own generators, transmission lines, or transformers other than load serving.

Load-responsive protective relays include any protective functions which could trip with or without time delay, on load current.

Requirement R1

The Planning Coordinator has a wide-area view and is in the position to identify what, if any, Elements meet the criteria. The criterion-based approach is consistent with the NERC System Protection and Control Subcommittee (SPCS) technical document, *Protection System Response to Power Swings (*August 2013),[11] which recommends a focused approach to determine an at-risk Element. Identification of Elements comes from the annual Planning Assessments pursuant to the transmission planning (i.e., "TPL") and other NERC Reliability Standards (e.g., PRC-006), and the standard is not requiring any other assessments to be performed by the Planning Coordinator. The required notification on a calendar year basis to the respective Generator Owner and Transmission Owner is sufficient because it is expected that the Planning Coordinator will make its notifications following the completion of its annual Planning Assessments. The Planning Coordinator will continue to provide notification of Elements on a calendar year basis even if a study is performed less frequently (e.g., PRC-006 – Automatic Underfrequency Load Shedding, which is five years) and has not changed. It is possible that a Planning Coordinator could utilize studies from a prior year in determining the necessary notifications pursuant to Requirement R1.

Criterion 1

The first criterion involves generator(s) where an angular stability constraint exists that is addressed by a System Operating Limit (SOL) or a Remedial Action Scheme (RAS) and those Elements terminating at the Transmission station associated with the generator(s). For example, a scheme to remove generation for specific conditions is implemented for a four-unit generating plant (1,100 MW). Two of the units are 500 MW each; one is connected to the 345 kV system and one is connected to the 230 kV system. The Transmission Owner has two 230 kV transmission lines and one 345 kV transmission line all terminating at the generating facility as well as a 345/230 kV autotransformer. The remaining 100 MW consists of two 50 MW combustion turbine (CT) units connected to four 66 kV transmission lines. The 66 kV transmission lines are not electrically joined to the 345 kV and 230 kV transmission lines at the plant site and are not subject to the operating limit or RAS. A stability constraint limits the output of the portion of the plant affected

[11] http://www.nerc.com/comm/PC/System%20Protection%20and%20Control%20Subcommittee%20SPCS%20 20/SPCS%20Power%20Swing%20Report_Final_20131015.pdf)

by the RAS to 700 MW for an outage of the 345 kV transmission line. The RAS trips one of the 500 MW units to maintain stability for a loss of the 345 kV transmission line when the total output from both 500 MW units is above 700 MW. For this example, both 500 MW generating units and the associated generator step-up (GSU) transformers would be identified as Elements meeting this criterion. The 345/230 kV autotransformer, the 345 kV transmission line, and the two 230 kV transmission lines would also be identified as Elements meeting this criterion. The 50 MW combustion turbines and 66 kV transmission lines would not be identified pursuant to Criterion 1 because these Elements are not subject to an operating limit or RAS and do not terminate at the Transmission station associated with the generators that are subject to the SOL or RAS.

Criterion 2

The second criterion involves Elements that are monitored as a part of an established System Operating Limit (SOL) based on an angular stability limit regardless of the outage conditions that result in the enforcement of the SOL. For example, if two long parallel 500 kV transmission lines have a combined SOL of 1,200 MW, and this limit is based on angular instability resulting from a fault and subsequent loss of one of the two lines, then both lines would be identified as Elements meeting the criterion.

Criterion 3

The third criterion involves Elements that form the boundary of an island within an underfrequency load shedding (UFLS) design assessment. The criterion applies to islands identified based on application of the Planning Coordinator's criteria for identifying islands, where the island is formed by tripping the Elements based on angular instability. The criterion applies if the angular instability is modeled in the UFLS design assessment, or if the boundary is identified "off-line" (i.e., the Elements are selected based on angular instability considerations, but the Elements are tripped in the UFLS design assessment without modeling the initiating angular instability). In cases where an out-of-step condition is detected and tripping is initiated at an alternate location, the criterion applies to the Element on which the power swing is detected. The criterion does not apply to islands identified based on other considerations that do not involve angular instability, such as excessive loading, Planning Coordinator area boundary tie lines, or Balancing Authority boundary tie lines.

Criterion 4

The fourth criterion involves Elements identified in the most recent annual Planning Assessment where relay tripping occurs due to a stable or unstable[12] power swing during a simulated disturbance. The intent is for the Planning Coordinator to include any Element(s) where relay tripping was observed during simulations performed for the most recent annual Planning Assessment associated with the transmission planning TPL-001-4 Reliability Standard. Note that relay tripping must be assessed within those annual Planning Assessments per TPL-001-4, R4,

[12] Refer to the "Justification for Including Unstable Power Swings in the Requirements" section.

Part 4.3.1.3, which indicates that analysis shall include the "Tripping of Transmission lines and transformers where transient swings cause Protection System operation based on generic or actual relay models." Identifying such Elements according to Criterion 4 and notifying the respective Generator Owner and Transmission Owner will require that the owners of any load-responsive protective relay applied at the terminals of the identified Element evaluate the relay's susceptibility to tripping in response to a stable power swing.

Planning Coordinators have the discretion to determine whether the observed tripping for a power swing in its Planning Assessments occurs for valid contingencies and system conditions. The Planning Coordinator will address tripping that is observed in transient analyses on an individual basis; therefore, the Planning Coordinator is responsible for identifying the Elements based only on simulation results that are determined to be valid.

Due to the nature of how a Planning Assessment is performed, there may be cases where a previously-identified Element is not identified in the most recent annual Planning Assessment. If so, this is acceptable because the Generator Owner and Transmission Owner would have taken action upon the initial notification of the previously identified Element. When an Element is not identified in later Planning Assessments, the risk of load-responsive protective relays tripping in response to a stable power swing during non-Fault conditions would have already been assessed under Requirement R2 and mitigated according to Requirements R3 and R4 where the relays did not meet the PRC-026-1 – Attachment B criteria. According to Requirement R2, the Generator Owner and Transmission Owner are only required to re-evaluate each load-responsive protective relay for an identified Element where the evaluation has not been performed in the last five calendar years.

Although Requirement R1 requires the Planning Coordinator to notify the respective Generator Owner and Transmission Owner of any Elements meeting one or more of the four criteria, it does not preclude the Planning Coordinator from providing additional information, such as apparent impedance characteristics, in advance or upon request, that may be useful in evaluating protective relays. Generator Owners and Transmission Owners are able to complete protective relay evaluations and perform the required actions without additional information. The standard does not include any requirement for the entities to provide information that is already being shared or exchanged between entities for operating needs. While a Requirement has not been included for the exchange of information, entities should recognize that relay performance needs to be measured against the most current information.

Requirement R2

Requirement R2 requires the Generator Owner and Transmission Owner to evaluate its load-responsive protective relays to ensure that they are expected to not trip in response to stable power swings.

The PRC-026-1 – Attachment A lists the applicable load-responsive relays that must be evaluated which include phase distance, phase overcurrent, out-of-step tripping, and loss-of-field relay functions. Phase distance relays could include, but are not limited to, the following:

- Zone elements with instantaneous tripping or intentional time delays of less than 15 cycles
- Phase distance elements used in high-speed communication-aided tripping schemes including:
  - Directional Comparison Blocking (DCB) schemes
  - Directional Comparison Un-Blocking (DCUB) schemes
  - Permissive Overreach Transfer Trip (POTT) schemes
  - Permissive Underreach Transfer Trip (PUTT) schemes

A method is provided within the standard to support consistent evaluation by Generator Owners and Transmission Owners based on specified conditions. Once a Generator Owner or Transmission Owner is notified of Elements pursuant to Requirement R1, it has 12 full calendar months to determine if each Element's load-responsive protective relays meet the PRC-026-1 – Attachment B criteria, if the determination has not been performed in the last five calendar years. Additionally, each Generator Owner and Transmission Owner, that becomes aware of a generator, transformer, or transmission line BES Element that tripped in response to a stable or unstable power swing due to the operation of its protective relays pursuant to Requirement R2, Part 2.2, must perform the same PRC-026-1 – Attachment B criteria determination within 12 full calendar months.

Becoming Aware of an Element That Tripped in Response to a Power Swing

Part 2.2 in Requirement R2 is intended to initiate action by the Generator Owner and Transmission Owner when there is a known stable or unstable power swing and it resulted in the entity's Element tripping. The criterion starts with becoming aware of the event (i.e., power swing) and then any connection with the entity's Element tripping. By doing so, the focus is removed from the entity having to demonstrate that it made a determination whether a power swing was present for every Element trip. The basis for structuring the criterion in this manner is driven by the available ways that a Generator Owner and Transmission Owner could become aware of an Element that tripped in response to a stable or unstable power swing due to the operation of its protective relay(s).

Element trips caused by stable or unstable power swings, though infrequent, would be more common in a larger event. The identification of power swings will be revealed during an analysis of the event. Event analysis where an entity may become aware of a stable or unstable power swing could include internal analysis conducted by the entity, the entity's Protection System review following a trip, or a larger scale analysis by other entities. Event analysis could include involvement by the entity's Regional Entity, and in some cases NERC.

Information Common to Both Generation and Transmission Elements

The PRC-026-1 – Attachment A lists the load-responsive protective relays that are subject to this standard. Generator Owners and Transmission Owners may own load-responsive protective relays (e.g., distance relays) that directly affect generation or transmission BES Elements and will require analysis as a result of Elements being identified by the Planning Coordinator in Requirement R1

or the Generator Owner or Transmission Owner in Requirement R2. For example, distance relays owned by the Transmission Owner may be installed at the high-voltage side of the generator step-up (GSU) transformer (directional toward the generator) providing backup to generation protection. Generator Owners may have distance relays applied to backup transmission protection or backup protection to the GSU transformer. The Generator Owner may have relays installed at the generator terminals or the high-voltage side of the GSU transformer.

Exclusion of Time Based Load-Responsive Protective Relays

The purpose of the standard is "[t]o ensure that load-responsive protective relays are expected to not trip in response to stable power swings during non-Fault conditions." Load-responsive, high-speed tripping protective relays pose the highest risk of operating during a power swing. Because of this, high-speed tripping protective relays and relays with a time delay of less than 15 cycles are included in the standard; whereas other relays (i.e., Zones 2 and 3) with a time delay of 15 cycles or greater are excluded. The time delay used for exclusion on some load-responsive protective relays is based on the maximum expected time that load-responsive protective relays would be exposed to a stable power swing with a slow slip rate frequency.

In order to establish a time delay that distinguishes a high-risk load-responsive protective relay from one that has a time delay for tripping (lower-risk), a sample of swing rates were calculated based on a stable power swing entering and leaving the impedance characteristic as shown in Table 1. For a relay impedance characteristic that has a power swing entering and leaving, beginning at 90 degrees with a termination at 120 degrees before exiting the zone, the zone timer must be greater than the calculated time the stable power swing is inside the relay's operating zone to not trip in response to the stable power swing.

Eq. (1)
$$Zone\ timer > 2 \times \left(\frac{(120° - Angle\ of\ entry\ into\ the\ relay\ characteristic) \times 60}{(360 \times Slip\ Rate)}\right)$$

Table 1: Swing Rates

Zone Timer (Cycles)	Slip Rate (Hz)
10	1.00
15	0.67
20	0.50
30	0.33

With a minimum zone timer of 15 cycles, the corresponding slip rate of the system is 0.67 Hz. This represents an approximation of a slow slip rate during a system Disturbance. Longer time delays allow for slower slip rates.

Application to Transmission Elements

Criterion A in PRC-026-1 – Attachment B describes an unstable power swing region that is formed by the union of three shapes in the impedance (R-X) plane. The first shape is a lower loss-of-synchronism circle based on a ratio of the sending-end to receiving-end voltages of 0.7 (i.e., E_S / E_R = 0.7 / 1.0 = 0.7). The second shape is an upper loss-of-synchronism circle based on a ratio of the sending-end to receiving-end voltages of 1.43 (i.e., E_S / E_R = 1.0 / 0.7 = 1.43). The third shape is a lens that connects the endpoints of the total system impedance together by varying the sending-end and receiving-end system voltages from 0.0 to 1.0 per unit, while maintaining a constant system separation angle across the total system impedance (with the parallel transfer impedance removed—see Figures 1 through 5). The total system impedance is derived from a two-bus equivalent network and is determined by summing the sending-end source impedance, the line impedance (excluding the Thévenin equivalent transfer impedance), and the receiving-end source impedance as shown in Figures 6 and 7. Establishing the total system impedance provides a conservative condition that will maximize the security of the relay against various system conditions. The smallest total system impedance represents a condition where the size of the lens characteristic in the R-X plane is smallest and is a conservative operating point from the standpoint of ensuring a load-responsive protective relay is expected to not trip given a predetermined angular displacement between the sending-end and receiving-end voltages. The smallest total system impedance results when all generation is in service and all transmission BES Elements are modeled in their "normal" system configuration (PRC-026-1 – Attachment B, Criterion A). The parallel transfer impedance is removed to represent a likely condition where parallel Elements may be lost during the disturbance, and the loss of these Elements magnifies the sensitivity of the load-responsive relays on the parallel line by removing the "infeed effect" (i.e., the apparent impedance sensed by the relay is decreased as a result of the loss of the transfer impedance, thus making the relay more likely to trip for a stable power swing—See Figures 13 and 14).

The sending-end and receiving-end source voltages are varied from 0.7 to 1.0 per unit to form the lower and upper loss-of-synchronism circles. The ratio of these two voltages is used in the calculation of the loss-of-synchronism circles, and result in a ratio range from 0.7 to 1.43.

Eq. (2) $$\frac{E_S}{E_R} = \frac{0.7}{1.0} = 0.7$$

Eq. (3): $$\frac{E_S}{E_R} = \frac{1.0}{0.7} = 1.43$$

The internal generator voltage during severe power swings or transmission system fault conditions will be greater than zero due to voltage regulator support. The voltage ratio of 0.7 to 1.43 is chosen to be more conservative than the PRC-023[13] and PRC-025[14] NERC Reliability Standards where a lower bound voltage of 0.85 per unit voltage is used. A ±15% internal generator voltage range was chosen as a conservative voltage range for calculation of the voltage ratio used to calculate the loss-of-synchronism circles. For example, the voltage ratio using these voltages would result in a ratio range from 0.739 to 1.353.

[13] Transmission Relay Loadability

[14] Generator Relay Loadability

Eq. (4) $$\frac{E_S}{E_R} = \frac{0.85}{1.15} = 0.739$$ Eq. (5): $$\frac{E_S}{E_R} = \frac{1.15}{0.85} = 1.353$$

The lower ratio is rounded down to 0.7 to be more conservative, allowing a voltage range of 0.7 to 1.0 per unit to be used for the calculation of the loss-of-synchronism circles.[15]

When the parallel transfer impedance is included in the model, the division of current through the parallel transfer impedance path results in actual measured relay impedances that are larger than those measured when the parallel transfer impedance is removed (i.e., infeed effect), which would make it more likely for an impedance relay element to be completely contained within the unstable power swing region as shown in Figure 11. If the transfer impedance is included in the evaluation, a distance relay element could be deemed as meeting PRC-026-1 – Attachment B criteria and, in fact would be secure, assuming all Elements were in their normal state. In this case, the distance relay element could trip in response to a stable power swing during an actual event if the system was weakened (i.e., a higher transfer impedance) by the loss of a subset of lines that make up the parallel transfer impedance as shown in Figure 10. This could happen because the subset of lines that make up the parallel transfer impedance tripped on unstable swings, contained the initiating fault, and/or were lost due to operation of breaker failure or remote back-up protection schemes.

Table 10 shows the percent size increase of the lens shape as seen by the relay under evaluation when the parallel transfer impedance is included. The parallel transfer impedance has minimal effect on the apparent size of the lens shape as long as the parallel transfer impedance is at least 10 multiples of the parallel line impedance (less than 5% lens shape expansion), therefore, its removal has minimal impact, but results in a slightly more conservative, smaller lens shape. Parallel transfer impedances of 5 multiples of the parallel line impedance or less result in an apparent lens shape size of 10% or greater as seen by the relay. If two parallel lines and a parallel transfer impedance tie the sending-end and receiving-end buses together, the total parallel transfer impedance will be one or less multiples of the parallel line impedance, resulting in an apparent lens shape size of 45% or greater. It is a realistic contingency that the parallel line could be out-of-service, leaving the parallel transfer impedance making up the rest of the system in parallel with the line impedance. Since it is not known exactly which lines making up the parallel transfer impedance will be out of service during a major system disturbance, it is most conservative to assume that all of them are out, leaving just the line under evaluation in service.

Either the saturated transient or sub-transient direct axis reactance may be used for machines in the evaluation because they are smaller than the un-saturated reactances. Since saturated sub-transient generator reactances are smaller than the transient or synchronous reactances, the use of sub-transient reactances will result in a smaller source impedance and a smaller unstable power swing region in the graphical analysis as shown in Figures 8 and 9. Because power swings occur in a time frame where generator transient reactances will be prevalent, it is acceptable to use saturated transient reactances instead of saturated sub-transient reactances. Because some short-

[15] *Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations*, April 2004, Section 6 (The Cascade Stage of the Blackout), p. 94 under "Why the Generators Tripped Off," states, "Some generator undervoltage relays were set to trip at or above 90% voltage. However, a motor stalls out at about 70% voltage and a motor starter contactor drops out around 75%, so if there is a compelling need to protect the turbine from the system the under-voltage trigger point should be no higher than 80%."

circuit models may not include transient reactances, the use of sub-transient reactances is also acceptable because it produces more conservative results. For this reason, either value is acceptable when determining the system source impedances (PRC-026-1 – Attachment B, Criterion A and B, No. 3).

Saturated reactances are used in short-circuit programs that produce the system impedance mentioned above. Planning and stability software generally use un-saturated reactances. Generator models used in transient stability analyses recognize that the extent of the saturation effect depends upon both rotor (field) and stator currents. Accordingly, they derive the effective saturated parameters of the machine at each instant by internal calculation from the specified (constant) unsaturated values of machine reactances and the instantaneous internal flux level. The specific assumptions regarding which inductances are affected by saturation, and the relative effect of that saturation, are different for the various generator models used. Thus, unsaturated values of all machine reactances are used in setting up planning and stability software data, and the appropriate set of open-circuit magnetization curve data is provided for each machine.

Saturated reactance values are smaller than unsaturated reactance values and are used in short-circuit programs owned by the Generator and Transmission Owners. Because of this, saturated reactance values are to be used in the development of the system source impedances.

The source or system equivalent impedances can be obtained by a number of different methods using commercially available short-circuit calculation tools.[16] Most short-circuit tools have a network reduction feature that allows the user to select the local and remote terminal buses to retain. The first method reduces the system to one that contains two buses, an equivalent generator at each bus (representing the source impedances at the sending-end and receiving-end), and two parallel lines; one being the line impedance of the protected line with relays being analyzed, the other being the parallel transfer impedance representing all other combinations of lines that connect the two buses together as shown in Figure 6. Another conservative method is to open both ends of the line being evaluated, and apply a three-phase bolted fault at each bus to determine the Thévenin equivalent impedance at each bus. The source impedances are set equal to the Thévenin equivalent impedances and will be less than or equal to the actual source impedances calculated by the network reduction method. Either method can be used to develop the system source impedances at both ends.

The two bullets of PRC-026-1 – Attachment B, Criterion A, No. 1, identify the system separation angles used to identify the size of the power swing stability boundary for evaluating load-responsive protective relay impedance elements. The first bullet of PRC-026-1 – Attachment B, Criterion A, No. 1 evaluates a system separation angle of at least 120 degrees that is held constant while varying the sending-end and receiving-end source voltages from 0.7 to 1.0 per unit, thus creating an unstable power swing region about the total system impedance in Figure 1. This unstable power swing region is compared to the tripping portion of the distance relay characteristic; that is, the portion that is not supervised by load encroachment, blinders, or some other form of supervision as shown in Figure 12 that restricts the distance element from tripping

[16] Demetrios A. Tziouvaras and Daqing Hou, Appendix in *Out-Of-Step Protection Fundamentals and Advancements,* April 17, 2014: https://www.selinc.com.

for heavy, balanced load conditions. If the tripping portion of the impedance characteristics are completely contained within the unstable power swing region, the relay impedance element meets Criterion A in PRC-026-1 – Attachment B. A system separation angle of 120 degrees was chosen for the evaluation because it is generally accepted in the industry that recovery for a swing beyond this angle is unlikely to occur.[17]

The second bullet of PRC-026-1 – Attachment B, Criterion A, No. 1 evaluates impedance relay elements at a system separation angle of less than 120 degrees, similar to the first bullet described above. An angle less than 120 degrees may be used if a documented stability analysis demonstrates that the power swing becomes unstable at a system separation angle of less than 120 degrees.

The exclusion of relay elements supervised by Power Swing Blocking (PSB) in PRC-026-1 – Attachment A allows the Generator Owner or Transmission Owner to exclude protective relay elements if they are blocked from tripping by PSB relays. A PSB relay applied and set according to industry accepted practices prevent supervised load-responsive protective relays from tripping in response to power swings. Further, PSB relays are set to allow dependable tripping of supervised elements. The criteria in PRC-026-1 – Attachment B specifically applies to unsupervised elements that could trip for stable power swings. Therefore, load-responsive protective relay elements supervised by PSB can be excluded from the Requirements of this standard.

[17] "The critical angle for maintaining stability will vary depending on the contingency and the system condition at the time the contingency occurs; however, the likelihood of recovering from a swing that exceeds 120 degrees is marginal and 120 degrees is generally accepted as an appropriate basis for setting out-of-step protection. Given the importance of separating unstable systems, defining 120 degrees as the critical angle is appropriate to achieve a proper balance between dependable tripping for unstable power swings and secure operation for stable power swings." NERC System Protection and Control Subcommittee, *Protection System Response to Power Swings*, August 2013: http://www.nerc.com/comm/PC/System%20Protection%20and%20Control%20Subcommittee%20SPCS%2020/SPCS%20Power%20Swing%20Report_Final_20131015.pdf), p. 28.

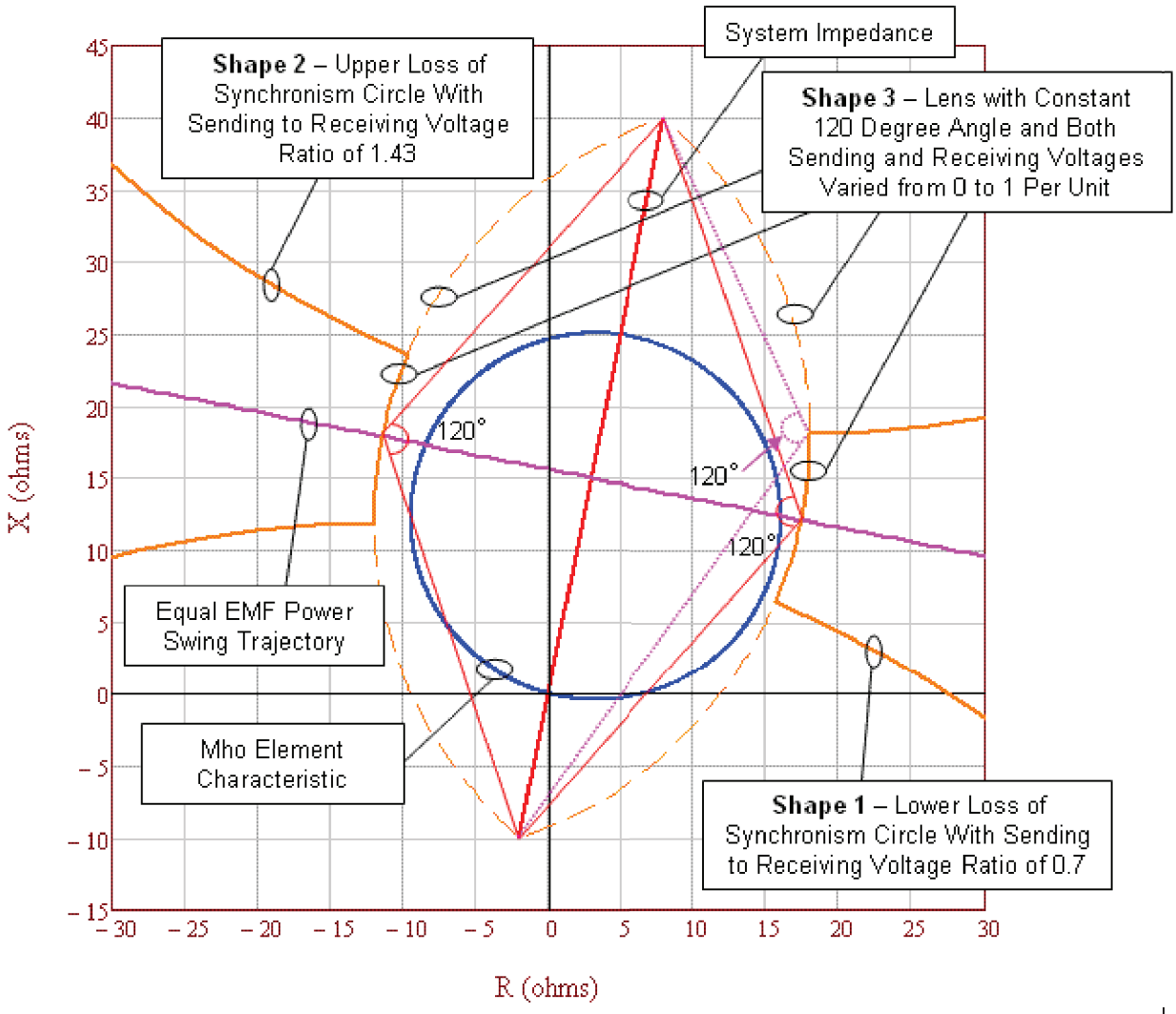


Figure 1: An enlarged graphic illustrating the unstable power swing region formed by the union of three shapes in the impedance (R-X) plane: Shape 1) Lower loss-of-synchronism circle, Shape 2) Upper loss-of-synchronism circle, and Shape 3) Lens. The mho element characteristic is completely contained within the unstable power swing region (i.e., it does not intersect any portion of the unstable power swing region), therefore it meets PRC-026-1 – Attachment B, Criterion A, No. 1.

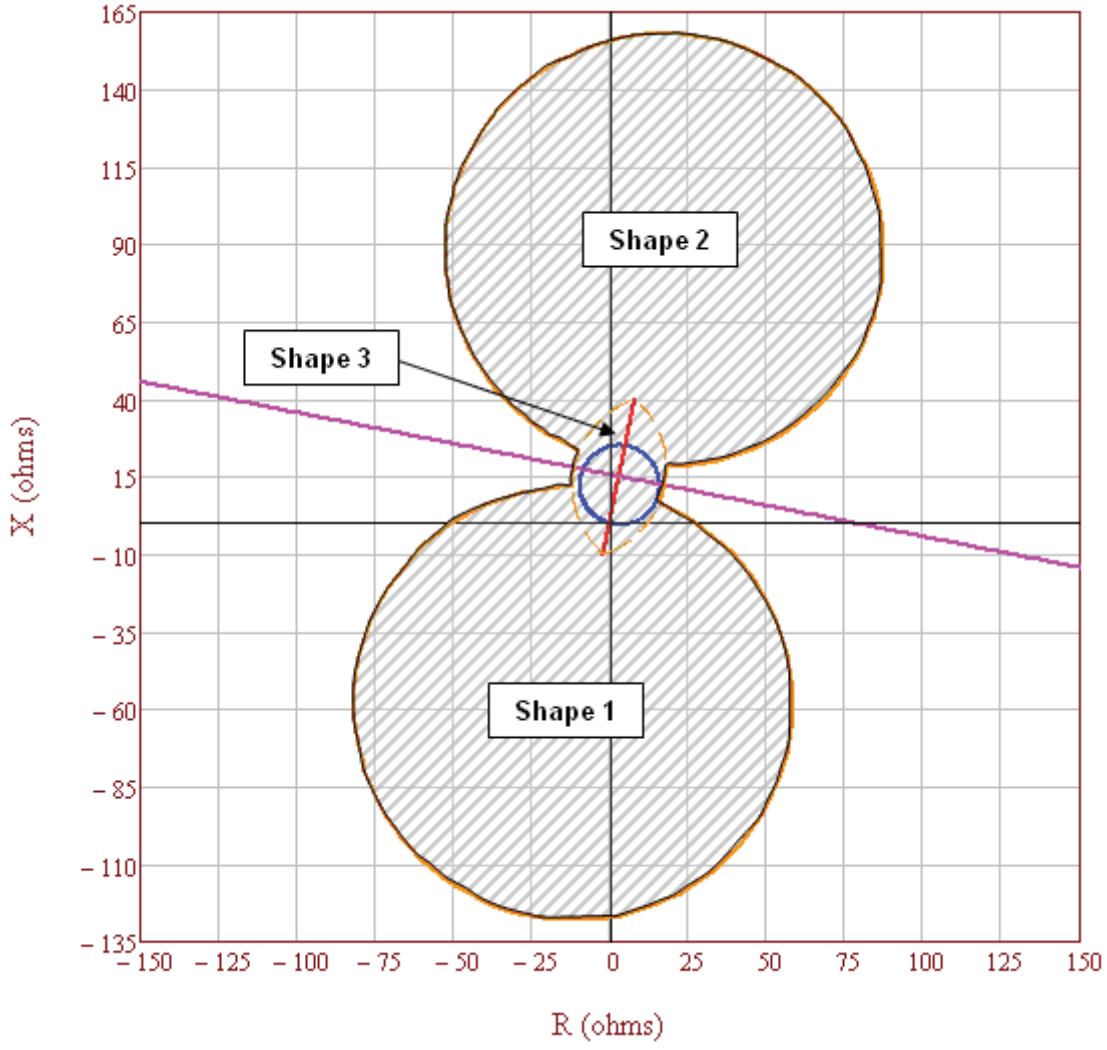


Figure 2: Full graphic of the unstable power swing region formed by the union of the three shapes in the impedance (R-X) plane: Shape 1) Lower loss-of-synchronism circle, Shape 2) Upper loss-of-synchronism circle, and Shape 3) Lens. The mho element characteristic is completely contained within the unstable power swing region, therefore it meets PRC-26-1 – Attachment B, Criterion A, No.1.

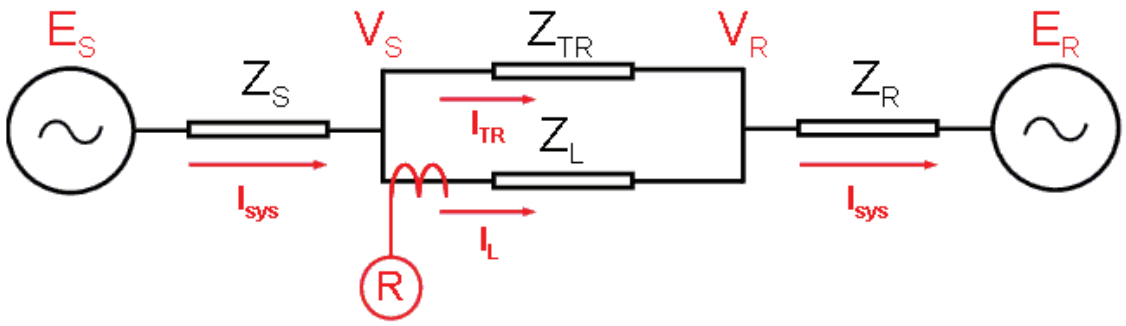


Figure 3: System impedances as seen by Relay R (voltage connections are not shown).

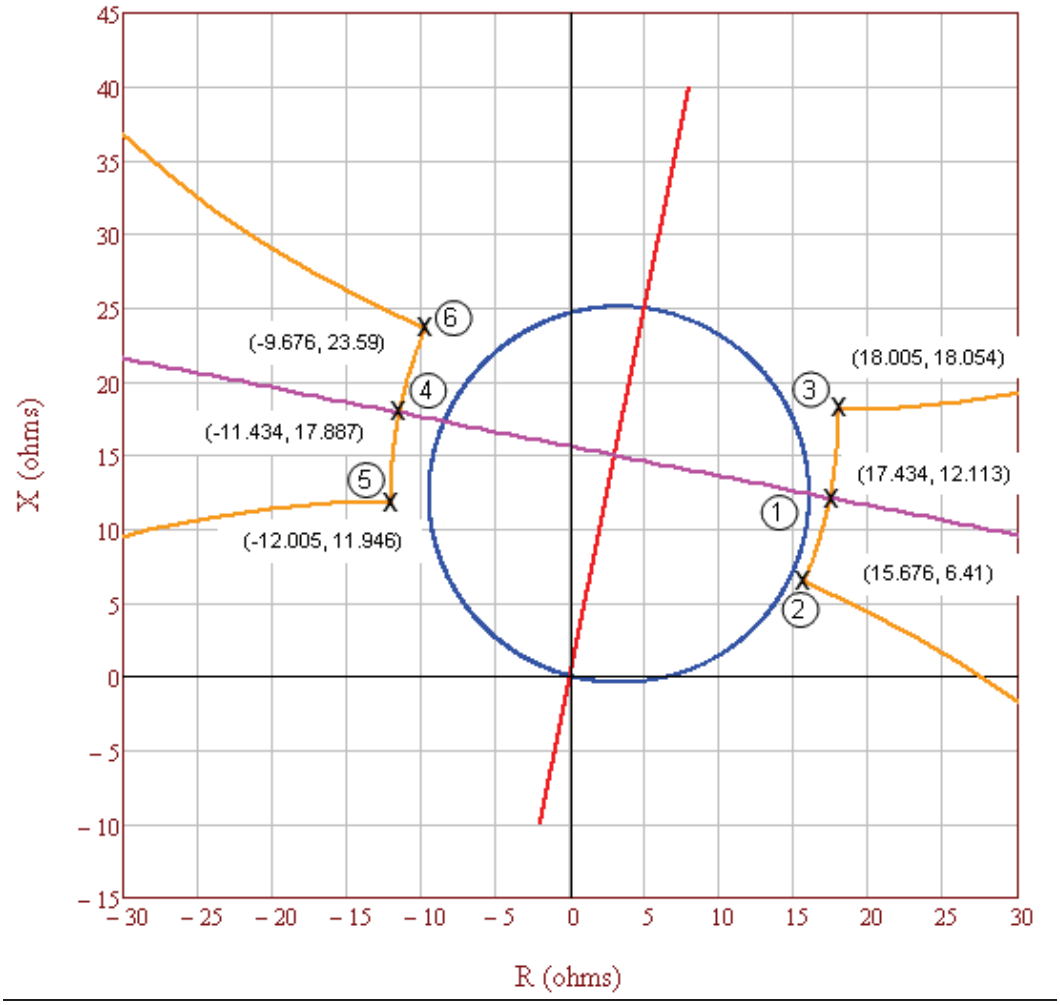


Figure 4: The defining unstable power swing region points where the lens shape intersects the lower and upper loss-of-synchronism circle shapes and where the lens intersects the equal EMF (electromotive force) power swing.

	Left Side Coordinates		Right Side Coordinates	
E_S / E_R Voltage Ratio	R	+ jX	R	+ jX
0.7	**-12.005**	**11.946**	**15.676**	**6.41**
0.72	-12.004	12.407	15.852	6.836
0.74	-11.996	12.857	16.018	7.255
0.76	-11.982	13.298	16.175	7.667
0.78	-11.961	13.729	16.321	8.073
0.8	-11.935	14.151	16.459	8.472
0.82	-11.903	14.563	16.589	8.865
0.84	-11.867	14.966	16.71	9.251
0.86	-11.826	15.361	16.824	9.631
0.88	-11.78	15.746	16.93	10.004
0.9	-11.731	16.123	17.03	10.371
0.92	-11.678	16.492	17.123	10.732
0.94	-11.621	16.852	17.209	11.086
0.96	-11.562	17.205	17.29	11.435
0.98	-11.499	17.55	17.364	11.777
1	**-11.434**	**17.887**	**17.434**	**12.113**
1.0286	-11.336	18.356	17.524	12.584
1.0572	-11.234	18.81	17.604	13.043
1.0858	-11.127	19.251	17.675	13.49
1.1144	-11.017	19.677	17.738	13.926
1.143	-10.904	20.091	17.792	14.351
1.1716	-10.788	20.491	17.84	14.766
1.2002	-10.67	20.88	17.88	15.17
1.2288	-10.55	21.256	17.914	15.564
1.2574	-10.428	21.621	17.942	15.948
1.286	-10.304	21.975	17.964	16.322
1.3146	-10.18	22.319	17.981	16.687
1.3432	-10.054	22.652	17.993	17.043
1.3718	-9.928	22.976	18.001	17.39
1.4004	-9.801	23.29	18.005	17.728
1.429	**-9.676**	**23.59**	**18.005**	**18.054**

Figure 5: Full table of 31 detailed lens shape point calculations. The bold highlighted rows correspond to the detailed calculations in Tables 2-7.

Table 2: Example Calculation (Lens Point 1)	
This example is for calculating the impedance the first point of the lens characteristic. Equal source voltages are used for the 230 kV (base) line with the sending-end voltage (E_S) leading the receiving-end voltage (E_R) by 120 degrees. See Figures 3 and 4.	
Eq. (6)	$E_S = \frac{V_{LL}\angle 120°}{\sqrt{3}}$

Table 2: Example Calculation (Lens Point 1)			
	$E_S = \frac{230{,}000\angle 120°\ V}{\sqrt{3}}$		
	$E_S = 132{,}791\angle 120°\ V$		
Eq. (7)	$E_R = \frac{V_{LL}\angle 0°}{\sqrt{3}}$		
	$E_R = \frac{230{,}000\angle 0°\ V}{\sqrt{3}}$		
	$E_R = 132{,}791\angle 0°\ V$		
Positive sequence impedance data (with transfer impedance Z_{TR} set to a large value).			
Given:	$Z_S = 2 + j10\ \Omega$	$Z_L = 4 + j20\ \Omega$	$Z_R = 4 + j20\ \Omega$
Given:	$Z_{TR} = Z_L \times 10^{10}\ \Omega$		
Total impedance between the generators.			
Eq. (8)	$Z_{total} = \frac{(Z_L \times Z_{TR})}{(Z_L + Z_{TR})}$		
	$Z_{total} = \frac{\left((4 + j20)\ \Omega \times (4 + j20) \times 10^{10}\ \Omega\right)}{\left((4 + j20)\ \Omega + (4 + j20) \times 10^{10}\ \Omega\right)}$		
	$Z_{total} = 4 + j20\ \Omega$		
Total system impedance.			
Eq. (9)	$Z_{sys} = Z_S + Z_{total} + Z_R$		
	$Z_{sys} = (2 + j10)\ \Omega + (4 + j20)\ \Omega + (4 + j20)\ \Omega$		
	$Z_{sys} = 10 + j50\ \Omega$		
Total system current from sending-end source.			
Eq. (10)	$I_{sys} = \frac{E_S - E_R}{Z_{sys}}$		
	$I_{sys} = \frac{132{,}791\angle 120°\ V - 132{,}791\angle 0°\ V}{(10 + j50\ )\Omega}$		
	$I_{sys} = 4{,}511\angle 71.3°\ A$		
The current, as measured by the relay on Z_L (Figure 3), is only the current flowing through that line as determined by using the current divider equation.			
Eq. (11)	$I_L = I_{sys} \times \frac{Z_{TR}}{Z_L + Z_{TR}}$		

Table 2: Example Calculation (Lens Point 1)	
	$I_L = 4{,}511\angle 71.3° \; A \times \frac{(4 + j20) \times 10^{10} \; \Omega}{(4 + j20) \; \Omega + (4 + j20) \times 10^{10} \; \Omega}$
	$I_L = 4{,}511\angle 71.3° \; A$
The voltage, as measured by the relay on Z_L (Figure 3), is the voltage drop from the sending-end source through the sending-end source impedance.	
Eq. (12)	$V_S = E_S - (Z_S \times I_{sys})$
	$V_S = 132{,}791\angle 120° \; V - [(2 + j10) \; \Omega \times 4{,}511\angle 71.3° \; A]$
	$V_S = 95{,}757\angle 106.1° \; V$
The impedance seen by the relay on Z_L.	
Eq. (13)	$Z_{L-Relay} = \frac{V_S}{I_L}$
	$Z_{L-Relay} = \frac{95{,}757\angle 106.1° \; V}{4{,}511\angle 71.3° \; A}$
	$Z_{L-Relay} = 17.434 + j12.113 \; \Omega$

Table 3: Example Calculation (Lens Point 2)			
This example is for calculating the impedance second point of the lens characteristic. Unequal source voltages are used for the 230 kV (base) line with the sending-end voltage (E_S) at 70% of the receiving-end voltage (E_R) and leading the receiving-end voltage by 120 degrees. See Figures 3 and 4.			
Eq. (14)	$E_S = \frac{V_{LL}\angle 120°}{\sqrt{3}} \times 70\%$		
	$E_S = \frac{230{,}000\angle 120° \; V}{\sqrt{3}} \times 0.70$		
	$E_S = 92{,}953.7\angle 120° \; V$		
Eq. (15)	$E_R = \frac{V_{LL}\angle 0°}{\sqrt{3}}$		
	$E_R = \frac{230{,}000\angle 0° \; V}{\sqrt{3}}$		
	$E_R = 132{,}791\angle 0° \; V$		
Positive sequence impedance data (with transfer impedance Z_{TR} set to a large value).			
Given:	$Z_S = 2 + j10 \; \Omega$	$Z_L = 4 + j20 \; \Omega$	$Z_R = 4 + j20 \; \Omega$
Given:	$Z_{TR} = Z_L \times 10^{10} \; \Omega$		

Table 3: Example Calculation (Lens Point 2)	
Total impedance between the generators.	
Eq. (16)	$Z_{total} = \frac{(Z_L \times Z_{TR})}{(Z_L + Z_{TR})}$
	$Z_{total} = \frac{\left((4 + j20)\ \Omega \times (4 + j20) \times 10^{10}\ \Omega\right)}{\left((4 + j20)\ \Omega + (4 + j20) \times 10^{10}\ \Omega\right)}$
	$Z_{total} = 4 + j20\ \Omega$
Total system impedance.	
Eq. (17)	$Z_{sys} = Z_S + Z_{total} + Z_R$
	$Z_{sys} = (2 + j10)\ \Omega + (4 + j20)\ \Omega + (4 + j20)\ \Omega$
	$Z_{sys} = 10 + j50\ \Omega$
Total system current from sending-end source.	
Eq. (18)	$I_{sys} = \frac{E_S - E_R}{Z_{sys}}$
	$I_{sys} = \frac{92{,}953.7\angle 120°\ V - 132{,}791\angle 0°\ V}{(10 + j50)\ \Omega}$
	$I_{sys} = 3{,}854\angle 77°\ A$
The current, as measured by the relay on Z_L (Figure 3), is only the current flowing through that line as determined by using the current divider equation.	
Eq. (19)	$I_L = I_{sys} \times \frac{Z_{TR}}{Z_L + Z_{TR}}$
	$I_L = 3{,}854\angle 77°\ A \times \frac{(4 + j20) \times 10^{10}\ \Omega}{(4 + j20)\ \Omega + (4 + j20) \times 10^{10}\ \Omega}$
	$I_L = 3{,}854\angle 77°\ A$
The voltage, as measured by the relay on Z_L (Figure 3), is the voltage drop from the sending-end source through the sending-end source impedance.	
Eq. (20)	$V_S = E_S - \left(Z_S \times I_{sys}\right)$
	$V_S = 92{,}953\angle 120°\ V - [(2 + j10\ )\Omega \times 3{,}854\angle 77°\ A]$
	$V_S = 65{,}271\angle 99°\ V$
The impedance seen by the relay on Z_L.	
Eq. (21)	$Z_{L-Relay} = \frac{V_S}{I_L}$

Table 3: Example Calculation (Lens Point 2)	
	$Z_{L-Relay} = \frac{65{,}271\angle 99°\ V}{3{,}854\angle 77°\ A}$
	$Z_{L-Relay} = 15.676 + j6.41\ \Omega$

Table 4: Example Calculation (Lens Point 3)			
This example is for calculating the impedance third point of the lens characteristic. Unequal source voltages are used for the 230 kV (base) line with the receiving-end voltage (E_R) at 70% of the sending-end voltage (E_S) and the sending-end voltage leading the receiving-end voltage by 120 degrees. See Figures 3 and 4.			
Eq. (22)	$E_S = \frac{V_{LL}\angle 120°}{\sqrt{3}}$		
	$E_S = \frac{230{,}000\angle 120°\ V}{\sqrt{3}}$		
	$E_S = 132{,}791\angle 120°\ V$		
Eq. (23)	$E_R = \frac{V_{LL}\angle 0°}{\sqrt{3}} \times 70\%$		
	$E_R = \frac{230{,}000\angle 0°\ V}{\sqrt{3}} \times 0.70$		
	$E_R = 92{,}953.7\angle 0°\ V$		
Positive sequence impedance data (with transfer impedance Z_{TR} set to a large value).			
Given:	$Z_S = 2 + j10\ \Omega$	$Z_L = 4 + j20\ \Omega$	$Z_R = 4 + j20\ \Omega$
Given:	$Z_{TR} = Z_L \times 10^{10}\ \Omega$		
Total impedance between the generators.			
Eq. (24)	$Z_{total} = \frac{(Z_L \times Z_{TR})}{(Z_L + Z_{TR})}$		
	$Z_{total} = \frac{\left((4 + j20)\ \Omega \times (4 + j20) \times 10^{10}\ \Omega\right)}{\left((4 + j20)\ \Omega + (4 + j20) \times 10^{10}\ \Omega\right)}$		
	$Z_{total} = 4 + j20\ \Omega$		
Total system impedance.			
Eq. (25)	$Z_{sys} = Z_S + Z_{total} + Z_R$		
	$Z_{sys} = (2 + j10)\ \Omega + (4 + j20)\ \Omega + (4 + j20)\ \Omega$		
	$Z_{sys} = 10 + j50\ \Omega$		

Table 4: Example Calculation (Lens Point 3)	
Total system current from sending-end source.	
Eq. (26)	$I_{sys} = \frac{E_S - E_R}{Z_{sys}}$
	$I_{sys} = \frac{132{,}791\angle 120°\ V - 92{,}953.7\angle 0°\ V}{(10 + j50)\ \Omega}$
	$I_{sys} = 3{,}854\angle 65.5°\ A$
The current, as measured by the relay on Z_L (Figure 3), is only the current flowing through that line as determined by using the current divider equation.	
Eq. (27)	$I_L = I_{sys} \times \frac{Z_{TR}}{Z_L + Z_{TR}}$
	$I_L = 3{,}854\angle 65.5°\ A \times \frac{(4 + j20) \times 10^{10}\ \Omega}{(4 + j20)\ \Omega + (4 + j20) \times 10^{10}\ \Omega}$
	$I_L = 3{,}854\angle 65.5°\ A$
The voltage, as measured by the relay on Z_L (Figure 3), is the voltage drop from the sending-end source through the sending-end source impedance.	
Eq. (28)	$V_S = E_S - (Z_S \times I_L)$
	$V_S = 132{,}791\angle 120°\ V - [(2 + j10)\ \Omega \times 3{,}854\angle 65.5°\ A]$
	$V_S = 98{,}265\angle 110.6°\ V$
The impedance seen by the relay on Z_L.	
Eq. (29)	$Z_{L-Relay} = \frac{V_S}{I_L}$
	$Z_{L-Relay} = \frac{98{,}265\angle 110.6°\ V}{3{,}854\angle 65.5°\ A}$
	$Z_{L-Relay} = 18.005 + j18.054\ \Omega$

Table 5: Example Calculation (Lens Point 4)	
This example is for calculating the impedance fourth point of the lens characteristic. Equal source voltages are used for the 230 kV (base) line with the sending-end voltage (E_S) leading the receiving-end voltage (E_R) by 240 degrees. See Figures 3 and 4.	
Eq. (30)	$E_S = \frac{V_{LL}\angle 240°}{\sqrt{3}}$
	$E_S = \frac{230{,}000\angle 240°\ V}{\sqrt{3}}$

Table 5: Example Calculation (Lens Point 4)			
	$E_S = 132{,}791\angle 240°\ V$		
Eq. (31)	$E_R = \frac{V_{LL}\angle 0°}{\sqrt{3}}$		
	$E_R = \frac{230{,}000\angle 0°\ V}{\sqrt{3}}$		
	$E_R = 132{,}791\angle 0°\ V$		
Positive sequence impedance data (with transfer impedance Z_{TR} set to a large value).			
Given:	$Z_S = 2 + j10\ \Omega$	$Z_L = 4 + j20\ \Omega$	$Z_R = 4 + j20\ \Omega$
Given:	$Z_{TR} = Z_L \times 10^{10}\ \Omega$		
Total impedance between the generators.			
Eq. (32)	$Z_{total} = \frac{(Z_L \times Z_{TR})}{(Z_L + Z_{TR})}$		
	$Z_{total} = \frac{\left((4 + j20)\ \Omega \times (4 + j20) \times 10^{10}\ \Omega\right)}{\left((4 + j20)\ \Omega + (4 + j20) \times 10^{10}\ \Omega\right)}$		
	$Z_{total} = 4 + j20\ \Omega$		
Total system impedance.			
Eq. (33)	$Z_{sys} = Z_S + Z_{total} + Z_R$		
	$Z_{sys} = (2 + j10)\ \Omega + (4 + j20)\ \Omega + (4 + j20)\ \Omega$		
	$Z_{sys} = 10 + j50\ \Omega$		
Total system current from sending-end source.			
Eq. (34)	$I_{sys} = \frac{E_S - E_R}{Z_{sys}}$		
	$I_{sys} = \frac{132{,}791\angle 240°\ V - 132{,}791\angle 0°\ V}{(10 + j50\ )\Omega}$		
	$I_{sys} = 4{,}511\angle 131.3°\ A$		
The current, as measured by the relay on Z_L (Figure 3), is only the current flowing through that line as determined by using the current divider equation.			
Eq. (35)	$I_L = I_{sys} \times \frac{Z_{TR}}{Z_L + Z_{TR}}$		
	$I_L = 4{,}511\angle 131.1°\ A \times \frac{(4 + j20) \times 10^{10}\ \Omega}{(4 + j20)\ \Omega + (4 + j20) \times 10^{10}\ \Omega}$		
	$I_L = 4{,}511\angle 131.1°\ A$		

Table 5: Example Calculation (Lens Point 4)			
The voltage, as measured by the relay on Z_L (Figure 3), is the voltage drop from the sending-end source through the sending-end source impedance.			
Eq. (36)	$V_S = E_S - (Z_S \times I_L)$		
	$V_S = 132{,}791\angle 240° \, V - [(2 + j10\,)\,\Omega \times 4{,}511\angle 131.1° \, A]$		
	$V_S = 95{,}756\angle -106.1° \, V$		
The impedance seen by the relay on Z_L.			
Eq. (37)	$Z_{L-Relay} = \frac{V_S}{I_L}$		
	$Z_{L-Relay} = \frac{95{,}756\angle -106.1° \, V}{4{,}511\angle 131.1° \, A}$		
	$Z_{L-Relay} = -11.434 + j17.887\ \Omega$		

Table 6: Example Calculation (Lens Point 5)			
This example is for calculating the impedance fifth point of the lens characteristic. Unequal source voltages are used for the 230 kV (base) line with the sending-end voltage (E_S) at 70% of the receiving-end voltage (E_R) and leading the receiving-end voltage by 240 degrees. See Figures 3 and 4.			
Eq. (38)	$E_S = \frac{V_{LL}\angle 240°}{\sqrt{3}} \times 70\%$		
	$E_S = \frac{230{,}000\angle 240° \, V}{\sqrt{3}} \times 0.70$		
	$E_S = 92{,}953.7\angle 240° \, V$		
Eq. (39)	$E_R = \frac{V_{LL}\angle 0°}{\sqrt{3}}$		
	$E_R = \frac{230{,}000\angle 0° \, V}{\sqrt{3}}$		
	$E_R = 132{,}791\angle 0° \, V$		
Positive sequence impedance data (with transfer impedance Z_{TR} set to a large value).			
Given:	$Z_S = 2 + j10\ \Omega$	$Z_L = 4 + j20\ \Omega$	$Z_R = 4 + j20\ \Omega$
Given:	$Z_{TR} = Z_L \times 10^{10}\ \Omega$		
Total impedance between the generators.			
Eq. (40)	$Z_{total} = \frac{(Z_L \times Z_{TR})}{(Z_L + Z_{TR})}$		

Table 6: Example Calculation (Lens Point 5)	
	$Z_{total} = \frac{\left((4 + j20)\ \Omega \times (4 + j20) \times 10^{10}\ \Omega\right)}{\left((4 + j20)\ \Omega + (4 + j20) \times 10^{10}\ \Omega\right)}$
	$Z_{total} = 4 + j20\ \Omega$
Total system impedance.	
Eq. (41)	$Z_{sys} = Z_S + Z_{total} + Z_R$
	$Z_{sys} = (2 + j10\ \Omega) + (4 + j20\ \Omega) + (4 + j20\ \Omega)$
	$Z_{sys} = 10 + j50\ \Omega$
Total system current from sending-end source.	
Eq. (42)	$I_{sys} = \frac{E_S - E_R}{Z_{sys}}$
	$I_{sys} = \frac{92{,}953.7\angle 240°\ V - 132{,}791\angle 0°\ V}{10 + j50\ \Omega}$
	$I_{sys} = 3{,}854\angle 125.5°\ A$
The current, as measured by the relay on Z_L (Figure 3), is only the current flowing through that line as determined by using the current divider equation.	
Eq. (43)	$I_L = I_{sys} \times \frac{Z_{TR}}{Z_L + Z_{TR}}$
	$I_L = 3{,}854\angle 125.5°\ A \times \frac{(4 + j20) \times 10^{10}\ \Omega}{(4 + j20)\ \Omega + (4 + j20) \times 10^{10}\ \Omega}$
	$I_L = 3{,}854\angle 125.5°\ A$
The voltage, as measured by the relay on Z_L (Figure 3), is the voltage drop from the sending-end source through the sending-end source impedance.	
Eq. (44)	$V_S = E_S - (Z_S \times I_L)$
	$V_S = 92{,}953.7\angle 240°\ V - [(2 + j10\ )\ \Omega \times 3{,}854\angle 125.5°\ A]$
	$V_S = 65{,}270.5\angle -99.4°\ V$
The impedance seen by the relay on Z_L.	
Eq. (45)	$Z_{L-Relay} = \frac{V_S}{I_L}$
	$Z_{L-Relay} = \frac{65{,}270.5\angle -99.4°\ V}{3{,}854\angle 125.5°\ A}$
	$Z_{L-Relay} = -12.005 + j11.946\ \Omega$

Table 7: Example Calculation (Lens Point 6)			
This example is for calculating the impedance sixth point of the lens characteristic. Unequal source voltages are used for the 230 kV (base) line with the receiving-end voltage (E_R) at 70% of the sending-end voltage (E_S) and the sending-end voltage leading the receiving-end voltage by 240 degrees. See Figures 3 and 4.			
Eq. (46)	$E_S = \frac{V_{LL}\angle 240°}{\sqrt{3}}$		
	$E_S = \frac{230{,}000\angle 240°\ V}{\sqrt{3}}$		
	$E_S = 132{,}791\angle 240°\ V$		
Eq. (47)	$E_R = \frac{V_{LL}\angle 0°}{\sqrt{3}} \times 70\%$		
	$E_R = \frac{230{,}000\angle 0°\ V}{\sqrt{3}} \times 0.70$		
	$E_R = 92{,}953.7\angle 0°\ V$		
Positive sequence impedance data (with transfer impedance Z_{TR} set to a large value).			
Given:	$Z_S = 2 + j10\ \Omega$	$Z_L = 4 + j20\ \Omega$	$Z_R = 4 + j20\ \Omega$
Given:	$Z_{TR} = Z_L \times 10^{10}\ \Omega$		
Total impedance between the generators.			
Eq. (48)	$Z_{total} = \frac{(Z_L \times Z_{TR})}{(Z_L + Z_{TR})}$		
	$Z_{total} = \frac{\left((4 + j20)\ \Omega \times (4 + j20) \times 10^{10}\ \Omega\right)}{\left((4 + j20)\ \Omega + (4 + j20) \times 10^{10}\ \Omega\right)}$		
	$Z_{total} = 4 + j20\ \Omega$		
Total system impedance.			
Eq. (49)	$Z_{sys} = Z_S + Z_{total} + Z_R$		
	$Z_{sys} = (2 + j10)\ \Omega + (4 + j20)\ \Omega + (4 + j20)\ \Omega$		
	$Z_{sys} = 10 + j50\ \Omega$		
Total system current from sending-end source.			
Eq. (50)	$I_{sys} = \frac{E_S - E_R}{Z_{sys}}$		
	$I_{sys} = \frac{132{,}791\angle 240°\ V - 92{,}953.7\angle 0°\ V}{10 + j50\ \Omega}$		
	$I_{sys} = 3{,}854\angle 137.1°\ A$		

Table 7: Example Calculation (Lens Point 6)	
The current, as measured by the relay on Z_L (Figure 3), is only the current flowing through that line as determined by using the current divider equation.	
Eq. (51)	$I_L = I_{sys} \times \frac{Z_{TR}}{Z_L + Z_{TR}}$
	$I_L = 3{,}854\angle 137.1° \, A \times \frac{(4 + j20) \times 10^{10} \, \Omega}{(4 + j20) \, \Omega + (4 + j20) \times 10^{10} \, \Omega}$
	$I_L = 3{,}854\angle 137.1° \, A$
The voltage, as measured by the relay on Z_L (Figure 3), is the voltage drop from the sending-end source through the sending-end source impedance.	
Eq. (52)	$V_S = E_S - (Z_S \times I_L)$
	$V_S = 132{,}791\angle 240° \, V - [(2 + j10 \,) \, \Omega \times 3{,}854\angle 137.1° \, A]$
	$V_S = 98{,}265\angle -110.6° \, V$
The impedance seen by the relay on Z_L.	
Eq. (53)	$Z_{L-Relay} = \frac{V_S}{I_L}$
	$Z_{L-Relay} = \frac{98{,}265\angle -110.6° \, V}{3{,}854\angle 137.1° \, A}$
	$Z_{L-Relay} = -9.676 + j23.59 \, \Omega$

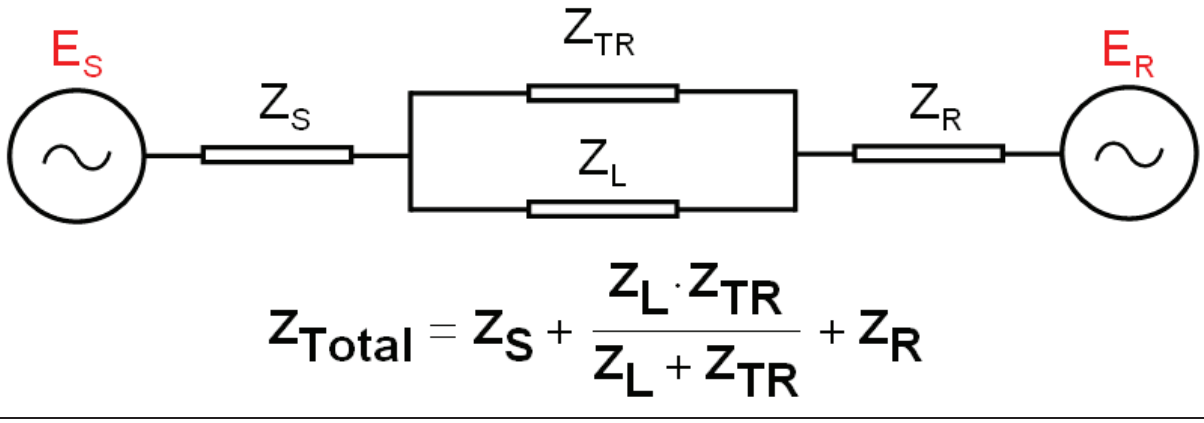


Figure 6: Reduced two bus system with sending-end source impedance Z_S, receiving-end source impedance Z_R, line impedance Z_L, and parallel transfer impedance Z_{TR}.

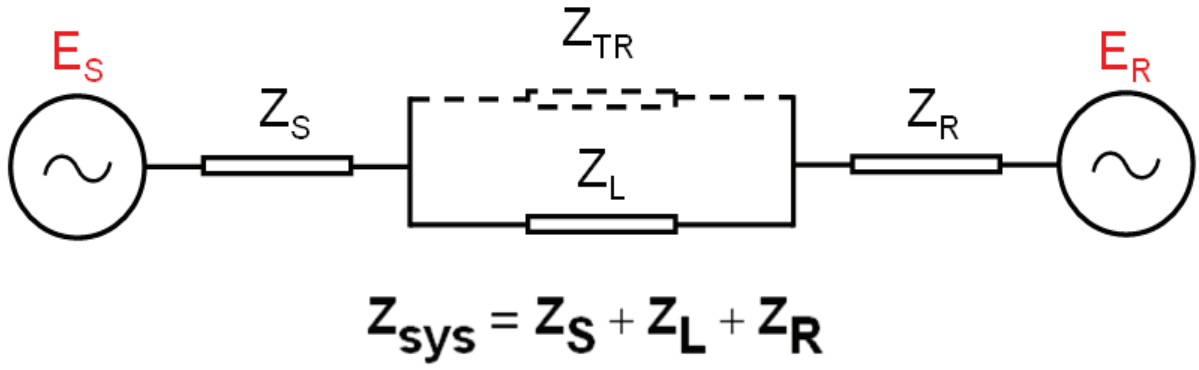


Figure 7: Reduced two bus system with sending-end source impedance Z_S, receiving-end source impedance Z_R, and line impedance Z_L with the parallel transfer impedance Z_{TR} removed.

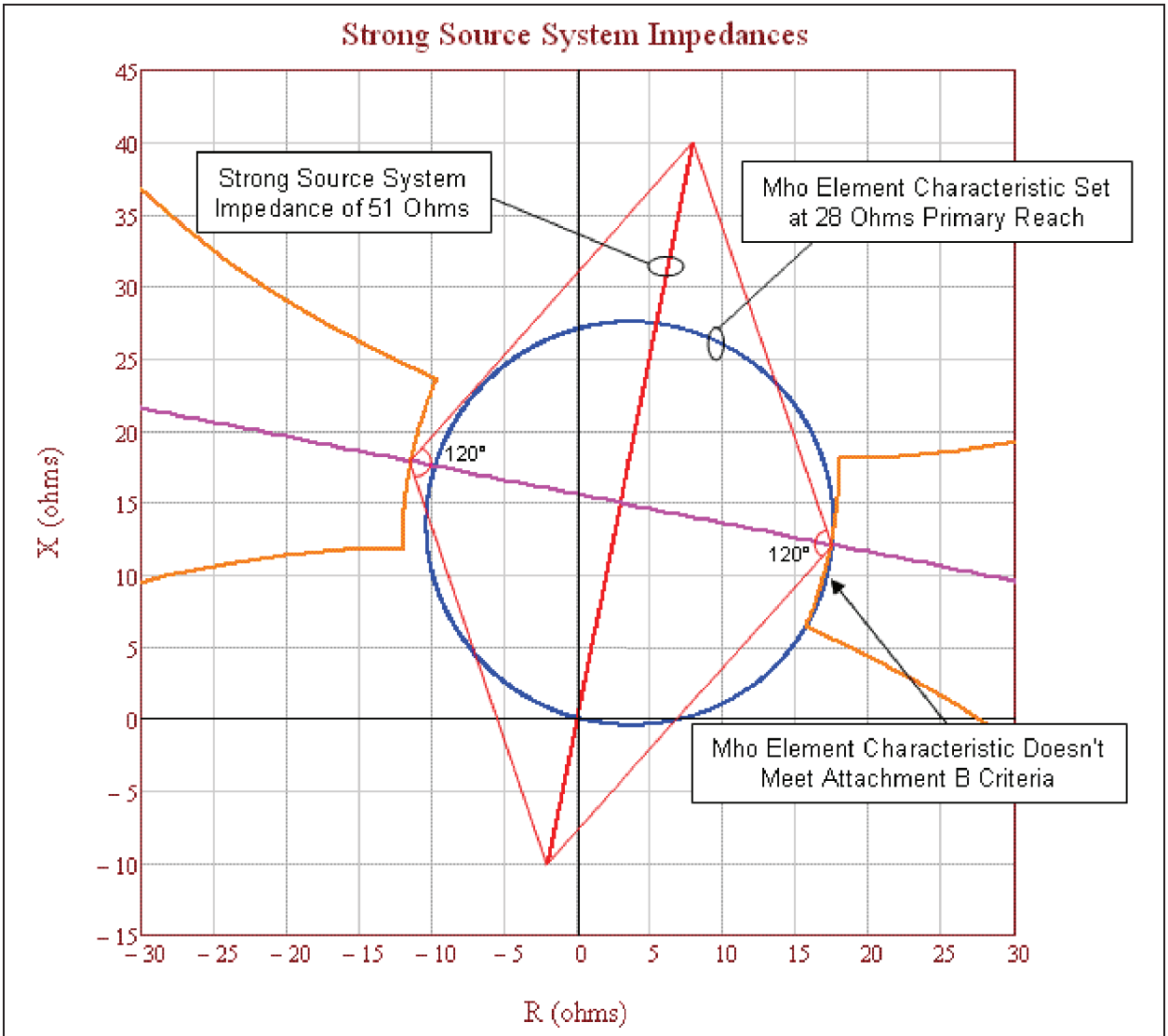


Figure 8: A strong-source system with a line impedance of Z_L = 20.4 ohms (i.e., the thicker red line). This mho element characteristic (i.e., the blue circle) does not meet the PRC-026-1 – Attachment B, Criterion A because it is not completely contained within the unstable power swing region (i.e., the orange characteristic).

Figure 8 above represents a heavily-loaded system with all generation in service and all transmission BES Elements in their normal operating state. The mho element characteristic (set at 137% of Z_L) extends into the unstable power swing region (i.e., the orange characteristic). Using the strongest source system is more conservative because it shrinks the unstable power swing region, bringing it closer to the mho element characteristic. This figure also graphically represents the effect of a system strengthening over time and this is the reason for re-evaluation if the relay has not been evaluated in the last five calendar years. Figure 9 below depicts a relay that meets the PRC-026-1 – Attachment B, Criterion A. Figure 8 depicts the same relay with the same setting five years later, where each source has strengthened by about 10% and now the same mho element characteristic does not meet Criterion A.

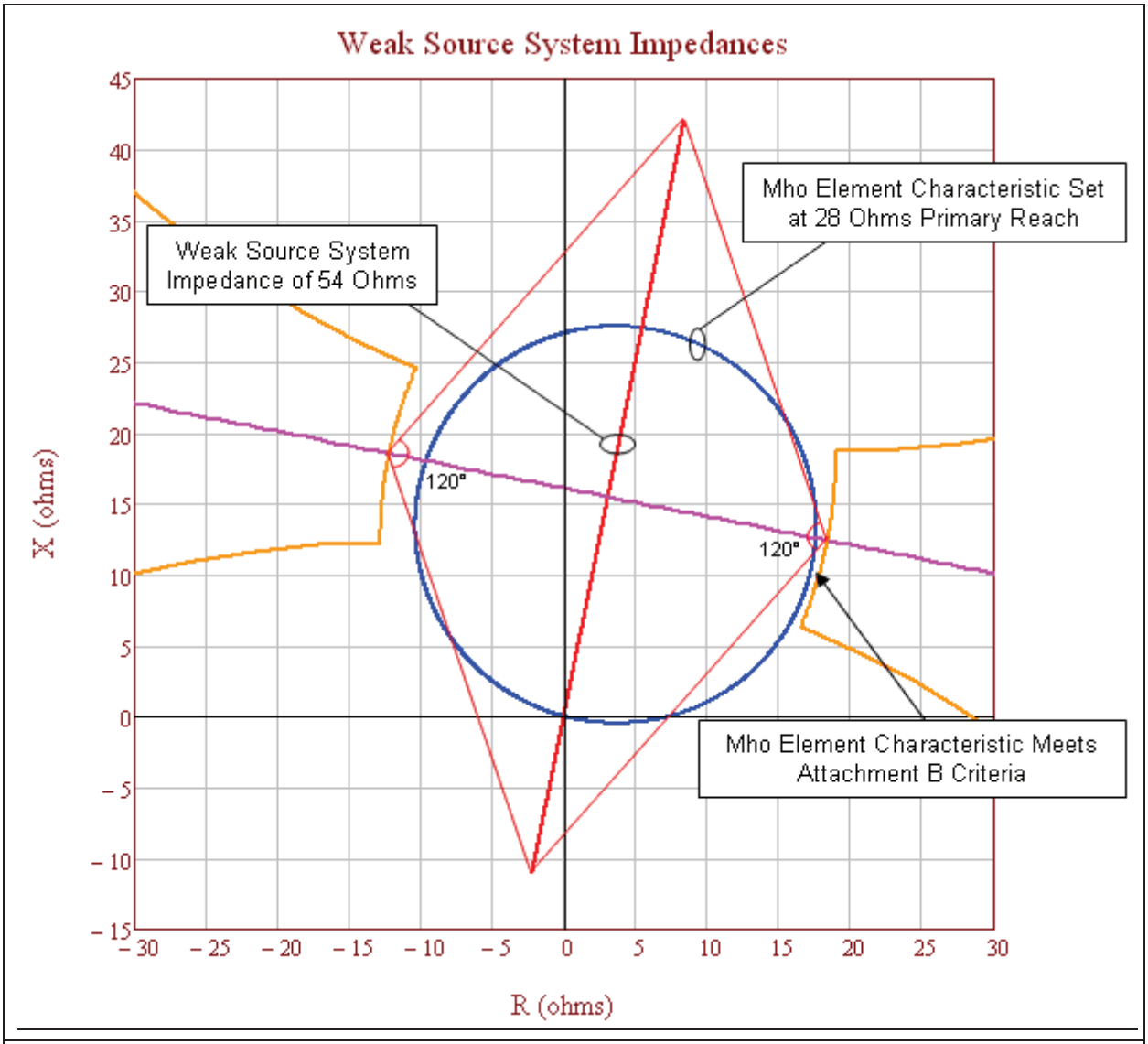


Figure 9: A weak-source system with a line impedance of Z_L = 20.4 ohms (i.e., the thicker red line). This mho element characteristic (i.e., the blue circle) meets the PRC-026-1 – Attachment B, Criterion A because it is completely contained within the unstable power swing region (i.e., the orange characteristic).

Figure 9 above represents a lightly-loaded system, using a minimum generation profile. The mho element characteristic (set at 137% of Z_L) does not extend into the unstable power swing region (i.e., the orange characteristic). Using a weaker source system expands the unstable power swing region away from the mho element characteristic.

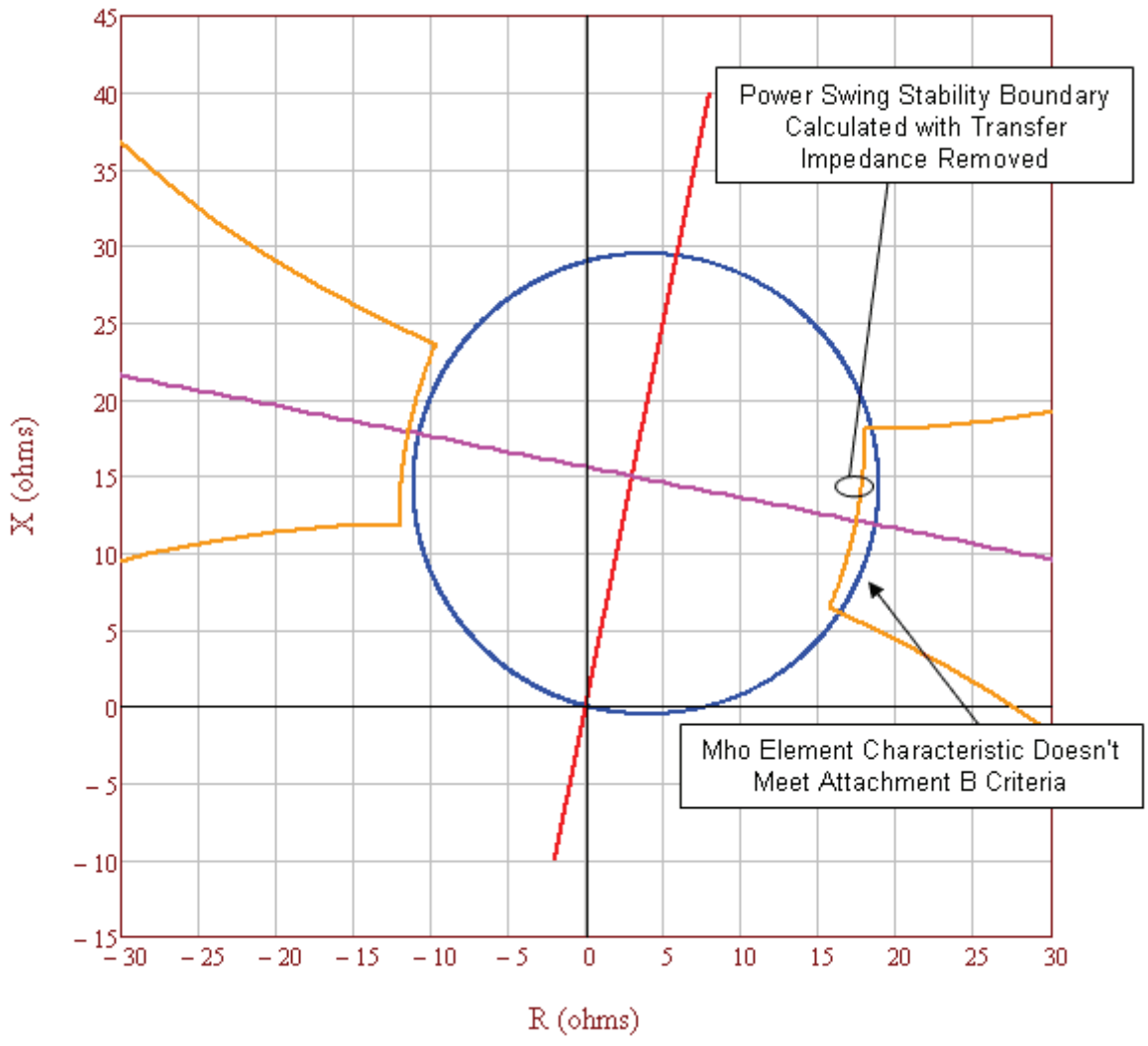


Figure 10: This is an example of an unstable power swing region (i.e., the orange characteristic) with the parallel transfer impedance removed. This relay mho element characteristic (i.e., the blue circle) does not meet PRC-026-1 – Attachment B, Criterion A because it is not completely contained within the unstable power swing region.

Table 8: Example Calculation (Parallel Transfer Impedance Removed)	
Calculations for the point at 120 degrees with equal source impedances. The total system current equals the line current. See Figure 10.	
Eq. (54)	$E_S = \frac{V_{LL}\angle 120°}{\sqrt{3}}$
	$E_S = \frac{230{,}000\angle 120°\ V}{\sqrt{3}}$
	$E_S = 132{,}791\angle 120°\ V$

Table 8: Example Calculation (Parallel Transfer Impedance Removed)			
Eq. (55)	$E_R = \frac{V_{LL}\angle 0°}{\sqrt{3}}$		
	$E_R = \frac{230{,}000\angle 0°\ V}{\sqrt{3}}$		
	$E_R = 132{,}791\angle 0°\ V$		
Given impedance data.			
Given:	$Z_S = 2 + j10\ \Omega$	$Z_L = 4 + j20\ \Omega$	$Z_R = 4 + j20\ \Omega$
Given:	$Z_{TR} = Z_L \times 10^{10}\ \Omega$		
Total impedance between the generators.			
Eq. (56)	$Z_{total} = \frac{(Z_L \times Z_{TR})}{(Z_L + Z_{TR})}$		
	$Z_{total} = \frac{\left((4 + j20)\ \Omega \times (4 + j20) \times 10^{10}\ \Omega\right)}{\left((4 + j20)\ \Omega + (4 + j20) \times 10^{10}\ \Omega\right)}$		
	$Z_{total} = 4 + j20\ \Omega$		
Total system impedance.			
Eq. (57)	$Z_{sys} = Z_S + Z_{total} + Z_R$		
	$Z_{sys} = (2 + j10)\ \Omega + (4 + j20)\ \Omega + (4 + j20)\ \Omega$		
	$Z_{sys} = 10 + j50\ \Omega$		
Total system current from sending-end source.			
Eq. (58)	$I_{sys} = \frac{E_S - E_R}{Z_{sys}}$		
	$I_{sys} = \frac{132{,}791\angle 120°\ V - 132{,}791\angle 0°\ V}{10 + j50\ \Omega}$		
	$I_{sys} = 4{,}511\angle 71.3°\ A$		
The current, as measured by the relay on Z_L (Figure 3), is only the current flowing through that line as determined by using the current divider equation.			
Eq. (59)	$I_L = I_{sys} \times \frac{Z_{TR}}{Z_L + Z_{TR}}$		
	$I_L = 4{,}511\angle 71.3°\ A \times \frac{(4 + j20) \times 10^{10}\ \Omega}{(4 + j20)\ \Omega + (4 + j20) \times 10^{10}\ \Omega}$		
	$I_L = 4{,}511\angle 71.3°\ A$		

Table 8: Example Calculation (Parallel Transfer Impedance Removed)	
The voltage, as measured by the relay on Z_L (Figure 3), is the voltage drop from the sending-end source through the sending-end source impedance.	
Eq. (60)	$V_S = E_S - (Z_S \times I_{sys})$
	$V_S = 132{,}791\angle 120° \, V - [(2 + j10\ \Omega) \times 4{,}511\angle 71.3° \, A]$
	$V_S = 95{,}757\angle 106.1° \, V$
The impedance seen by the relay on Z_L.	
Eq. (61)	$Z_{L-Relay} = \frac{V_S}{I_L}$
	$Z_{L-Relay} = \frac{95{,}757\angle 106.1° \, V}{4{,}511\angle 71.3° \, A}$
	$Z_{L-Relay} = 17.434 + j12.113\ \Omega$

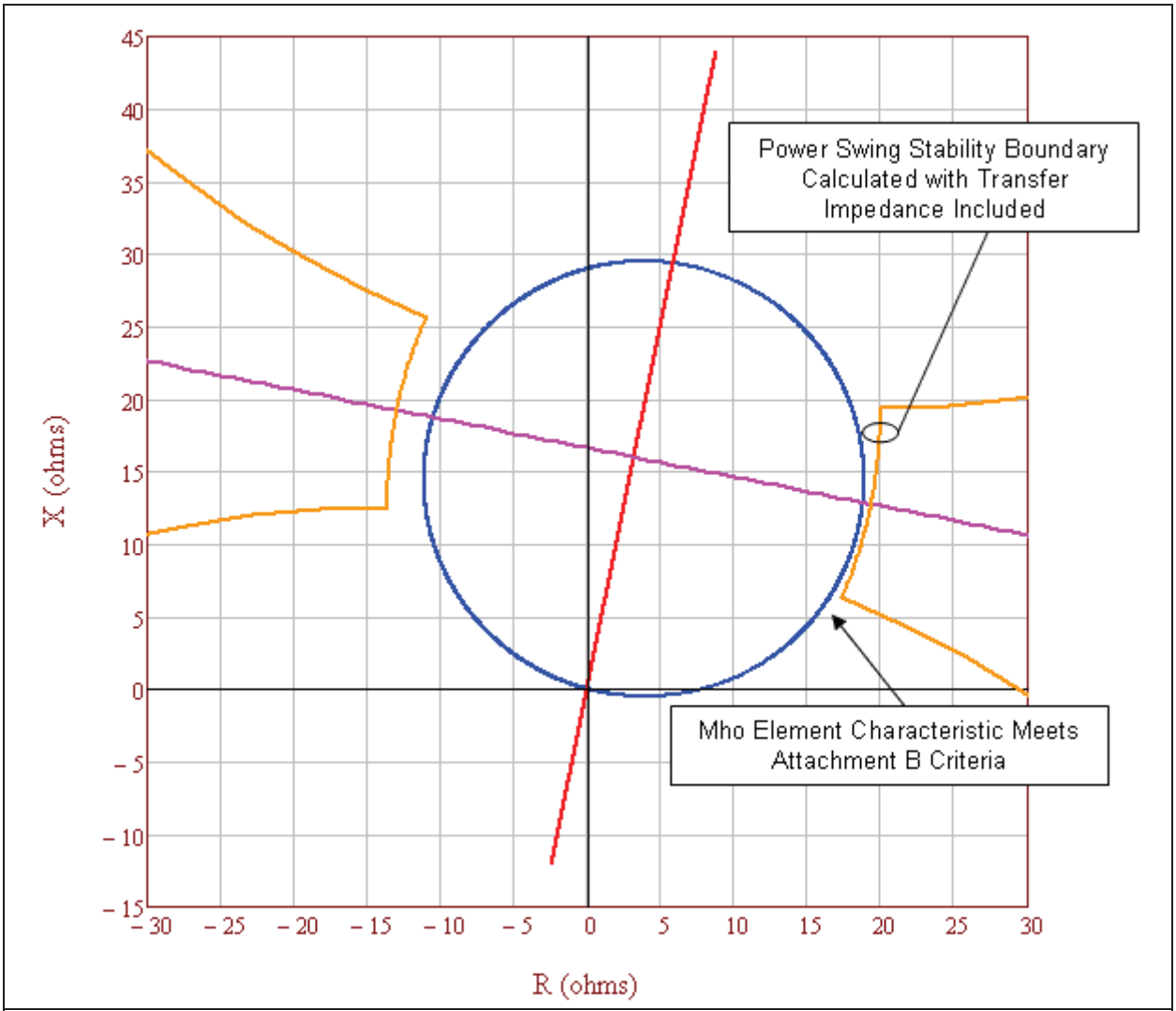


Figure 11: This is an example of an unstable power swing region (i.e., the orange characteristic) with the parallel transfer impedance included causing the mho element characteristic (i.e., the blue circle) to appear to meet the PRC-026-1 – Attachment B, Criterion A because it is completely contained within the unstable power swing region. Including the parallel transfer impedance in the calculation is not allowed by the PRC-026-1 – Attachment B, Criterion A.

In Figure 11 above, the parallel transfer impedance is 5 times the line impedance. The unstable power swing region has expanded out beyond the mho element characteristic due to the infeed effect from the parallel current through the parallel transfer impedance, thus allowing the mho element characteristic to appear to meet the PRC-026-1 – Attachment B, Criterion A. Including the parallel transfer impedance in the calculation is not allowed by the PRC-026-1 – Attachment B, Criterion A.

Table 9: Example Calculation (Parallel Transfer Impedance Included)			
Calculations for the point at 120 degrees with equal source impedances. The total system current does not equal the line current. See Figure 11.			
Eq. (62)	$E_S = \frac{V_{LL}\angle 120°}{\sqrt{3}}$		
	$E_S = \frac{230{,}000\angle 120°\ V}{\sqrt{3}}$		
	$E_S = 132{,}791\angle 120°\ V$		
Eq. (63)	$E_R = \frac{V_{LL}\angle 0°}{\sqrt{3}}$		
	$E_R = \frac{230{,}000\angle 0°\ V}{\sqrt{3}}$		
	$E_R = 132{,}791\angle 0°\ V$		
Given impedance data.			
Given:	$Z_S = 2 + j10\ \Omega$	$Z_L = 4 + j20\ \Omega$	$Z_R = 4 + j20\ \Omega$
Given:	$Z_{TR} = Z_L \times 5$		
	$Z_{TR} = (4 + j20)\ \Omega \times 5$		
	$Z_{TR} = 20 + j100\ \Omega$		
Total impedance between the generators.			
Eq. (64)	$Z_{total} = \frac{(Z_L \times Z_{TR})}{(Z_L + Z_{TR})}$		
	$Z_{total} = \frac{(4 + j20)\ \Omega \times (20 + j100)\ \Omega}{(4 + j20)\ \Omega + (20 + j100)\ \Omega}$		
	$Z_{total} = 3.333 + j16.667\ \Omega$		
Total system impedance.			
Eq. (65)	$Z_{sys} = Z_S + Z_{total} + Z_R$		
	$Z_{sys} = (2 + j10)\ \Omega + (3.333 + j16.667)\ \Omega + (4 + j20)\ \Omega$		
	$Z_{sys} = 9.333 + j46.667\ \Omega$		
Total system current from sending-end source.			
Eq. (66)	$I_{sys} = \frac{E_S - E_R}{Z_{sys}}$		
	$I_{sys} = \frac{132{,}791\angle 120°\ V - 132{,}791\angle 0°\ V}{9.333 + j46.667\ \Omega}$		

Table 9: Example Calculation (Parallel Transfer Impedance Included)	
	$I_{sys} = 4{,}833\angle 71.3° \; A$
The current, as measured by the relay on Z_L (Figure 3), is only the current flowing through that line as determined by using the current divider equation.	
Eq. (67)	$I_L = I_{sys} \times \frac{Z_{TR}}{Z_L + Z_{TR}}$
	$I_L = 4{,}833\angle 71.3° \; A \times \frac{(20 + j100)\;\Omega}{(4 + j20)\;\Omega + (20 + j100)\;\Omega}$
	$I_L = 4{,}027.4\angle 71.3° \; A$
The voltage, as measured by the relay on Z_L (Figure 3), is the voltage drop from the sending-end source through the sending-end source impedance.	
Eq. (68)	$V_S = E_S - (Z_S \times I_{sys})$
	$V_S = 132{,}791\angle 120° \; V - [(2 + j10\;\Omega) \times 4{,}833\angle 71.3° \; A]$
	$V_S = 93{,}417\angle 104.7° \; V$
The impedance seen by the relay on Z_L.	
Eq. (69)	$Z_{L-Relay} = \frac{V_S}{I_L}$
	$Z_{L-Relay} = \frac{93{,}417\angle 104.7° \; V}{4{,}027\angle 71.3° \; A}$
	$Z_{L-Relay} = 19.366 + j12.767\;\Omega$

Table 10: Percent Increase of a Lens Due To Parallel Transfer Impedance.	
The following demonstrates the percent size increase of the lens characteristic for Z_{TR} in multiples of Z_L with the parallel transfer impedance included.	
Z_{TR} in multiples of Z_L	Percent increase of lens with equal EMF sources (Infinite source as reference)
Infinite	N/A
1000	0.05%
100	0.46%
10	4.63%
5	9.27%
2	23.26%
1	46.76%
0.5	94.14%
0.25	189.56%

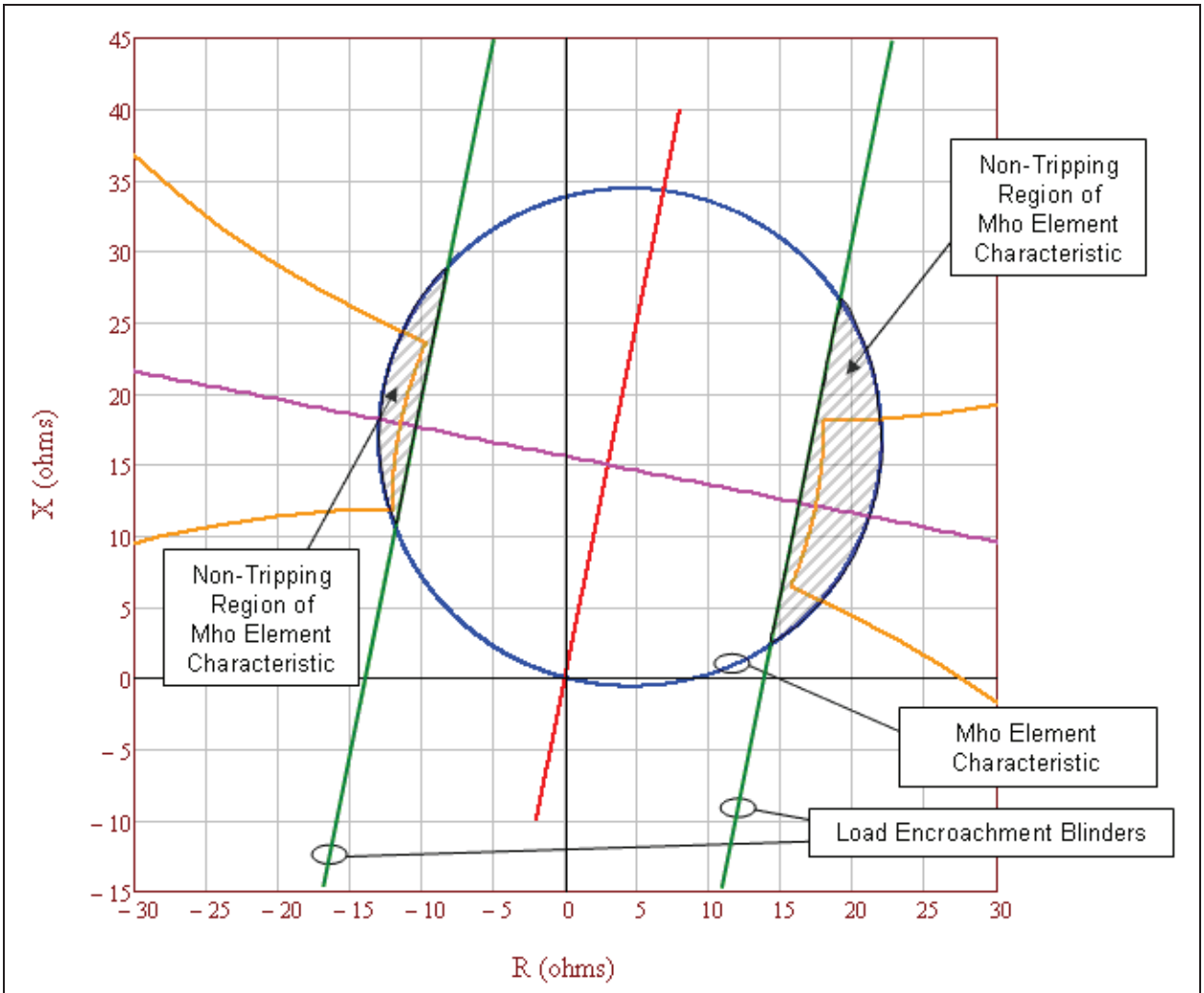


Figure 12: The tripping portion of the mho element characteristic (i.e., the blue circle) not blocked by load encroachment (i.e., the parallel green lines) is completely contained within the unstable power swing region (i.e., the orange characteristic). Therefore, the mho element characteristic meets the PRC-026-1 – Attachment B, Criterion A.

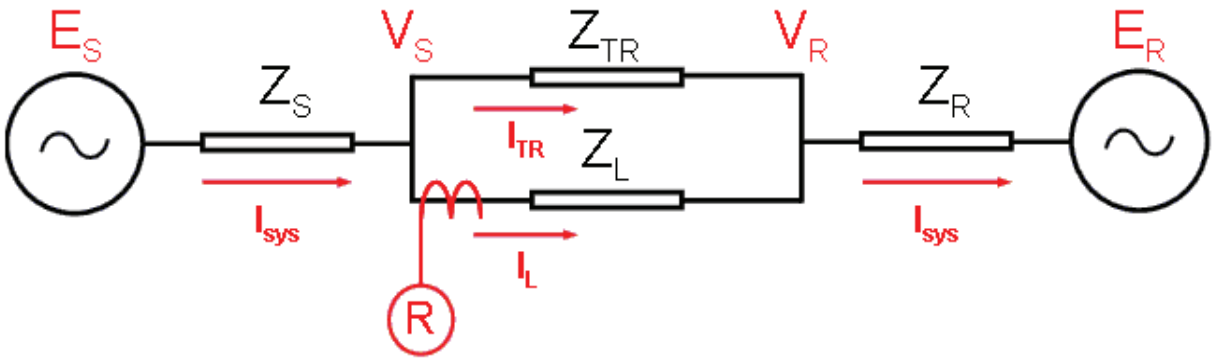


Figure 13: The infeed diagram shows the impedance in front of the relay R with the parallel transfer impedance included. As the parallel transfer impedance approaches infinity, the impedances seen by the relay R in the forward direction becomes $Z_L + Z_R$.

Table 11: Calculations (System Apparent Impedance in the forward direction)

The following equations are provided for calculating the apparent impedance back to the E_R source voltage as seen by relay R. Infeed equations from V_S to source E_R where $E_R = 0$. See Figure 13.

Eq. (70)	$I_L = \frac{V_S - V_R}{Z_L}$			
Eq. (71)	$I_{sys} = \frac{V_R - E_R}{Z_R}$			
Eq. (72)	$I_{sys} = I_L + I_{TR}$			
Eq. (73)	$I_{sys} = \frac{V_R}{Z_R}$	Since $E_R = 0$	Rearranged:	$V_R = I_{sys} \times Z_R$
Eq. (74)	$I_L = \frac{V_S - I_{sys} \times Z_R}{Z_L}$			
Eq. (75)	$I_L = \frac{V_S - [(I_L + I_{TR}) \times Z_R]}{Z_L}$			
Eq. (76)	$V_S = (I_L \times Z_L) + (I_L \times Z_R) + (I_{TR} \times Z_R)$			
Eq. (77)	$Z_{Relay} = \frac{V_S}{I_L} = Z_L + Z_R + \frac{I_{TR} \times Z_R}{I_L} = Z_L + Z_R \times \left(1 + \frac{I_{TR}}{I_L}\right)$			
Eq. (78)	$I_{TR} = I_{sys} \times \frac{Z_L}{Z_L + Z_{TR}}$			
Eq. (79)	$I_L = I_{sys} \times \frac{Z_{TR}}{Z_L + Z_{TR}}$			

Table 11: Calculations (System Apparent Impedance in the forward direction)	
Eq. (80)	$\frac{I_{TR}}{I_L} = \frac{Z_L}{Z_{TR}}$
The infeed equations shows the impedance in front of the relay R (Figure 13) with the parallel transfer impedance included. As the parallel transfer impedance approaches infinity, the impedances seen by the relay R in the forward direction becomes $Z_L + Z_R$.	
Eq. (81)	$Z_{Relay} = Z_L + Z_R \times \left(1 + \frac{Z_L}{Z_{TR}}\right)$

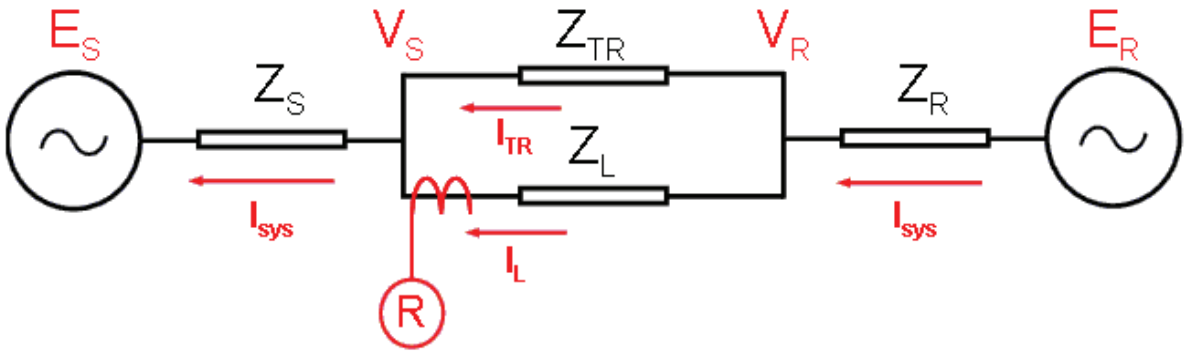


Figure 14: The infeed diagram shows the impedance behind relay R with the parallel transfer impedance included. As the parallel transfer impedance approaches infinity, the impedances seen by the relay R in the reverse direction becomes Z_S.

Table 12: Calculations (System Apparent Impedance in the Reverse Direction)				
The following equations are provided for calculating the apparent impedance back to the E_S source voltage as seen by relay R. Infeed equations from V_R back to source E_S where $E_S = 0$. See Figure 14.				
Eq. (82)	$I_L = \frac{V_R - V_S}{Z_L}$			
Eq. (83)	$I_{sys} = \frac{V_S - E_S}{Z_S}$			
Eq. (84)	$I_{sys} = I_L + I_{TR}$			
Eq. (85)	$I_{sys} = \frac{V_S}{Z_S}$	Since $E_s = 0$	Rearranged:	$V_S = I_{sys} \times Z_S$
Eq. (86)	$I_L = \frac{V_R - I_{sys} \times Z_S}{Z_L}$			

Table 12: Calculations (System Apparent Impedance in the Reverse Direction)		
Eq. (87)	$I_L = \frac{V_R - [(I_L + I_{TR}) \times Z_S]}{Z_L}$	
Eq. (88)	$V_R = (I_L \times Z_L) + (I_L \times Z_S) + (I_{TR} \times Z_{RS})$	
Eq. (89)	$Z_{Relay} = \frac{V_R}{I_L} = Z_L + Z_S + \frac{I_{TR} \times Z_S}{I_L} = Z_L + Z_S \times \left(1 + \frac{I_{TR}}{I_L}\right)$	
Eq. (90)	$I_{TR} = I_{sys} \times \frac{Z_L}{Z_L + Z_{TR}}$	
Eq. (91)	$I_L = I_{sys} \times \frac{Z_{TR}}{Z_L + Z_{TR}}$	
Eq. (92)	$\frac{I_{TR}}{I_L} = \frac{Z_L}{Z_{TR}}$	
The infeed equations shows the impedance behind relay R (Figure 14) with the parallel transfer impedance included. As the parallel transfer impedance approaches infinity, the impedances seen by the relay R in the reverse direction becomes Z_S.		
Eq. (93)	$Z_{Relay} = Z_L + Z_S \times \left(1 + \frac{Z_L}{Z_{TR}}\right)$	As seen by relay R at the receiving-end of the line.
Eq. (94)	$Z_{Relay} = Z_S \times \left(1 + \frac{Z_L}{Z_{TR}}\right)$	Subtract Z_L for relay R impedance as seen at sending-end of the line.

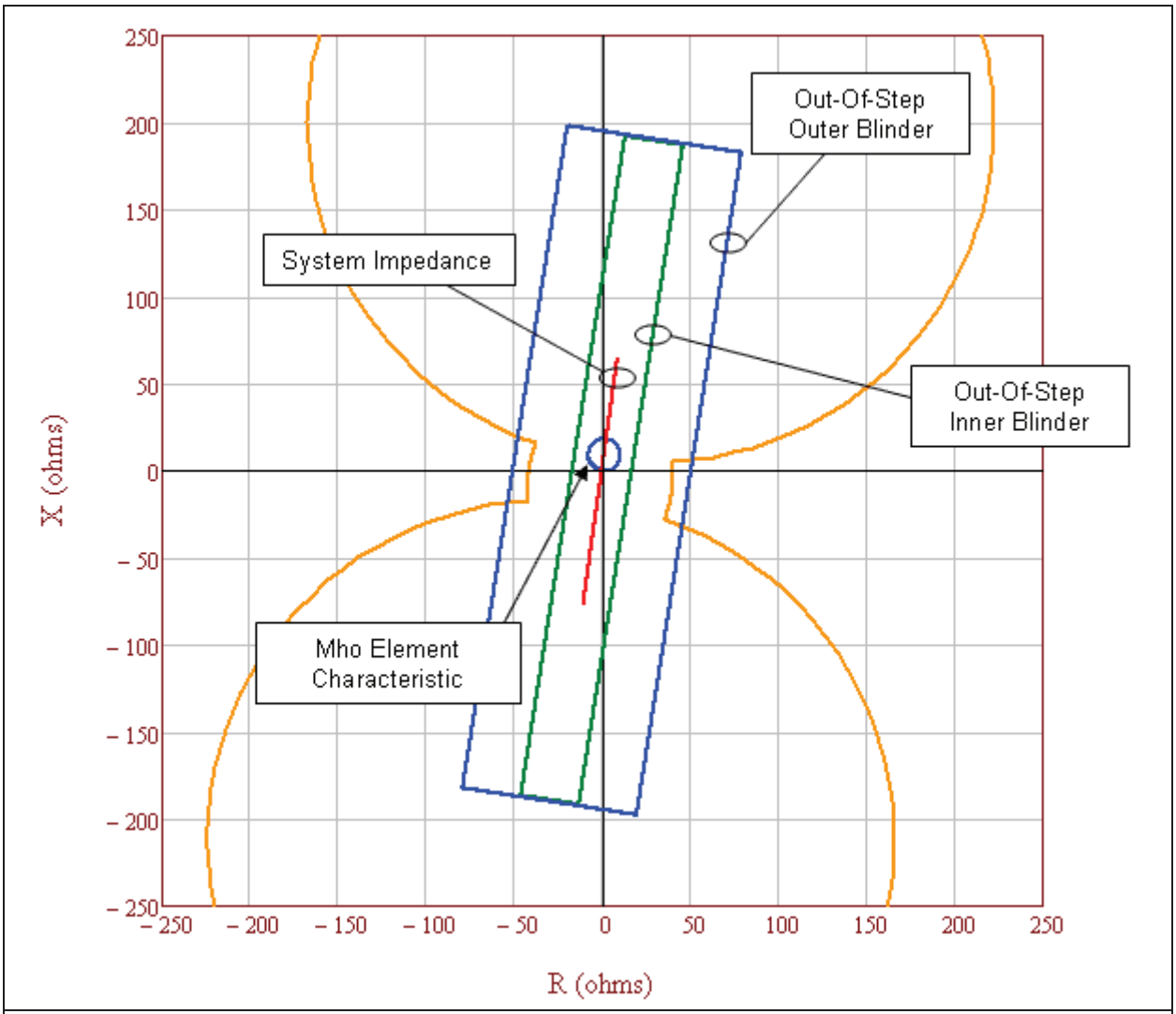


Figure 15: Out-of-step trip (OST) inner blinder (i.e., the parallel green lines) meets the PRC-026-1 – Attachment B, Criterion A because the inner OST blinder initiates tripping either On-The-Way-In or On-The-Way-Out. Since the inner blinder is completely contained within the unstable power swing region (i.e., the orange characteristic), it meets the PRC-026-1 – Attachment B, Criterion A.

Table 13: Example Calculation (Voltage Ratios)			
These calculations are based on the loss-of-synchronism characteristics for the cases of N < 1 and N > 1 as found in the *Application of Out-of-Step Blocking and Tripping Relays*, GER-3180, p. 12, Figure 3.[18] The GE illustration shows the formulae used to calculate the radius and center of the circles that make up the ends of the portion of the lens.			
Voltage ratio equations, source impedance equation with infeed formulae applied, and circle equations.			
Given:	$E_S = 0.7$	$E_R = 1.0$	
Eq. (95)	$N = \frac{\lvert E_S \rvert}{\lvert E_R \rvert} = \frac{0.7}{1.0} = 0.7$		
The total system impedance as seen by the relay with infeed formulae applied.			
Given:	$Z_S = 2 + j10\ \Omega$	$Z_L = 4 + j20\ \Omega$	$Z_R = 4 + j20\ \Omega$
Given:	$Z_{TR} = Z_L \times 10^{10}\ \Omega$		
	$Z_{TR} = (4 + j20) \times 10^{10}\ \Omega$		
Eq. (96)	$Z_{sys} = Z_S \times \left(1 + \frac{Z_L}{Z_{TR}}\right) + \left[Z_L + Z_R \times \left(1 + \frac{Z_L}{Z_{TR}}\right)\right]$		
	$Z_{sys} = 10 + j50\ \Omega$		
The calculated coordinates of the lower loss-of-synchronism circle center.			
Eq. (97)	$Z_{C1} = -\left[Z_S \times \left(1 + \frac{Z_L}{Z_{TR}}\right)\right] - \left[\frac{N^2 \times Z_{sys}}{1 - N^2}\right]$		
	$Z_{C1} = -\left[(2 + j10)\ \Omega \times \left(1 + \frac{(4 + j20)\ \Omega}{(4 + j20) \times 10^{10}\ \Omega}\right)\right] - \left[\frac{0.7^2 \times (10 + j50)\ \Omega}{1 - 0.7^2}\right]$		
	$Z_{C1} = -11.608 - j58.039\ \Omega$		
The calculated radius of the lower loss-of-synchronism circle.			
Eq. (98)	$r_a = \left\lvert \frac{N \times Z_{sys}}{1 - N^2} \right\rvert$		
	$r_a = \left\lvert \frac{0.7 \times (10 + j50)\ \Omega}{1 - 0.7^2} \right\rvert$		
	$r_a = 69.987\ \Omega$		
The calculated coordinates of the upper loss-of-synchronism circle center.			
Given:	$E_S = 1.0$	$E_R = 0.7$	

[18] http://store.gedigitalenergy.com/faq/Documents/Alps/GER-3180.pdf

Table 13: Example Calculation (Voltage Ratios)	
Eq. (99)	$N = \frac{\lvert E_S \rvert}{\lvert E_R \rvert} = \frac{1.0}{0.7} = 1.43$
Eq. (100)	$Z_{C2} = Z_L + \left[Z_R \times \left(1 + \frac{Z_L}{Z_{TR}} \right) \right] + \left[\frac{Z_{sys}}{N^2 - 1} \right]$
	$Z_{C2} = 4 + j20\ \Omega + \left[(4 + j20)\ \Omega \times \left(1 + \frac{(4 + j20)\ \Omega}{(4 + j20) \times 10^{10}\ \Omega} \right) \right] + \left[\frac{(10 + j50)\ \Omega}{1.43^2 - 1} \right]$
	$Z_{C2} = 17.608 + j88.039\ \Omega$
The calculated radius of the upper loss-of-synchronism circle.	
Eq. (101)	$r_b = \left\lvert \frac{N \times Z_{sys}}{N^2 - 1} \right\rvert$
	$r_b = \left\lvert \frac{1.43 \times (10 + j50)\ \Omega}{1.43^2 - 1} \right\rvert$
	$r_b = 69.987\ \Omega$

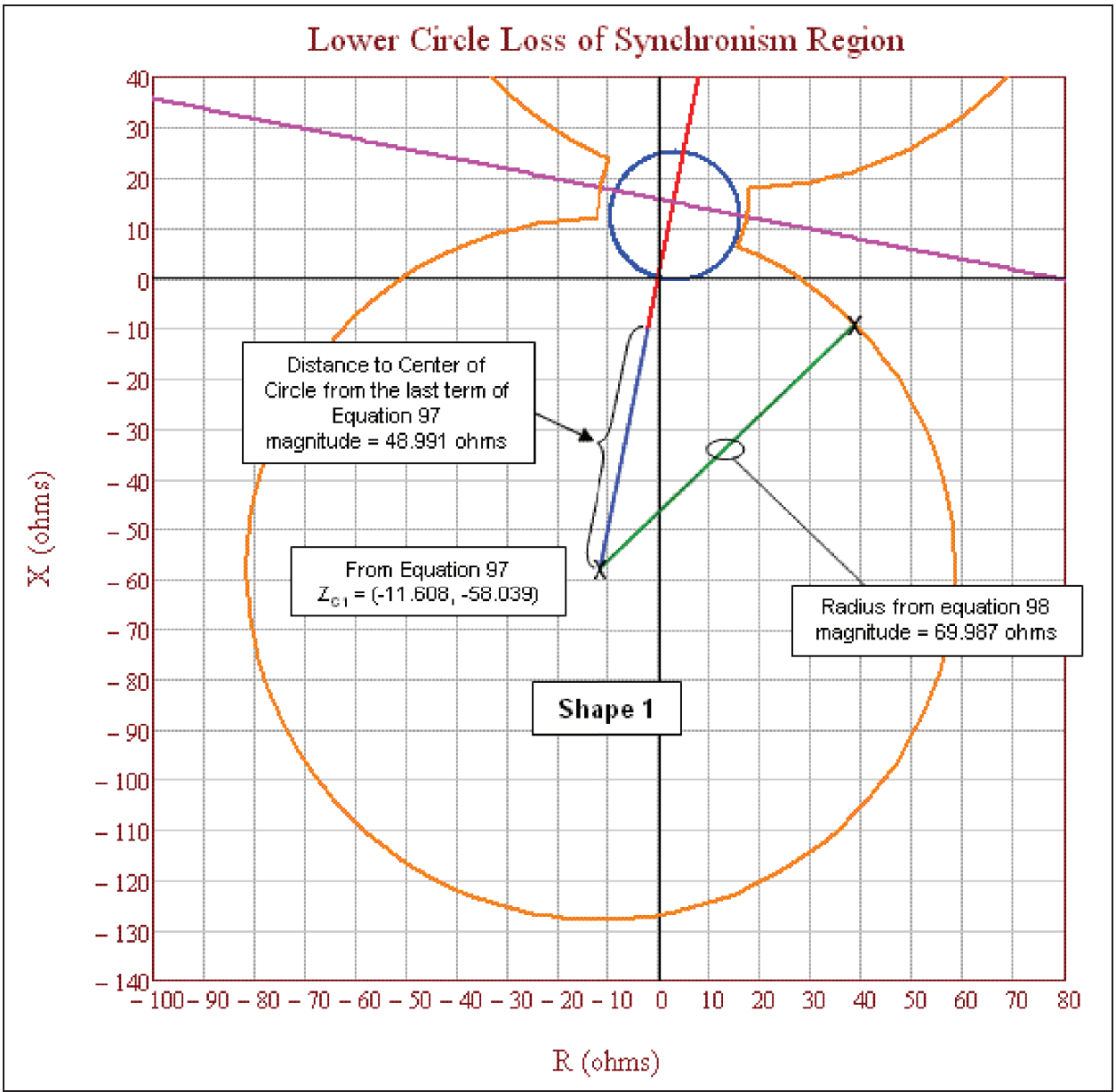


Figure 15a: Lower circle loss-of-synchronism region showing the coordinates of the circle center and the circle radius.

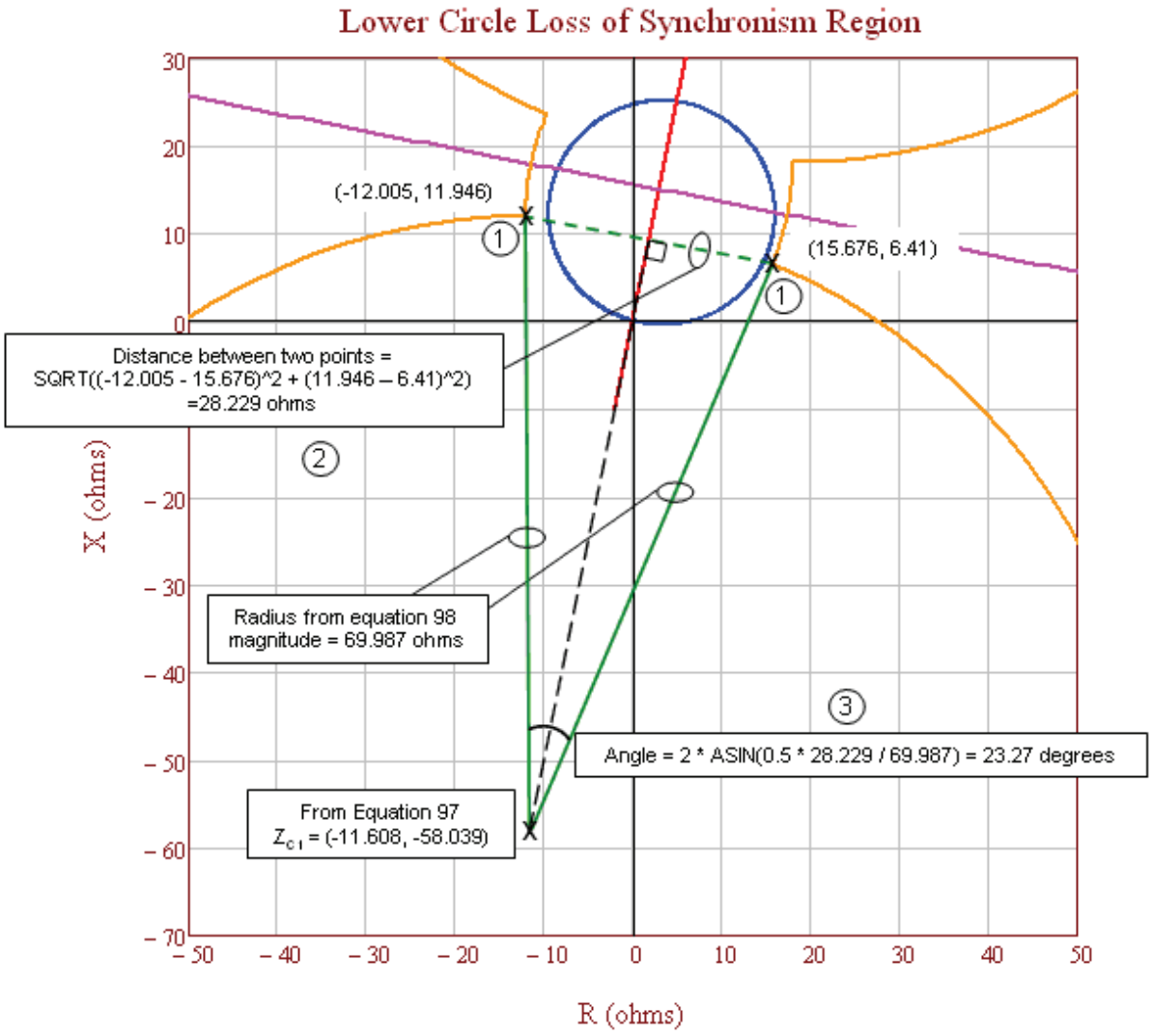


Figure 15b: Lower circle loss-of-synchronism region showing the first three steps to calculate the coordinates of the points on the circle. 1) Identify the lower circle loss-of-synchronism points that intersect the lens shape where the sending-end to receiving-end voltage ratio is 0.7 (see lens shape calculations in Tables 2-7). 2) Calculate the distance between the two lower circle loss-of-synchronism points identified in Step 1. 3) Calculate the angle of arc that connects the two lower circle loss-of-synchronism points identified in Step 1.

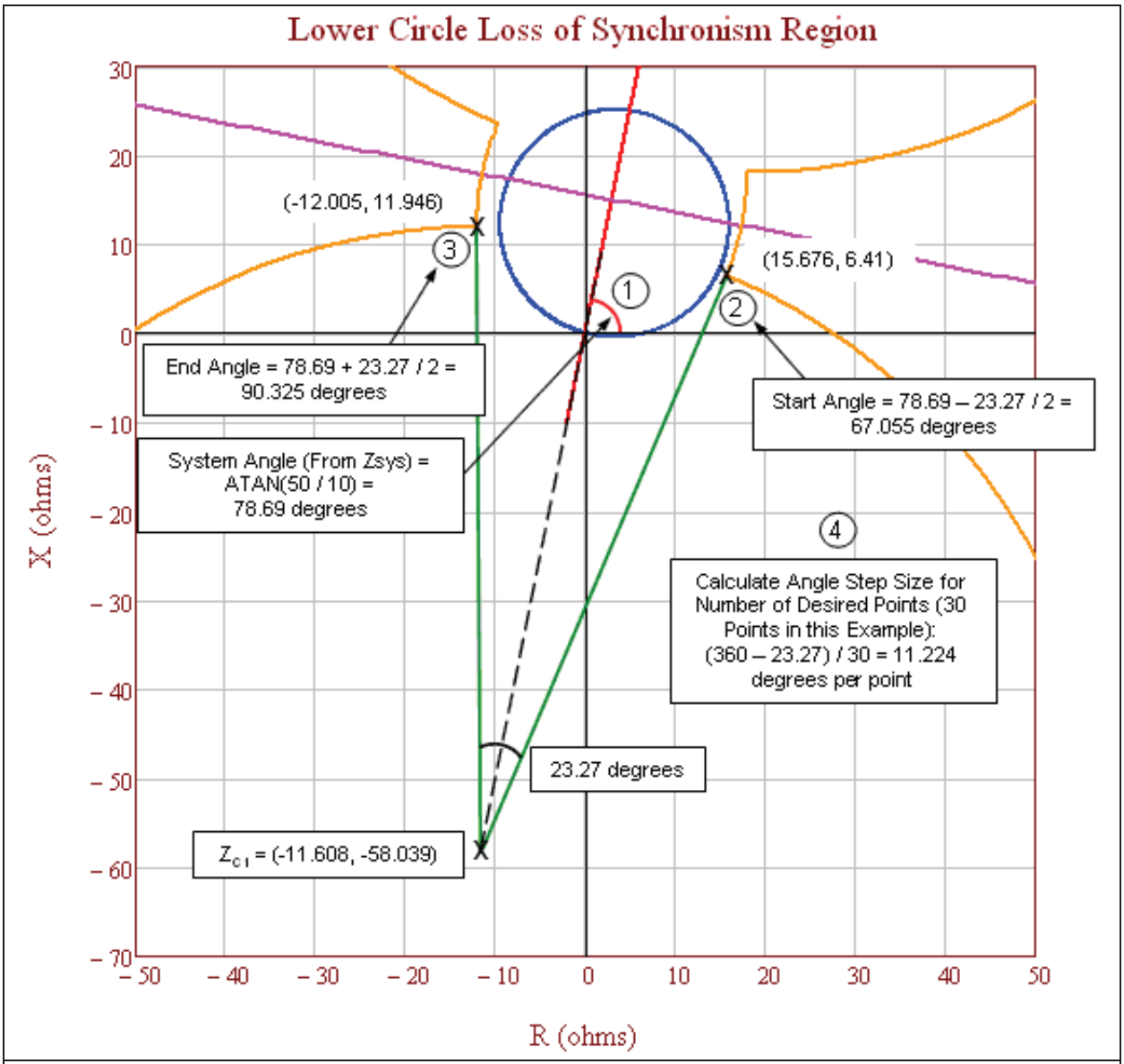


Figure 15c: Lower circle loss-of-synchronism region showing the steps to calculate the start angle, end angle, and the angle step size for the desired number of calculated points. 1) Calculate the system angle. 2) Calculate the start angle. 3) Calculate the end angle. 4) Calculate the angle step size for the desired number of points.

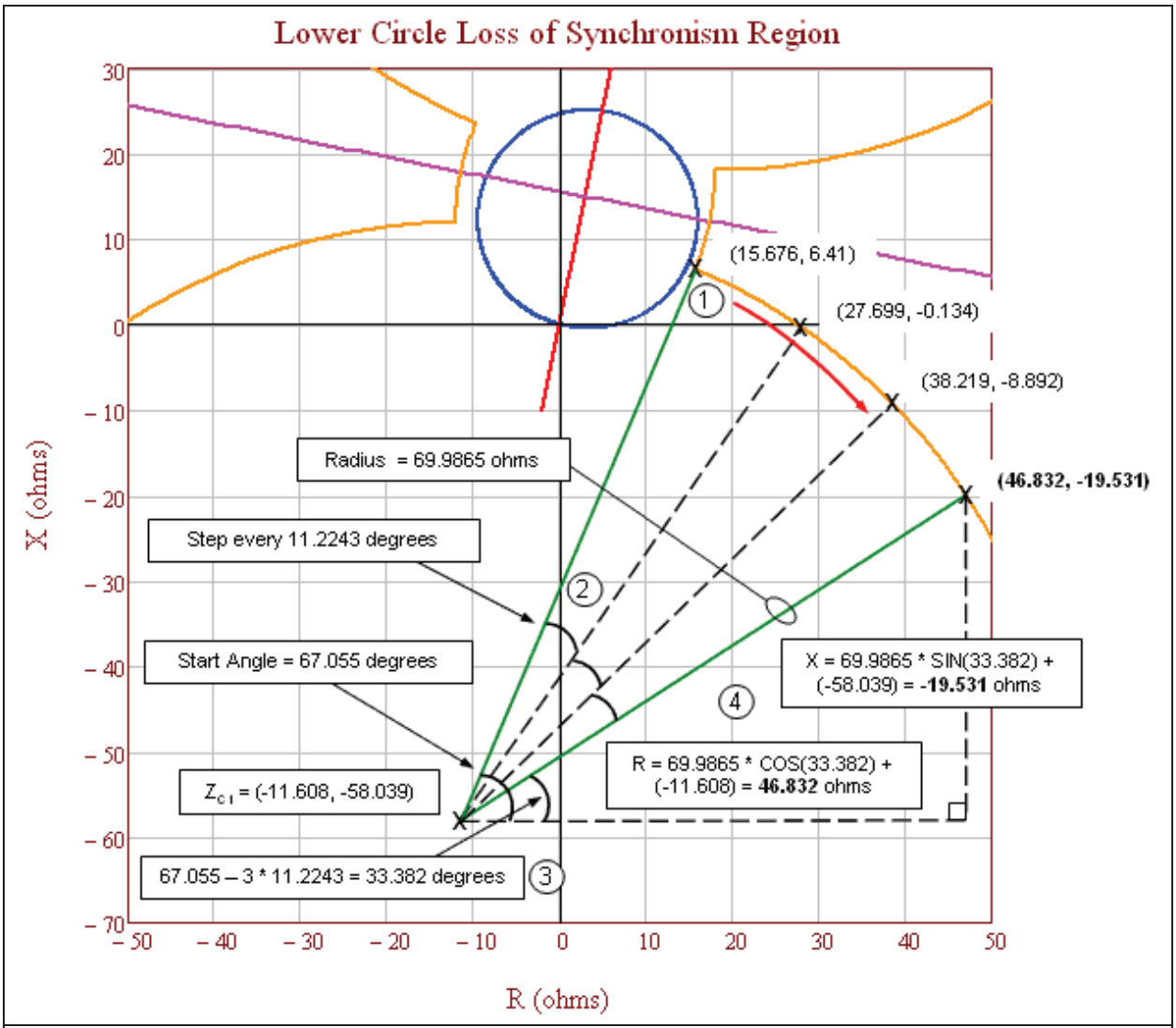


Figure 15d: Lower circle loss-of-synchronism region showing the final steps to calculate the coordinates of the points on the circle. 1) Start at the intersection with the lens shape and proceed in a clockwise direction. 2) Advance the step angle for each point. 3) Calculate the new angle after step advancement. 4) Calculate the R–X coordinates.

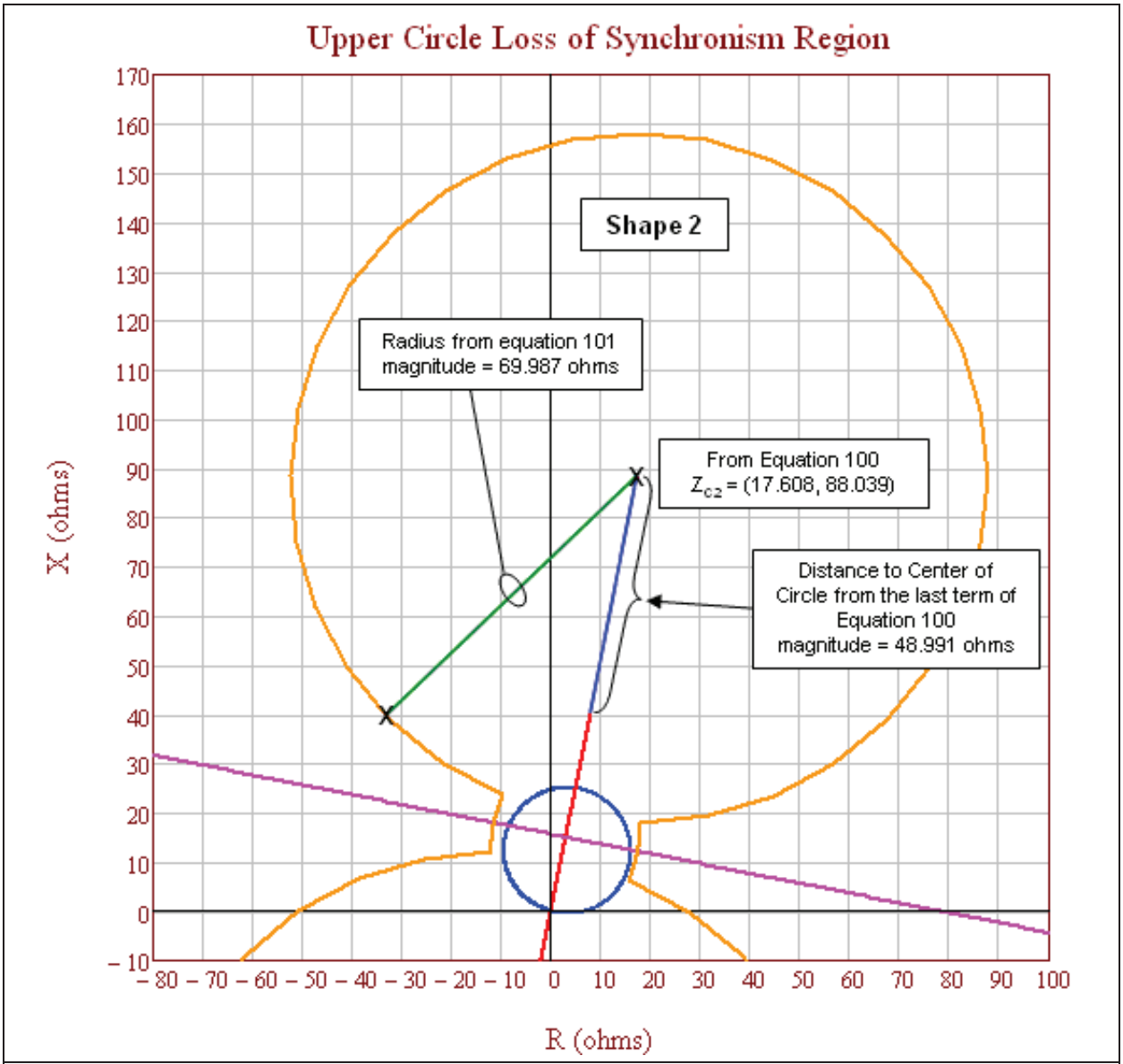


Figure 15e: Upper circle loss-of-synchronism region showing the coordinates of the circle center and the circle radius.

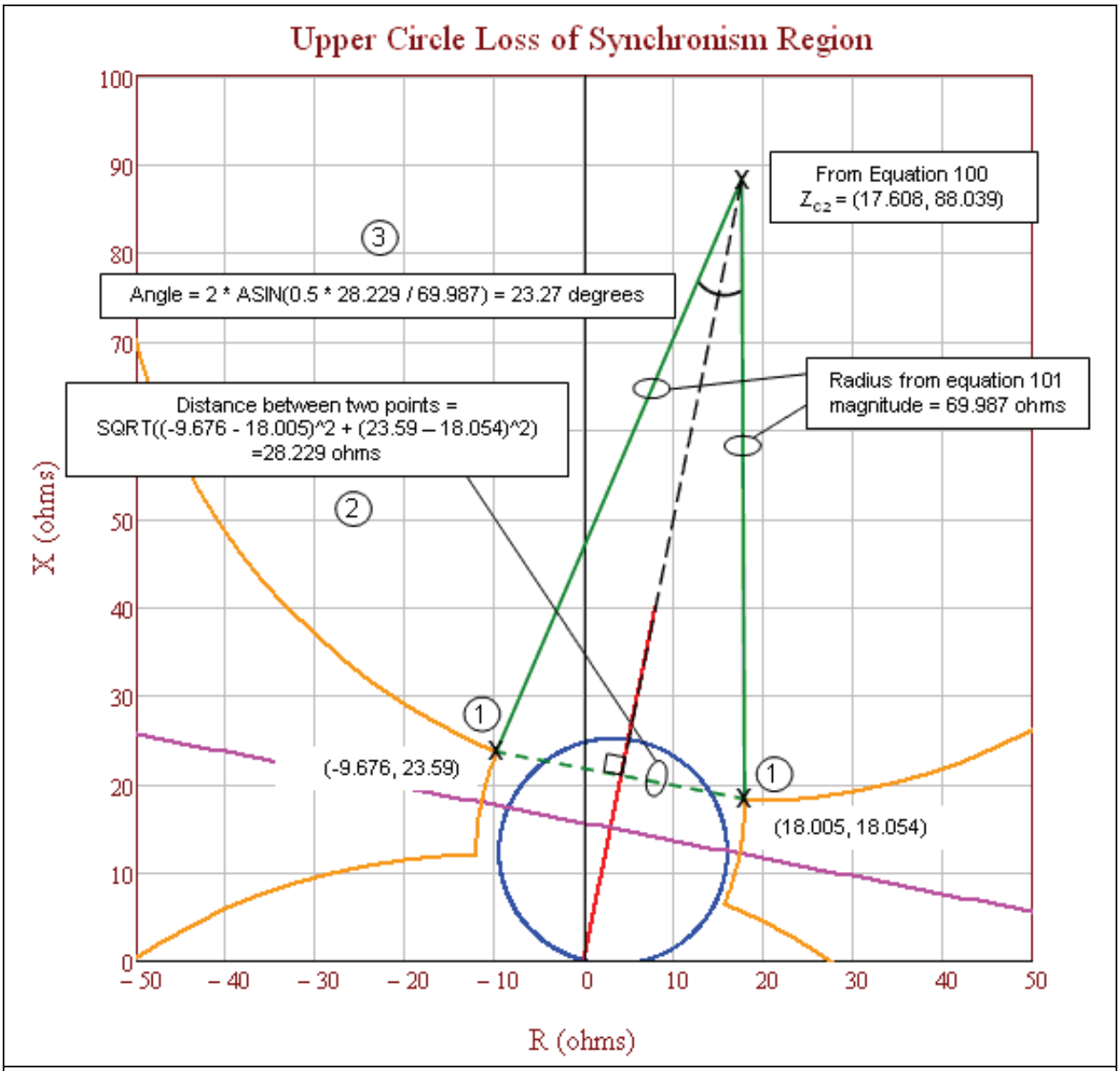


Figure 15f: Upper circle loss-of-synchronism region showing the first three steps to calculate the coordinates of the points on the circle. 1) Identify the upper circle points that intersect the lens shape where the sending-end to receiving-end voltage ratio is 1.43 (see lens shape calculations in Tables 2-7). 2) Calculate the distance between the two upper circle points identified in Step 1. 3) Calculate the angle of arc that connects the two upper circle points identified in Step 1.

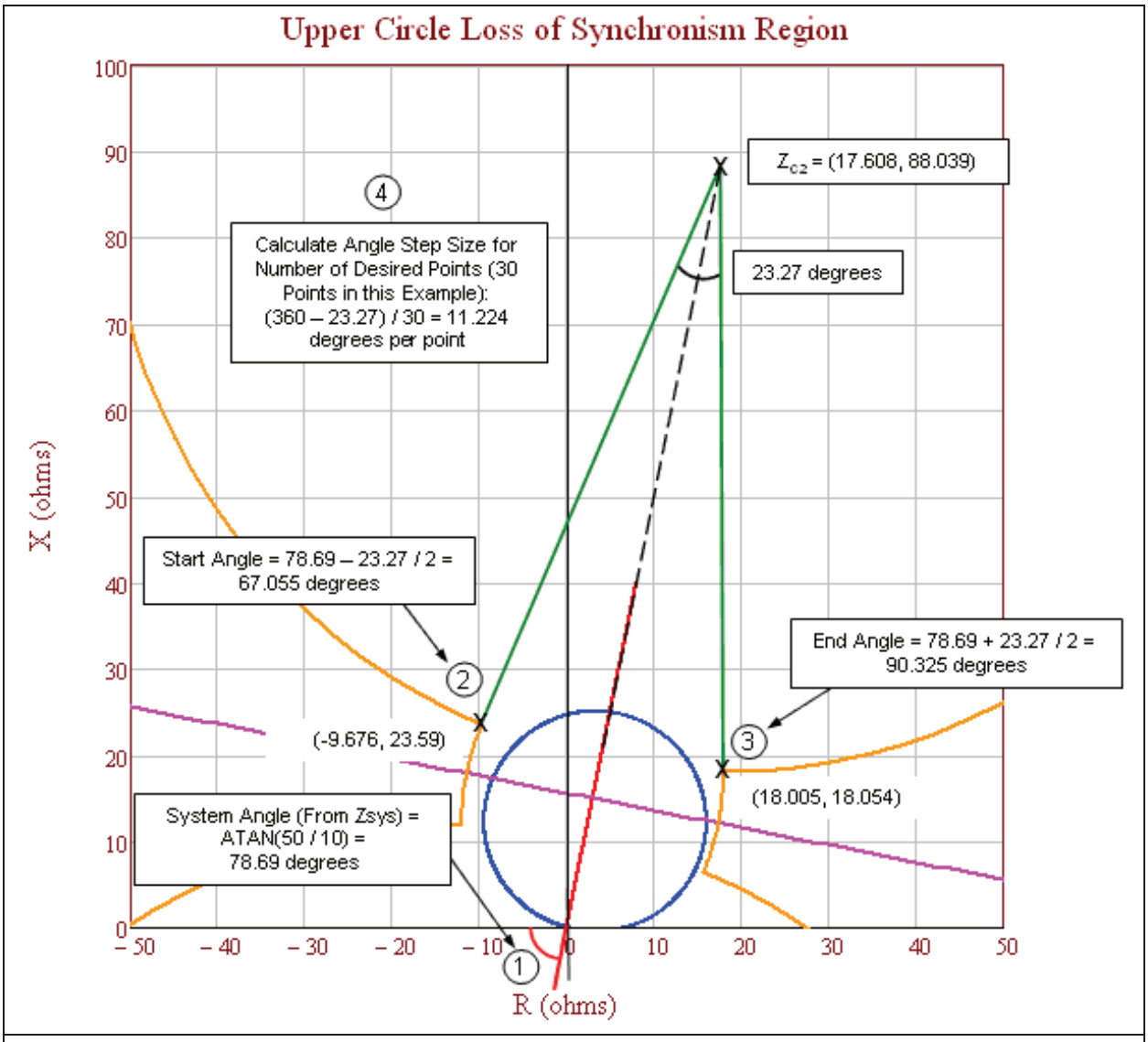


Figure 15g: Upper circle loss-of-synchronism region showing the steps to calculate the start angle, end angle, and the angle step size for the desired number of calculated points. 1) Calculate the system angle. 2) Calculate the start angle. 3) Calculate the end angle. 4) Calculate the angle step size for the desired number of points.

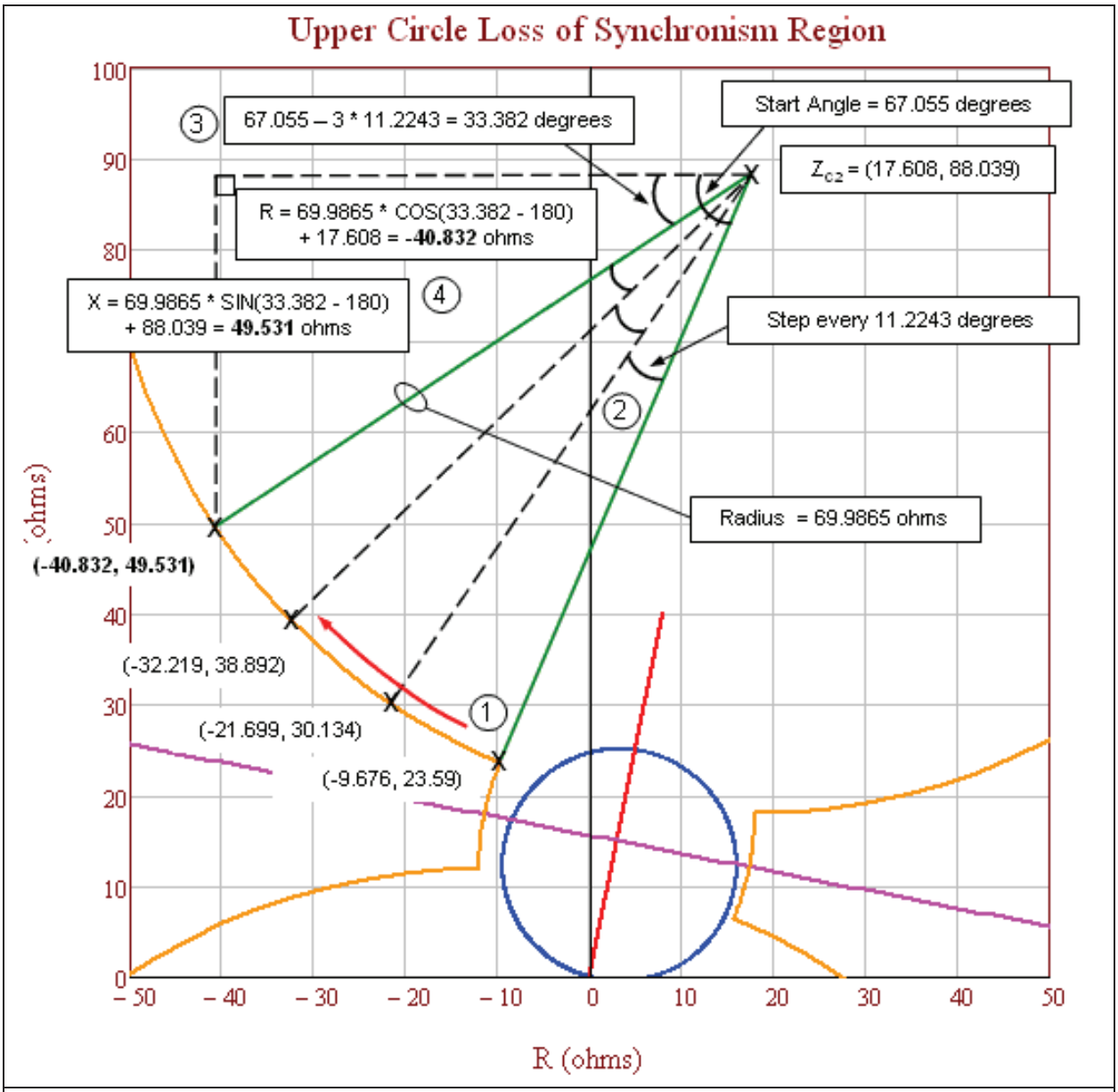


Figure 15h: Upper circle loss-of-synchronism region showing the final steps to calculate the coordinates of the points on the circle. 1) Start at the intersection with the lens shape and proceed in a clockwise direction. 2) Advance the step angle for each point. 3) Calculate the new angle after step advancement. 4) Calculate the R-X coordinates.

Lower Loss of Synchronism Circle Coordinates		
Angle (degrees)	R	+ jX
67.055	15.676	6.41
55.831	27.699	-0.134
44.606	38.219	-8.892
33.382	**46.832**	**-19.531**
22.158	53.21	-31.643
10.933	57.108	-44.765
359.709	58.378	-58.395
348.485	56.97	-72.011
337.26	52.939	-85.092
326.036	46.438	-97.139
314.812	37.717	-107.69
303.587	27.109	-116.341
292.363	15.02	-122.762
281.139	1.913	-126.707
269.914	-11.712	-128.026
258.69	-25.333	-126.667
247.466	-38.429	-122.682
236.241	-50.499	-116.225
225.017	-61.081	-107.542
213.793	-69.771	-96.965
202.568	-76.235	-84.899
191.344	-80.227	-71.806
180.12	-81.594	-58.185
168.895	-80.284	-44.56
157.671	-76.347	-31.45
146.447	-69.933	-19.357
135.222	-61.288	-8.744
123.998	-50.742	-0.016
112.774	-38.699	6.491
101.549	-25.62	10.53
90.325	-12.005	11.946

Upper Loss of Synchronism Circle Coordinates		
Angle (degrees)	R	+ jX
67.055	-9.676	23.59
55.831	-21.699	30.134
44.606	-32.219	38.892
33.382	**-40.832**	**49.531**
22.158	-47.21	61.643
10.933	-51.108	74.765
359.709	-52.378	88.395
348.485	-50.97	102.011
337.26	-46.939	115.092
326.036	-40.438	127.139
314.812	-31.717	137.69
303.587	-21.109	146.341
292.363	-9.02	152.762
281.139	4.087	156.707
269.914	17.712	158.026
258.69	31.333	156.667
247.466	44.429	152.682
236.241	56.499	146.225
225.017	67.081	137.542
213.793	75.771	126.965
202.568	82.235	114.899
191.344	86.227	101.806
180.12	87.594	88.185
168.895	86.284	74.56
157.671	82.347	61.45
146.447	75.933	49.357
135.222	67.288	38.744
123.998	56.742	30.016
112.774	44.699	23.509
101.549	31.62	19.47
90.325	18.005	18.054

Figure 15i: Full tables of calculated lower and upper loss-of-synchronism circle coordinates. The highlighted row is the detailed calculated points in Figures 15d and 15h.

Application Specific to Criterion B

The PRC-026-1 – Attachment B, Criterion B evaluates overcurrent elements used for tripping. The same criteria as PRC-026-1 – Attachment B, Criterion A is used except for an additional criterion (No. 4) that calculates a current magnitude based upon generator internal voltage of 1.05 per unit. A value of 1.05 per unit generator voltage is used to establish a minimum pickup current value for overcurrent relays that have a time delay less than 15 cycles. The sending-end and receiving-end voltages are established at 1.05 per unit at 120 degree system separation angle. The 1.05 per unit is the typical upper end of the operating voltage, which is also consistent with the maximum power

transfer calculation using actual system source impedances in the PRC-023 NERC Reliability Standard. The formulas used to calculate the current are in Table 14 below.

Table 14: Example Calculation (Overcurrent)

This example is for a 230 kV line terminal with a directional instantaneous phase overcurrent element set to 50 amps secondary times a CT ratio of 160:1 that equals 8,000 amps, primary. The following calculation is where V_S equals the base line-to-ground sending-end generator source voltage times 1.05 at an angle of 120 degrees, V_R equals the base line-to-ground receiving-end generator internal voltage times 1.05 at an angle of 0 degrees, and Z_{sys} equals the sum of the sending-end source, line, and receiving-end source impedances in ohms. Here, the instantaneous phase setting of 8,000 amps is greater than the calculated system current of 5,716 amps; therefore, it meets PRC-026-1 – Attachment B, Criterion B.			
Eq. (102)	$V_S = \frac{V_{LL}\angle 120°}{\sqrt{3}} \times 1.05$		
	$V_S = \frac{230{,}000\angle 120°\ V}{\sqrt{3}} \times 1.05$		
	$V_S = 139{,}430\angle 120°\ V$		
Receiving-end generator terminal voltage.			
Eq. (103)	$V_R = \frac{V_{LL}\angle 0°}{\sqrt{3}} \times 1.05$		
	$V_R = \frac{230{,}000\angle 0°\ V}{\sqrt{3}} \times 1.05$		
	$V_R = 139{,}430\angle 0°\ V$		
The total impedance of the system (Z_{sys}) equals the sum of the sending-end source impedance (Z_S), the impedance of the line (Z_L), and receiving-end impedance (Z_R) in ohms.			
Given:	$Z_S = 3 + j26\ \Omega$	$Z_L = 1.3 + j8.7\ \Omega$	$Z_R = 0.3 + j7.3\ \Omega$
Eq. (104)	$Z_{sys} = Z_S + Z_L + Z_R$		
	$Z_{sys} = (3 + j26)\ \Omega + (1.3 + j8.7)\ \Omega + (0.3 + j7.3)\ \Omega$		
	$Z_{sys} = 4.6 + j42\ \Omega$		
Total system current.			
Eq. (105)	$I_{sys} = \frac{(V_S - V_R)}{Z_{sys}}$		
	$I_{sys} = \frac{(139{,}430\angle 120°\ V - 139{,}430\angle 0°\ V)}{(4.6 + j42)\ \Omega}$		
	$I_{sys} = 5{,}715.82\angle 66.25°\ A$		

Application Specific to Three-Terminal Lines

If a three-terminal line is identified as an Element that is susceptible to a power swing based on Requirement R1, the load-responsive protective relays at each end of the three-terminal line must be evaluated.

As shown in Figure 15j, the source impedances at each end of the line can be obtained from the similar short circuit calculation as for the two-terminal line (assuming the parallel transfer impedances are ignored).

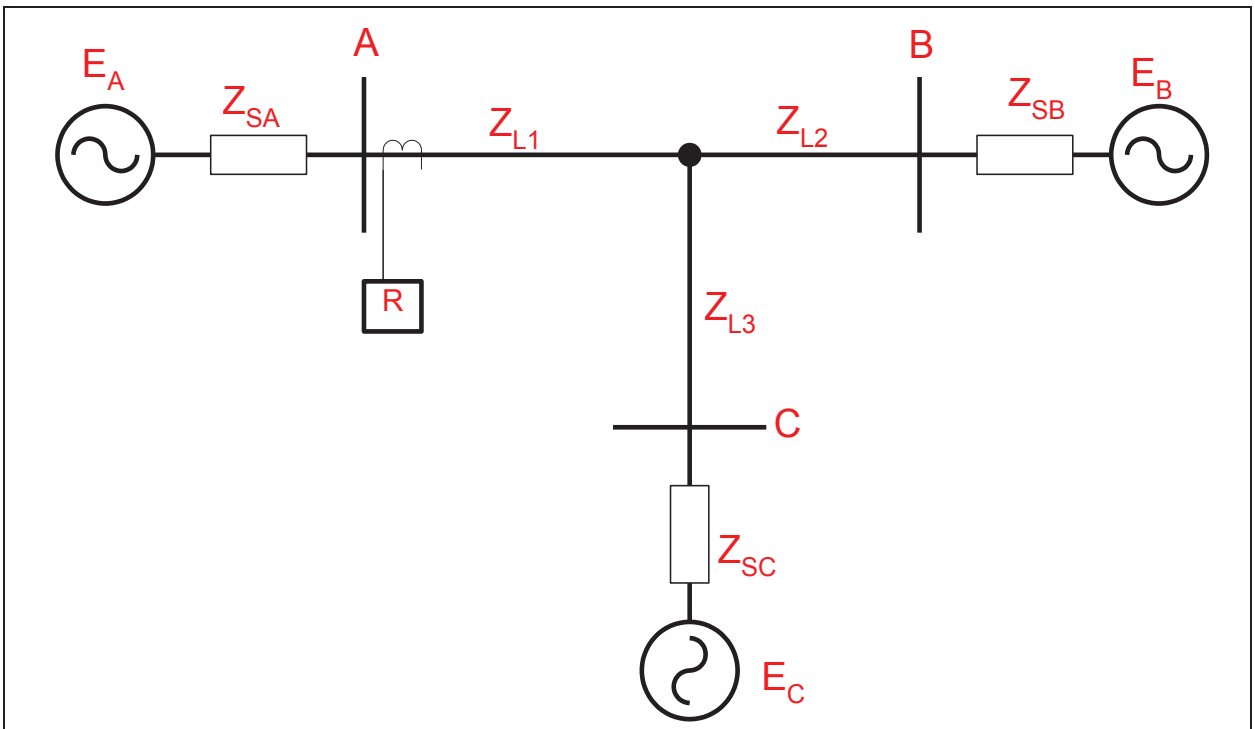


Figure 15j: Three-terminal line. To evaluate the load-responsive protective relays on the three-terminal line at Terminal A, the circuit in Figure 15j is first reduced to the equivalent circuit shown in Figure 15k. The evaluation process for the load-responsive protective relays on the line at Terminal A will now be the same as that of the two-terminal line.

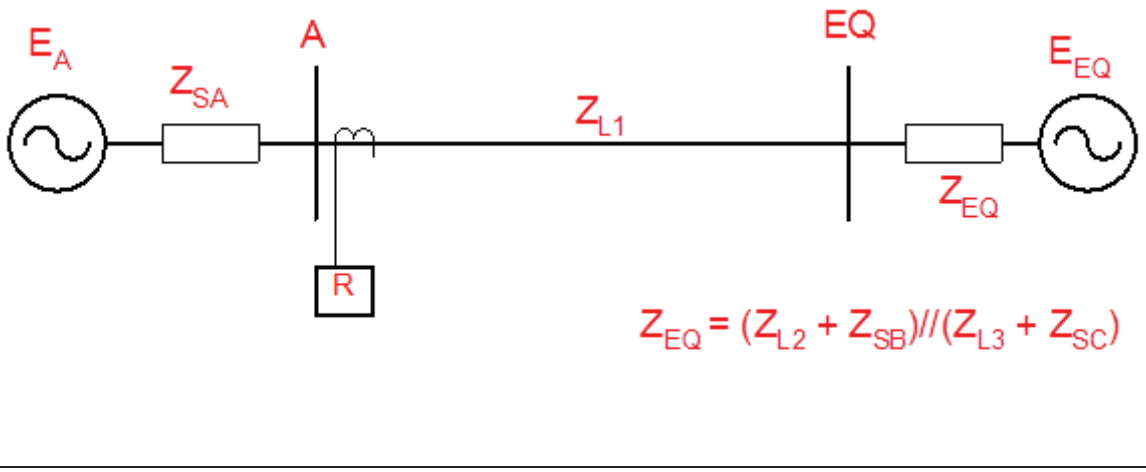


Figure 15k: Three-terminal line reduced to a two-terminal line.

Application to Generation Elements

As with transmission BES Elements, the determination of the apparent impedance seen at an Element located at, or near, a generation Facility is complex for power swings due to various interdependent quantities. These variances in quantities are caused by changes in machine internal voltage, speed governor action, voltage regulator action, the reaction of other local generators, and the reaction of other interconnected transmission BES Elements as the event progresses through the time domain. Though transient stability simulations may be used to determine the apparent impedance for verifying load-responsive relay settings,[19,20] Requirement R2, PRC-026-1 – Attachment B, Criteria A and B provides a simplified method for evaluating the load-responsive protective relay's susceptibility to tripping in response to a stable power swing without requiring stability simulations.

In general, the electrical center will be in the transmission system for cases where the generator is connected through a weak transmission system (high external impedance). In other cases where the generator is connected through a strong transmission system, the electrical center could be inside the unit connected zone.[21] In either case, load-responsive protective relays connected at the generator terminals or at the high-voltage side of the generator step-up (GSU) transformer may be challenged by power swings. Relays that may be challenged by power swings will be determined by the Planning Coordinator in Requirement R1 or by the Generator Owner after becoming aware of a generator, transformer, or transmission line BES Element that tripped[22] in response to a stable or unstable power swing due to the operation of its protective relay(s) in Requirement R2.

[19] Donald Reimert, *Protective Relaying for Power Generation Systems*, Boca Raton, FL, CRC Press, 2006.

[20] Prabha Kundur, *Power System Stability and Control*, EPRI, McGraw Hill, Inc., 1994.

[21] Ibid, Kundur.

[22] See Guidelines and Technical Basis section, "Becoming Aware of an Element That Tripped in Response to a Power Swing,"

Voltage controlled time-overcurrent and voltage-restrained time-overcurrent relays are excluded from this standard. When these relays are set based on equipment permissible overload capability, their operating times are much greater than 15 cycles for the current levels observed during a power swing.

Instantaneous overcurrent, time-overcurrent, and definite-time overcurrent relays with a time delay of less than 15 cycles for the current levels observed during a power swing are applicable and are required to be evaluated for identified Elements.

The generator loss-of-field protective function is provided by impedance relay(s) connected at the generator terminals. The settings are applied to protect the generator from a partial or complete loss of excitation under all generator loading conditions and, at the same time, be immune to tripping on stable power swings. It is more likely that the loss-of-field relay would operate during a power swing when the automatic voltage regulator (AVR) is in manual mode rather than when in automatic mode.[23] Figure 16 illustrates the loss-of-field relay in the R-X plot, which typically includes up to three zones of protection.

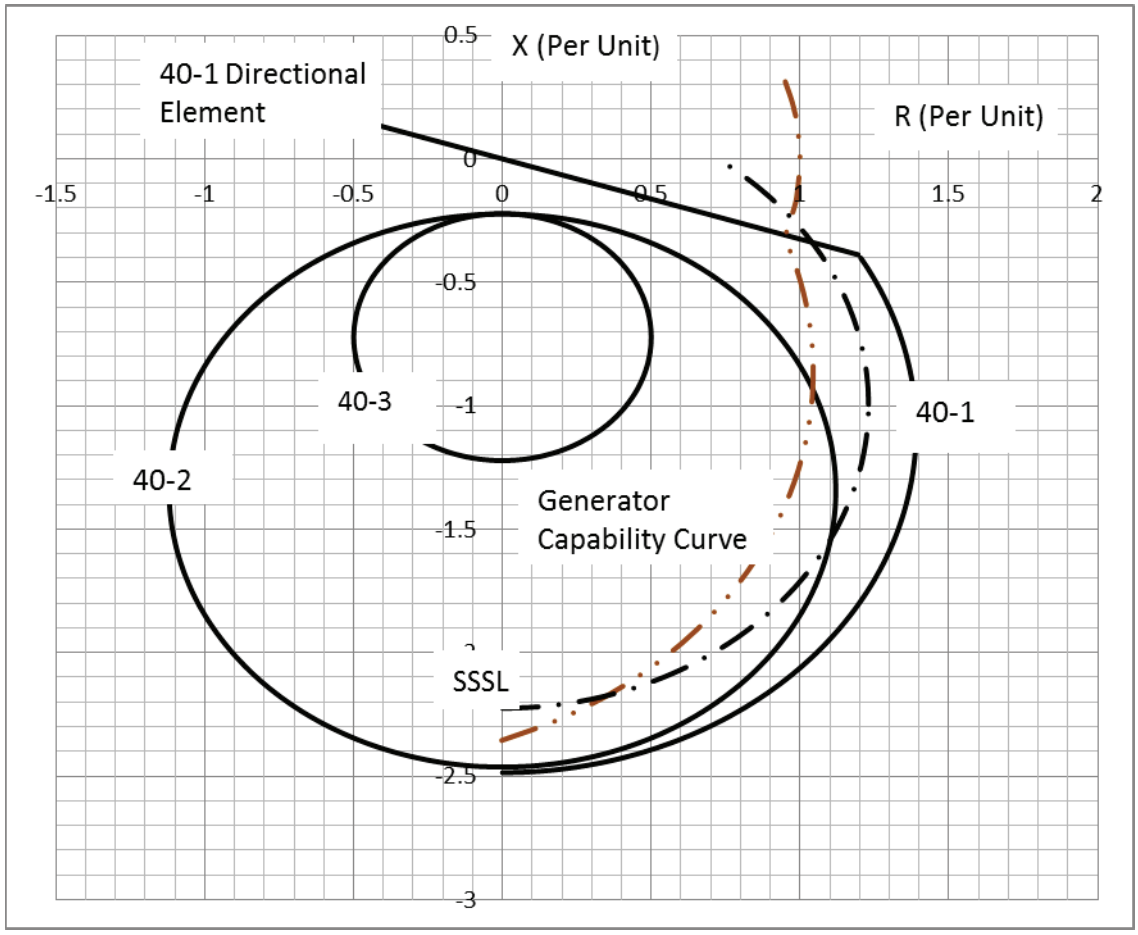


Figure 16: An R-X graph of typical impedance settings for loss-of-field relays.

[23] John Burdy, *Loss-of-excitation Protection for Synchronous Generators GER-3183*, General Electric Company.

Loss-of-field characteristic 40-1 has a wider impedance characteristic (positive offset) than characteristic 40-2 or characteristic 40-3 and provides additional generator protection for a partial loss of field or a loss of field under low load (less than 10% of rated). The tripping logic of this protection scheme is established by a directional contact, a voltage setpoint, and a time delay. The voltage and time delay add security to the relay operation for stable power swings. Characteristic 40-3 is less sensitive to power swings than characteristic 40-2 and is set outside the generator capability curve in the leading direction. Regardless of the relay impedance setting, PRC-019[24] requires that the "in-service limiters operate before Protection Systems to avoid unnecessary trip" and "in-service Protection System devices are set to isolate or de-energize equipment in order to limit the extent of damage when operating conditions exceed equipment capabilities or stability limits." Time delays for tripping associated with loss-of-field relays[25,26] have a range from 15 cycles for characteristic 40-2 to 60 cycles for characteristic 40-1 to minimize tripping during stable power swings. In PRC-026-1, 15 cycles establishes a threshold for applicability; however, it is the responsibility of the Generator Owner to establish settings that provide security against stable power swings and, at the same time, dependable protection for the generator.

The simple two-machine system circuit (method also used in the Application to Transmission Elements section) is used to analyze the effect of a power swing at a generator facility for load-responsive relays. In this section, the calculation method is used for calculating the impedance seen by the relay connected at a point in the circuit.[27] The electrical quantities used to determine the apparent impedance plot using this method are generator saturated transient reactance (X'_d), GSU transformer impedance (X_{GSU}), transmission line impedance (Z_L), and the system equivalent (Z_e) at the point of interconnection. All impedance values are known to the Generator Owner except for the system equivalent. The system equivalent is obtainable from the Transmission Owner. The sending-end and receiving-end source voltages are varied from 0.0 to 1.0 per unit to form the lens shape portion of the unstable power swing region. The voltage range of 0.7 to 1.0 results in a ratio range from 0.7 to 1.43. This ratio range is used to form the lower and upper loss-of-synchronism circle shapes of the unstable power swing region. A system separation angle of 120 degrees is used in accordance with PRC-026-1 – Attachment B criteria for each load-responsive protective relay evaluation.

Table 15 below is an example calculation of the apparent impedance locus method based on Figures 17 and 18.[28] In this example, the generator is connected to the 345 kV transmission system through the GSU transformer and has the listed ratings. Note that the load-responsive protective relays in this example may have ownership with the Generator Owner or the Transmission Owner.

---

[24] Coordination of Generating Unit or Plant Capabilities, Voltage Regulating Controls, and Protection

[25] Ibid, Burdy.

[26] *Applied Protective Relaying*, Westinghouse Electric Corporation, 1979.

[27] Edward Wilson Kimbark, *Power System Stability, Volume II: Power Circuit Breakers and Protective Relays*, Published by John Wiley and Sons, 1950.

[28] Ibid, Kimbark.

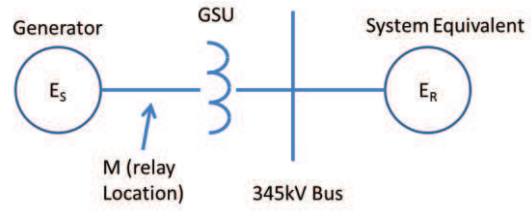


Figure 17: Simple one-line diagram of the system to be evaluated.

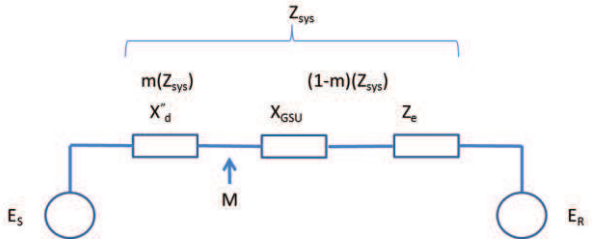


Figure 18: Simple system equivalent impedance diagram to be evaluated.[29]

Table15: Example Data (Generator)	
Input Descriptions	**Input Values**
Synchronous Generator nameplate (MVA)	940 MVA
Saturated transient reactance (940 MVA base)	$X'_d = 0.3845$ per unit
Generator rated voltage (Line-to-Line)	20 kV
Generator step-up (GSU) transformer rating	880 MVA
GSU transformer reactance (880 MVA base)	$X_{GSU} = 16.05\%$
System Equivalent (100 MVA base)	$Z_e = 0.00723\angle 90°$ per unit
Generator Owner Load-Responsive Protective Relays	
40-1	Positive Offset Impedance
	Offset = 0.294 per unit
	Diameter = 0.294 per unit
40-2	Negative Offset Impedance
	Offset = 0.22 per unit
	Diameter = 2.24 per unit
40-3	Negative Offset Impedance
	Offset = 0.22 per unit
	Diameter = 1.00 per unit
21-1	Diameter = 0.643 per unit
	MTA = 85°

[29] Ibid, Kimbark.

Table15: Example Data (Generator)	
50	I (pickup) = 5.0 per unit
Transmission Owned Load-Responsive Protective Relays	
21-2	Diameter = 0.55 per unit
	MTA = 85°

Calculations shown for a 120 degree angle and $E_S/E_R = 1$. The equation for calculating Z_R is:[30]

Eq. (106) $$Z_R = \left(\frac{(1-m)(E_S\angle\delta) + (m)(E_R)}{E_S\angle\delta - E_R}\right) \times Z_{sys}$$

Where m is the relay location as a function of the total impedance (real number less than 1)

E_S and E_R is the sending-end and receiving-end voltages

Z_{sys} is the total system impedance

Z_R is the complex impedance at the relay location and plotted on an R-X diagram

All of the above are constants (940 MVA base) while the angle δ is varied. Table 16 below contains calculations for a generator using the data listed in Table 15.

Table16: Example Calculations (Generator)			
The following calculations are on a 940 MVA base.			
Given:	$X'_d = j0.3845\ pu$	$X_{GSU} = j0.17144\ pu$	$Z_e = j0.06796\ pu$
Eq. (107)	$Z_{sys} = X'_d + X_{GSU} + Z_e$		
	$Z_{sys} = j0.3845\ pu + j0.17144\ pu + j0.06796\ pu$		
	$Z_{sys} = 0.6239\ \angle 90°\ pu$		
Eq. (108)	$m = \frac{X'_d}{Z_{sys}} = \frac{0.3845}{0.6239} = 0.6163$		
Eq. (109)	$Z_R = \left(\frac{(1-m)(E_S\angle\delta) + (m)(E_R)}{E_S\angle\delta - E_R}\right) \times Z_{sys}$		
	$Z_R = \left(\frac{(1-0.6163) \times (1\angle 120°) + (0.6163)(1\angle 0°)}{1\angle 120° - 1\angle 0°}\right) \times (0.6239\angle 90°)\ pu$		

[30] Ibid, Kimbark.

Table16: Example Calculations (Generator)	
	$Z_R = \left(\frac{0.4244 + j0.3323}{-1.5 + j\ 0.866}\right) \times (0.6239\angle 90°)\ pu$
	$Z_R = (0.3116 \angle -111.95°) \times (0.6239\angle 90°)\ pu$
	$Z_R = 0.194 \angle -21.95°\ pu$
	$Z_R = -0.18 - j0.073\ pu$

Table 17 lists the swing impedance values at other angles and at E_S/E_R = 1, 1.43, and 0.7. The impedance values are plotted on an R-X graph with the center being at the generator terminals for use in evaluating impedance relay settings.

Table 17: Sample Calculations for a Swing Impedance Chart for Varying Voltages at the Sending-End and Receiving-End.

	E_S/E_R=1		E_S/E_R=1.43		E_S/E_R=0.7	
	Z_R		Z_R		Z_R	
Angle (δ) (Degrees)	Magnitude (pu)	Angle (Degrees)	Magnitude (pu)	Angle (Degrees)	Magnitude (pu)	Angle (Degrees)
90	0.320	-13.1	0.296	6.3	0.344	-31.5
120	0.194	-21.9	0.173	-0.4	0.227	-40.1
150	0.111	-41.0	0.082	-10.3	0.154	-58.4
210	0.111	-25.9	0.082	190.3	0.154	238.4
240	0.194	201.9	0.173	180.4	0.225	220.1
270	0.320	193.1	0.296	173.7	0.344	211.5

Requirement R2 Generator Examples

Distance Relay Application

Based on PRC-026-1 – Attachment B, Criterion A, the distance relay (21-1) (i.e., owned by the Generation Owner) characteristic is in the region where a stable power swing would not occur as shown in Figure 19. There is no further obligation to the owner in this standard for this load-responsive protective relay.

The distance relay (21-2) (i.e., owned by the Transmission Owner) is connected at the high-voltage side of the GSU transformer and its impedance characteristic is in the region where a stable power swing could occur causing the relay to operate. In this example, if the intentional time delay of this relay is less than 15 cycles, the PRC-026 – Attachment B, Criterion A cannot be met, thus the Transmission Owner is required to create a CAP (Requirement R3). Some of the options include,

but are not limited to, changing the relay setting (i.e., impedance reach, angle, time delay), modify the scheme (i.e., add PSB), or replace the Protection System. Note that the relay may be excluded from this standard if it has an intentional time delay equal to or greater than 15 cycles.

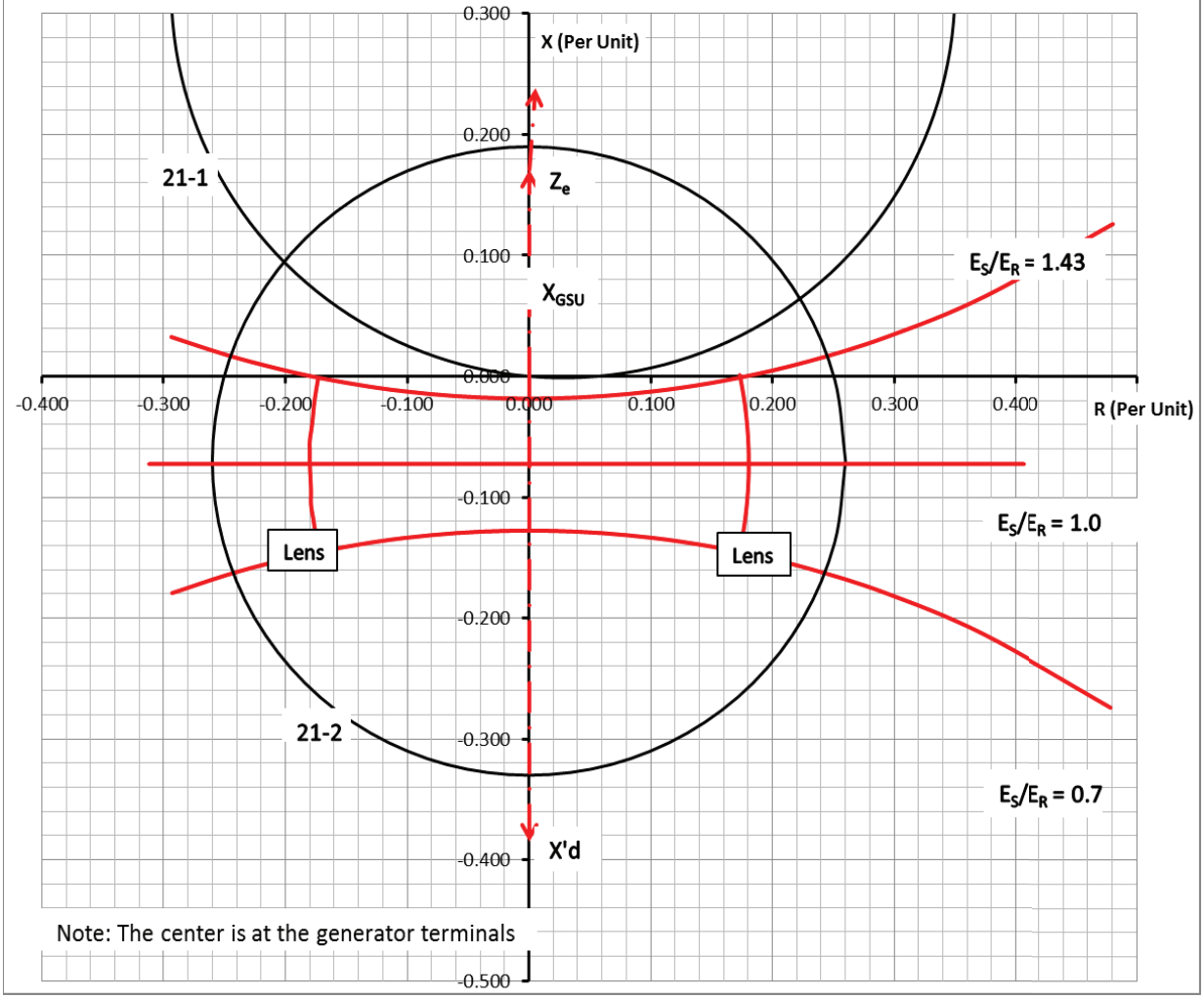


Figure 19: Swing impedance graph for impedance relays at a generating facility.

Loss-of-Field Relay Application

In Figure 20, the R-X diagram shows the loss-of-field relay (40-1 and 40-2) characteristics are in the region where a stable power swing can cause a relay operation. Protective relay 40-1 would be excluded if it has an intentional time delay equal to or greater than 15 cycles. Similarly, 40-2 would be excluded if its intentional time delay is equal to or greater than 15 cycles. For example, if 40-1 has a time delay of 1 second and 40-2 has a time delay of 0.25 seconds, they are excluded and there is no further obligation on the Generator Owner in this standard for these relays. The

loss-of-field relay characteristic 40-3 is entirely inside the unstable power swing region. In this case, the owner may select high speed tripping on operation of the 40-3 impedance element.

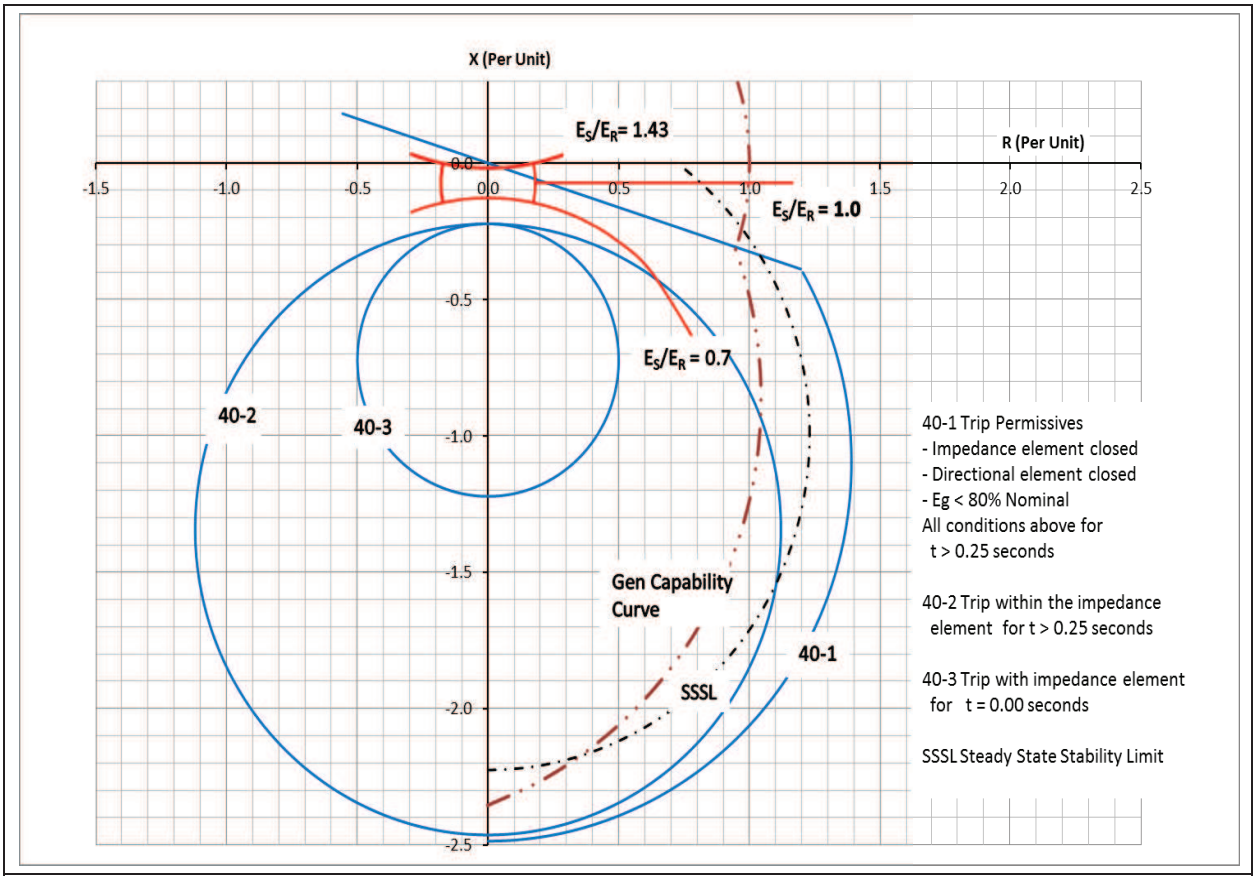


Figure 20: Typical R-X graph for loss-of-field relays with a portion of the unstable power swing region defined by PRC-026-1 – Attachment B, Criterion A.

Instantaneous Overcurrent Relay

In similar fashion to the transmission line overcurrent example calculation in Table 14, the instantaneous overcurrent relay minimum setting is established by PRC-026-1 – Attachment B, Criterion B. The solution is found by:

Eq. (110) $$I_{sys} = \frac{E_S - E_R}{Z_{\text{sys}}}$$

As stated in the relay settings in Table 15, the relay is installed on the high-voltage side of the GSU transformer with a pickup of 5.0 per unit. The maximum allowable current is calculated below.

$$I_{sys} = \frac{(1.05\angle 120° - 1.05\angle 0°)}{0.6239\angle 90°}\ pu$$

$$I_{sys} = \frac{1.819\angle 150°}{0.6239\angle 90°} pu$$

$$I_{sys} = 2.91\ \angle 60°\ pu$$

The instantaneous phase setting of 5.0 per unit is greater than the calculated system current of 2.91 per unit; therefore, it meets the PRC-026-1 – Attachment B, Criterion B.

Out-of-Step Tripping for Generation Facilities

Out-of-step protection for the generator generally falls into three different schemes. The first scheme is a distance relay connected at the high-voltage side of the GSU transformer with the directional element looking toward the generator. Because this relay setting may be the same setting used for generator backup protection (see Requirement R2 Generator Examples, Distance Relay Application), it is susceptible to tripping in response to stable power swings and would require modification. Because this scheme is susceptible to tripping in response to stable power swings and any modification to the mho circle will jeopardize the overall protection of the out-of-step protection of the generator, available technical literature does not recommend using this scheme specifically for generator out-of-step protection. The second and third out-of-step Protection System schemes are commonly referred to as single and double blinder schemes. These schemes are installed or enabled for out-of-step protection using a combination of blinders, a mho element, and timers. The combination of these protective relay functions provides out-of-step protection and discrimination logic for stable and unstable power swings. Single blinder schemes use logic that discriminate between stable and unstable power swings by issuing a trip command after the first slip cycle. Double blinder schemes are more complex than the single blinder scheme and, depending on the settings of the inner blinder, a trip for a stable power swing may occur. While the logic discriminates between stable and unstable power swings in either scheme, it is important that the trip initiating blinders be set at an angle greater than the stability limit of 120 degrees to remove the possibility of a trip for a stable power swing. Below is a discussion of the double blinder scheme.

Double Blinder Scheme

The double blinder scheme is a method for measuring the rate of change of positive sequence impedance for out-of-step swing detection. The scheme compares a timer setting to the actual elapsed time required by the impedance locus to pass between two impedance characteristics. In this case, the two impedance characteristics are simple blinders, each set to a specific resistive reach on the R-X plane. Typically, the two blinders on the left half plane are the mirror images of those on the right half plane. The scheme typically includes a mho characteristic which acts as a starting element, but is not a tripping element.

The scheme detects the blinder crossings and time delays as represented on the R-X plane as shown in Figure 21. The system impedance is composed of the generator transient (X_d'), GSU transformer ($X_{T)}$, and transmission system (X_{system}), impedances.

The scheme logic is initiated when the swing locus crosses the outer Blinder R1 (Figure 21), on the right at separation angle α. The scheme only commits to take action when a swing crosses the

inner blinder. At this point the scheme logic seals in the out-of-step trip logic at separation angle β. Tripping actually asserts as the impedance locus leaves the scheme characteristic at separation angle δ.

The power swing may leave both inner and outer blinders in either direction, and tripping will assert. Therefore, the inner blinder must be set such that the separation angle β is large enough that the system cannot recover. This angle should be set at 120 degrees or more. Setting the angle greater than 120 degrees satisfies the PRC-026-1 – Attachment B, Criterion A (No. 1, 1st bullet) since the tripping function is asserted by the blinder element. Transient stability studies may indicate that a smaller stability limit angle is acceptable under PRC-026-1 – Attachment B, Criterion A (No. 1, 2nd bullet). In this respect, the double blinder scheme is similar to the double lens and triple lens schemes and many transmission application out-of-step schemes.

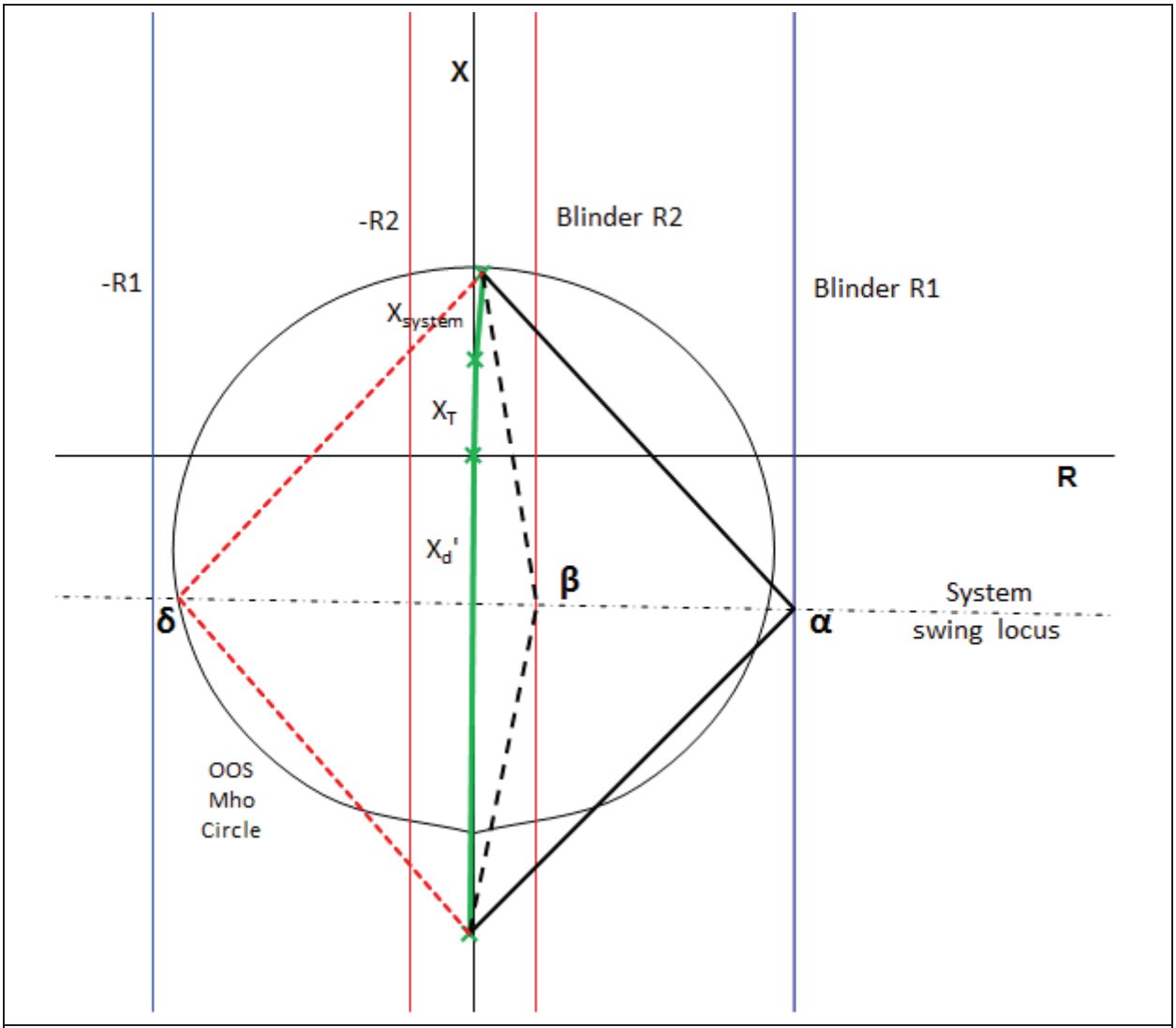


Figure 21: Double Blinder Scheme generic out of step characteristics.

Figure 22 illustrates a sample setting of the double blinder scheme for the example 940 MVA generator. The only setting requirement for this relay scheme is the right inner blinder, which must be set greater than the separation angle of 120 degrees (or a lesser angle based on a transient stability study) to ensure that the out-of-step protective function is expected to not trip in response to a stable power swing during non-Fault conditions. Other settings such as the mho characteristic, outer blinders, and timers are set according to transient stability studies and are not a part of this standard.

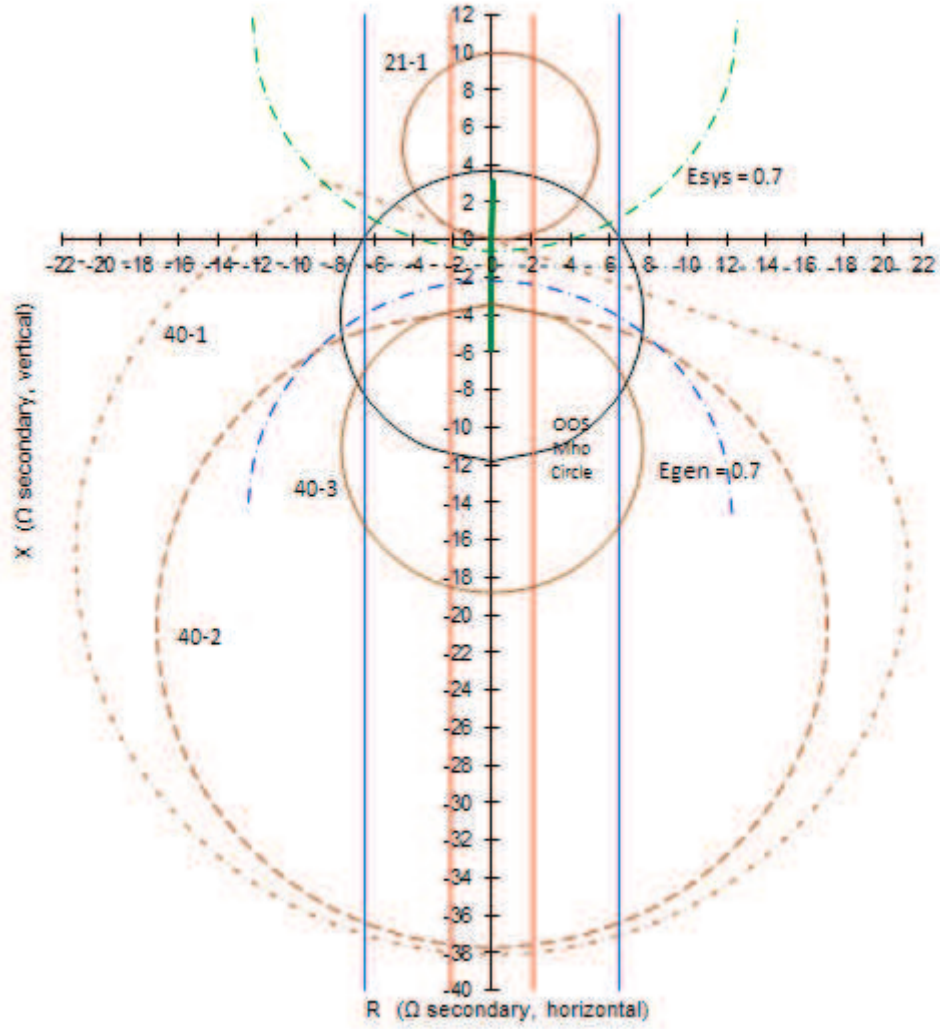


Figure 22: Double Blinder Out-of-Step Scheme with unit impedance data and load-responsive protective relay impedance characteristics for the example 940 MVA generator, scaled in relay secondary ohms.

Requirement R3

To achieve the stated purpose of this standard, which is to ensure that relays are expected to not trip in response to stable power swings during non-Fault conditions, this Requirement ensures that the applicable entity develops a Corrective Action Plan (CAP) that reduces the risk of relays tripping in response to a stable power swing during non-Fault conditions that may occur on any applicable BES Element.

Requirement R4

To achieve the stated purpose of this standard, which is to ensure that load-responsive protective relays are expected to not trip in response to stable power swings during non-Fault conditions, the applicable entity is required to implement any CAP developed pursuant to Requirement R3 such that the Protection System will meet PRC-026-1 – Attachment B criteria or can be excluded under the PRC-026-1 – Attachment A criteria (e.g., modifying the Protection System so that relay functions are supervised by power swing blocking or using relay systems that are immune to power swings), while maintaining dependable fault detection and dependable out-of-step tripping (if out-of-step tripping is applied at the terminal of the BES Element). Protection System owners are required in the implementation of a CAP to update it when actions or timetable change, until all actions are complete. Accomplishing this objective is intended to reduce the occurrence of Protection System tripping during a stable power swing, thereby improving reliability and minimizing risk to the BES.

The following are examples of actions taken to complete CAPs for a relay that did not meet PRC-026-1 – Attachment B and could be at-risk of tripping in response to a stable power swing during non-Fault conditions. A Protection System change was determined to be acceptable (without diminishing the ability of the relay to protect for faults within its zone of protection).

> **Example R4a:** Actions: Settings were issued on 6/02/2015 to reduce the Zone 2 reach of the impedance relay used in the directional comparison unblocking (DCUB) scheme from 30 ohms to 25 ohms so that the relay characteristic is completely contained within the lens characteristic identified by the criterion. The settings were applied to the relay on 6/25/2015. CAP was completed on 06/25/2015.
>
> **Example R4b:** Actions: Settings were issued on 6/02/2015 to enable out-of-step blocking on the existing microprocessor-based relay to prevent tripping in response to stable power swings. The setting changes were applied to the relay on 6/25/2015. CAP was completed on 06/25/2015.

The following is an example of actions taken to complete a CAP for a relay responding to a stable power swing that required the addition of an electromechanical power swing blocking relay.

> **Example R4c:** Actions: A project for the addition of an electromechanical power swing blocking relay to supervise the Zone 2 impedance relay was initiated on 6/5/2015 to prevent tripping in response to stable power swings. The relay installation was completed on 9/25/2015. CAP was completed on 9/25/2015.

The following is an example of actions taken to complete a CAP with a timetable that required updating for the replacement of the relay.

> **Example R4d:** Actions: A project for the replacement of the impedance relays at both terminals of line X with line current differential relays was initiated on 6/5/2015 to prevent tripping in response to stable power swings. The completion of the project was postponed due to line outage rescheduling from 11/15/2015 to 3/15/2016. Following the timetable change, the impedance relay replacement was completed on 3/18/2016. CAP was completed on 3/18/2016.

The CAP is complete when all the documented actions to remedy the specific problem (i.e., unnecessary tripping during stable power swings) are completed.

Justification for Including Unstable Power Swings in the Requirements

Protection Systems that are applicable to the Standard and must be secure for a stable power swing condition (i.e., meets PRC-026-1 – Attachment B criteria) are identified based on Elements that are susceptible to both stable and unstable power swings. This section provides an example of why Elements that trip in response to unstable power swings (in addition to stable power swings) are identified and that their load-responsive protective relays need to be evaluated under PRC-026-1 – Attachment B criteria.

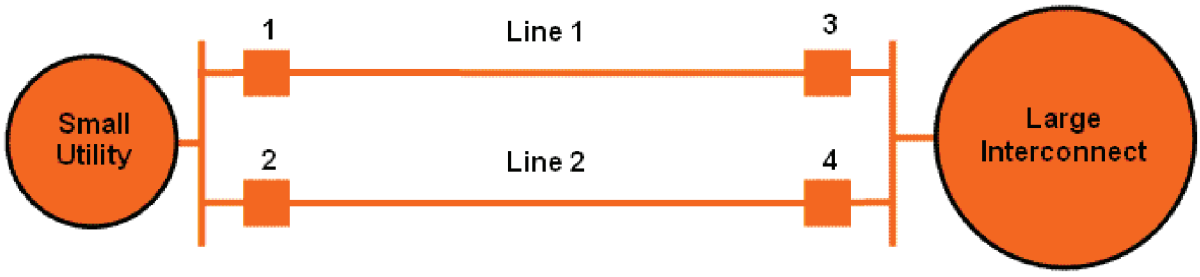


Figure 23: A simple electrical system where two lines tie a small utility to a much larger interconnection.

In Figure 23 the relays at circuit breakers 1, 2, 3, and 4 are equipped with a typical overreaching Zone 2 pilot system, using a Directional Comparison Blocking (DCB) scheme. Internal faults (or power swings) will result in instantaneous tripping of the Zone 2 relays if the measured fault or power swing impedance falls within the zone 2 operating characteristic. These lines will trip on

pilot Zone 2 for out-of-step conditions if the power swing impedance characteristic enters into Zone 2. All breakers are rated for out-of-phase switching.

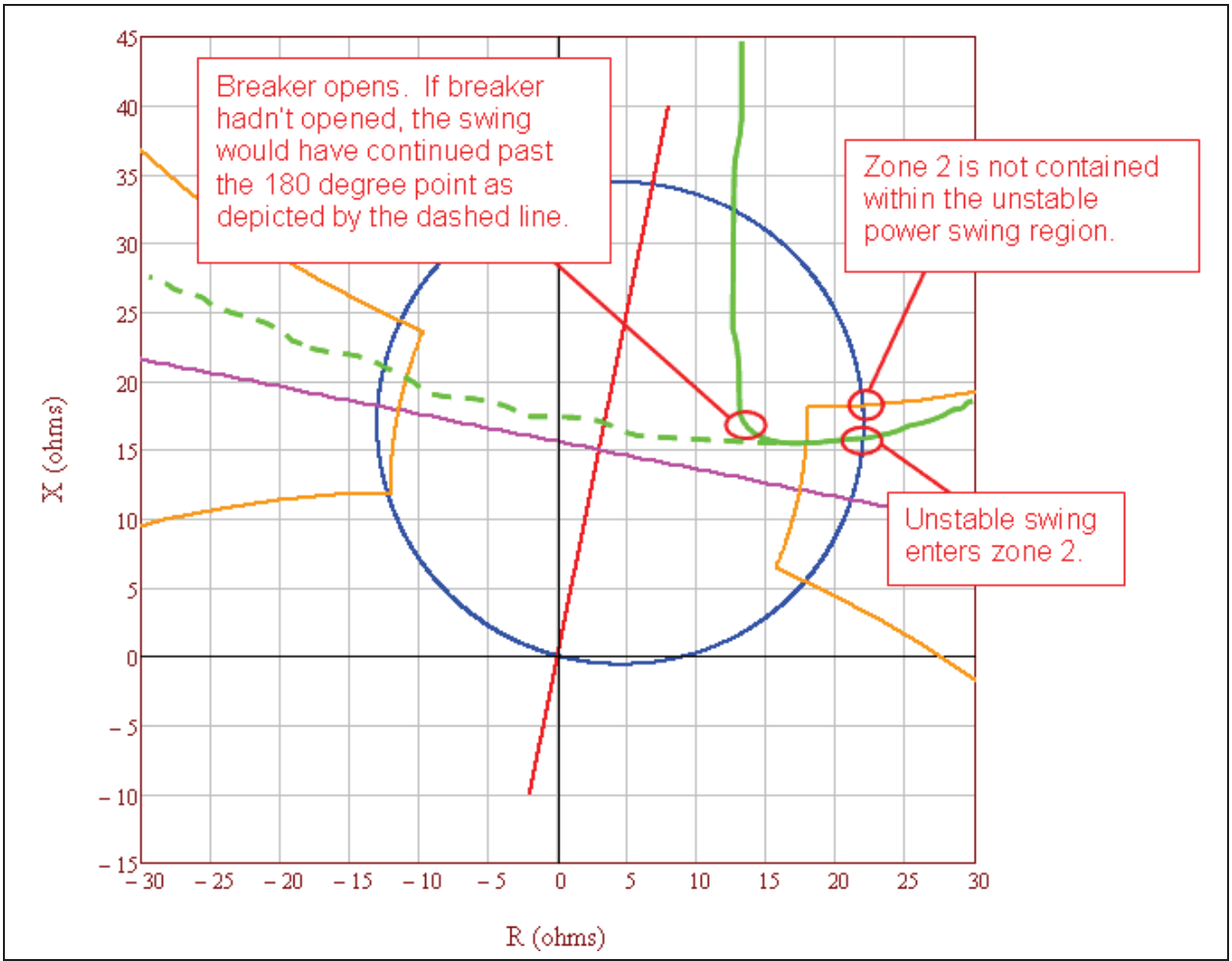


Figure 24: In this case, the Zone 2 element on circuit breakers 1, 2, 3, and 4 did not meet the PRC-026-1 – Attachment B criteria (this figure depicts the power swing as seen by relays on breakers 3 and 4).

In Figure 24, a large disturbance occurs within the small utility and its system goes out-of-step with the large interconnect. The small utility is importing power at the time of the disturbance. The actual power swing, as shown by the solid green line, enters the Zone 2 relay characteristic on the terminals of Lines 1, 2, 3, and 4 causing both lines to trip as shown in Figure 25.

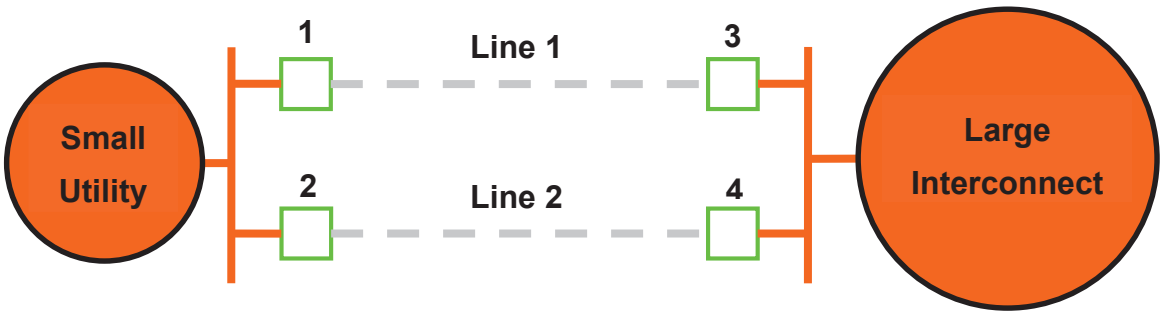


Figure 25: Islanding of the small utility due to Lines 1 and 2 tripping in response to an unstable power swing.

In Figure 25, the relays at circuit breakers 1, 2, 3, and 4 have correctly tripped due to the unstable power swing (shown by the dashed green line in Figure 24), de-energizing Lines 1 and 2, and creating an island between the small utility and the big interconnect. The small utility shed 500 MW of load on underfrequency and maintained a load to generation balance.

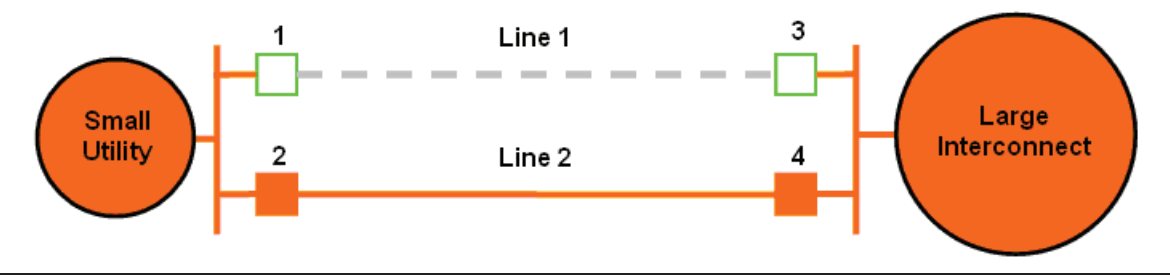


Figure 26: Line 1 is out-of-service for maintenance, Line 2 is loaded beyond its normal rating (but within its emergency rating).

Subsequent to the correct tripping of Lines 1 and 2 for the unstable power swing in Figure 25, another system disturbance occurs while the system is operating with Line 1 out-of-service for maintenance. The disturbance causes a stable power swing on Line 2, which challenges the relays at circuit breakers 2 and 4 as shown in Figure 27.

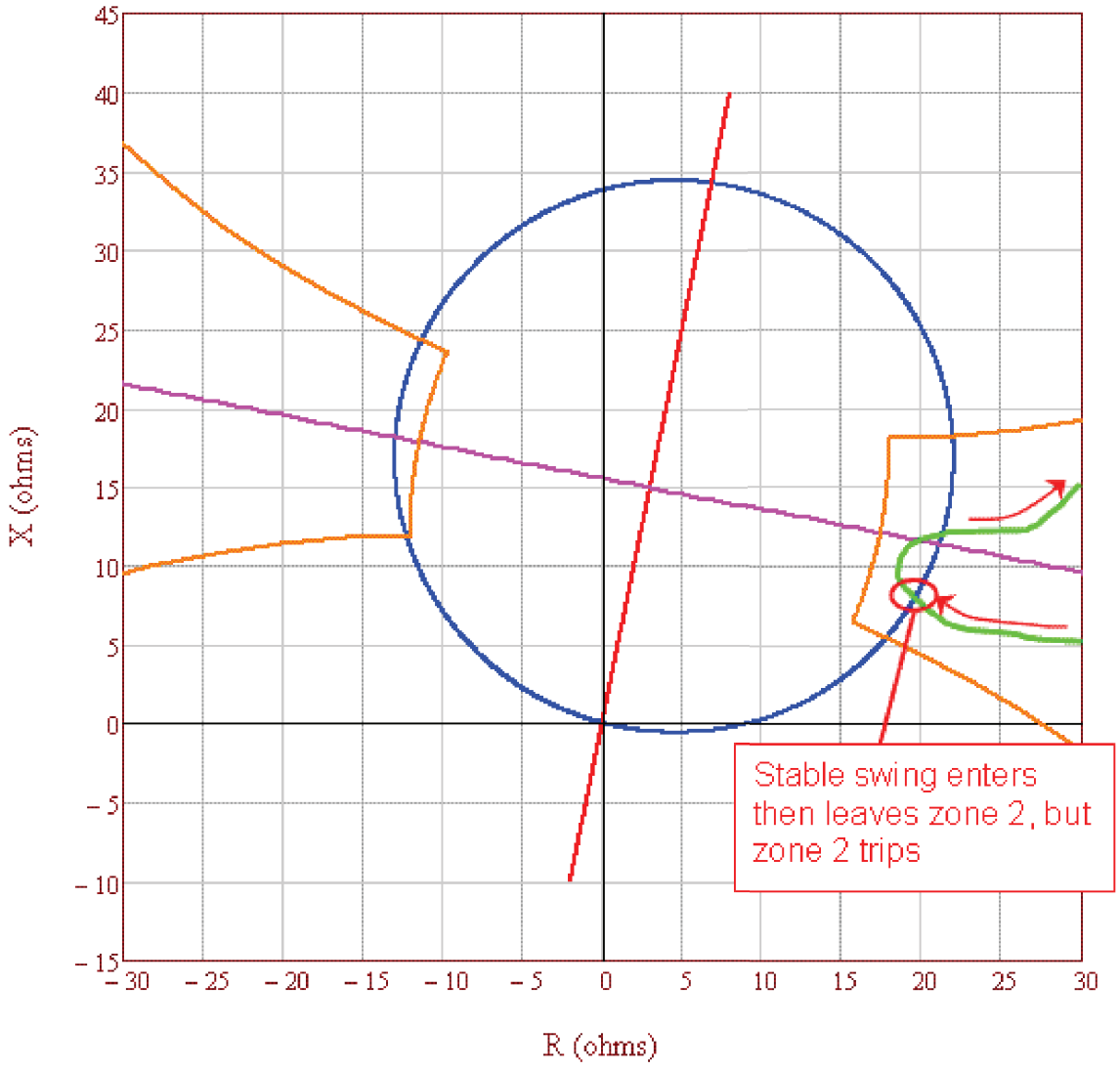


Figure 27: Relays on circuit breakers 2 and 4 were not addressed to meet the PRC-026-1 – Attachment B criteria following the previous unstable power swing event.

If the relays on circuit breakers 2 and 4 were not addressed under the Requirements for the previous unstable power swing condition, the relays would trip in response to the stable power swing, which would result in unnecessary system separation, load shedding, and possibly cascading or blackout.

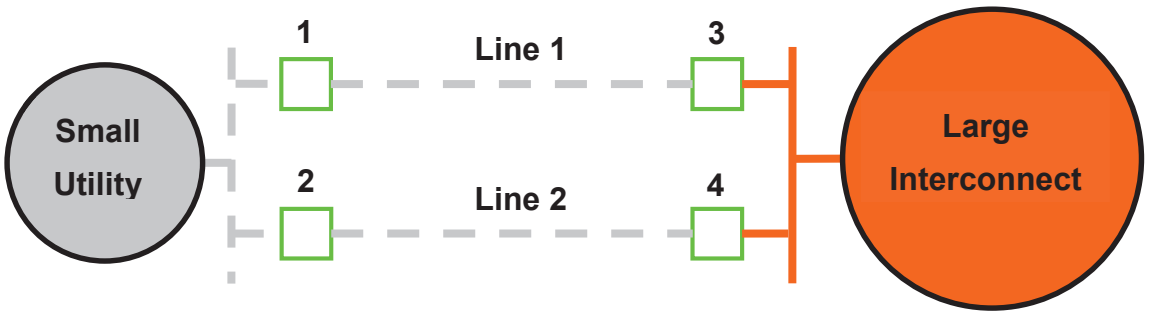


Figure 28: Possible blackout of the small utility.

If the relays that tripped in response to the previous unstable power swing condition in Figure 24 were addressed under the Requirements to meet PRC-026-1 - Attachment B criteria, the unnecessary tripping of the relays for the stable power swing shown in Figure 28 would have been averted, and the possible blackout of the small utility would have been avoided.

Rationale

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for R1

The Planning Coordinator has a wide-area view and is in the position to identify generator, transformer, and transmission line BES Elements which meet the criteria, if any. The criteria-based approach is consistent with the NERC System Protection and Control Subcommittee (SPCS) technical document *Protection System Response to Power Swings*, August 2013 ("PSRPS Report"),[31] which recommends a focused approach to determine an at-risk BES Element. See the Guidelines and Technical Basis for a detailed discussion of the criteria.

Rationale for R2

The Generator Owner and Transmission Owner are in a position to determine whether their load-responsive protective relays meet the PRC-026-1 – Attachment B criteria. Generator, transformer, and transmission line BES Elements are identified by the Planning Coordinator in Requirement R1 and by the Generator Owner and Transmission Owner following an actual event where the Generator Owner and Transmission Owner became aware (i.e., through an event analysis or

[31] NERC System Protection and Control Subcommittee, *Protection System Response to Power Swings*, August 2013: http://www.nerc.com/comm/PC/System%20Protection%20and%20Control%20Subcommittee%20SPCS%2020/SPCS%20Power%20Swing%20Report_Final_20131015.pdf)

Protection System review) tripping was due to a stable or unstable power swing. A period of 12 calendar months allows sufficient time for the entity to conduct the evaluation.

Rationale for R3

To meet the reliability purpose of the standard, a CAP is necessary to ensure the entity's Protection System meets the PRC-026-1 – Attachment B criteria (1st bullet) so that protective relays are expected to not trip in response to stable power swings. A CAP may also be developed to modify the Protection System for exclusion under PRC-026-1 – Attachment A (2nd bullet). Such an exclusion will allow the Protection System to be exempt from the Requirement for future events. The phrase, "…while maintaining dependable fault detection and dependable out-of-step tripping…" in Requirement R3 describes that the entity is to comply with this standard, while achieving their desired protection goals. Refer to the Guidelines and Technical Basis, Introduction, for more information.

Rationale for R4

Implementation of the CAP must accomplish all identified actions to be complete to achieve the desired reliability goal. During the course of implementing a CAP, updates may be necessary for a variety of reasons such as new information, scheduling conflicts, or resource issues. Documenting CAP changes and completion of activities provides measurable progress and confirmation of completion.

Rationale for Attachment B (Criterion A)

The PRC-026-1 – Attachment B, Criterion A provides a basis for determining if the relays are expected to not trip for a stable power swing having a system separation angle of up to 120 degrees with the sending-end and receiving-end voltages varying from 0.7 to 1.0 per unit (See Guidelines and Technical Basis).

Appendix QC-PRC-026-1
Provisions specific to the standard PRC-026-1 applicable in Québec

This appendix establishes specific provisions for the application of the standard in Québec. Provisions of the standard and of its appendix must be read together for the purposes of understanding and interpretation. Where the standard and appendix differ, the appendix shall prevail.

A. Introduction

1. Title: **Relay Performance During Stable Power Swings**

2. Number: PRC-026-1

3. Purpose: No specific provision

4. Applicability:

4.1. Functional Entity:

No specific provision

4.2. Facilities

This standard only applies to the facilities of the Main Transmission System (RTP) connected to the RTP.

4.2.1 No specific provision

4.2.2 No specific provision

4.2.3 No specific provision

5. Background

No specific provision

6. Effective Date:

6.1. Adoption of the standard by the Régie de l'énergie: July 10, 2017

6.2. Adoption of the appendix by the Régie de l'énergie: July 10, 2017

6.3. Effective date of the standard and its appendix in Québec:

- Requirement R1: January 1, 2018.
- Requirements R2, R3, R4 for the BPS facilities: January 1, 2020.
- Requirements R2, R3, R4 for the non-BPS RTP facilities connected to the RTP: April 1, 2021.

B. Requirements and Measures

No specific provision

C. Compliance

1. Compliance Monitoring Process

1.1 Compliance Enforcement Authority

The Régie de l'énergie is responsible, in Québec, for compliance monitoring with respect to the reliability standard and its appendix that it adopts.

1.2 Evidence Retention

No specific provision

1.3 Compliance Monitoring and Assessment Process

No specific provision

1.4 Additional Compliance Information

No specific provision

Table of Compliance Elements

No specific provision

D. Regional Differences

No specific provision

E. Interpretations

No specific provision

F. Associated documents

No specific provision

PRC-026-1 – Attachment A

No specific provision

PRC-026-1 – Attachment B

No specific provision

Guidelines and Technical Basis

No specific provision

Appendix QC-PRC-026-1
Provisions specific to the standard PRC-026-1 applicable in Québec

Revision History

Revision	Date	Action	Change Tracking
0	July 10, 2017	New appendix Decision D-2017-076 which: • Adopts the standard and its appendix. • Suspends the application of requirements R2, R3 and R4 for the non-BPS RTP facilities connected to the RTP. • Sets the effective dates for the requirements.	New
1	March 27, 2020	Decision D-2020-036R which lifts the suspension of Requirements 2, 3 and 4 for non-BPS RTP facilities connected to the RTP.	Revision

A. Introduction

1. **Title:** **Coordination of Protection Systems for Performance During Faults**

2. **Number:** PRC-027-1

3. **Purpose:** To maintain the coordination of Protection Systems installed to detect and isolate Faults on Bulk Electric System (BES) Elements, such that those Protection Systems operate in the intended sequence during Faults.

4. **Applicability:**

   4.1. Functional Entities:

   4.1.1. Transmission Owner

   4.1.2. Generator Owner

   4.1.3. Distribution Provider (that owns Protection Systems identified in the Facilities section 4.2 below)

   4.2. Facilities: Protection Systems installed to detect and isolate Faults on BES Elements.

5. **Effective Date:** See the Implementation Plan for PRC-027-1, Project 2007-06 System Protection Coordination.

B. Requirements and Measures

R1. Each Transmission Owner, Generator Owner, and Distribution Provider shall establish a process for developing new and revised Protection System settings for BES Elements, such that the Protection Systems operate in the intended sequence during Faults. The process shall include: *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

1.1. A review and update of short-circuit model data for the BES Elements under study.

1.2. A review of the developed Protection System settings.

1.3. For Protection System settings applied on BES Elements that electrically join Facilities owned by separate functional entities (Transmission Owners, Generator Owners, and Distribution Providers), provisions to:

1.3.1. Provide the proposed Protection System settings to the owner(s) of the electrically joined Facilities.

1.3.2. Respond to any owner(s) that provided its proposed Protection System settings pursuant to Requirement R1, Part 1.3.1 by identifying any coordination issue(s) or affirming that no coordination issue(s) were identified.

1.3.3. Verify that identified coordination issue(s) associated with the proposed Protection System settings for the associated BES Elements are addressed prior to implementation.

1.3.4. Communicate with the other owner(s) of the electrically joined Facilities regarding revised Protection System settings resulting from unforeseen circumstances that arise during implementation or commissioning, Misoperation investigations, maintenance activities, or emergency replacements required as a result of Protection System component failure.

M1. Acceptable evidence may include, but is not limited to, dated electronic or hard copy documentation to demonstrate that the responsible entity established a process to develop settings for its Protection Systems, in accordance with Requirement R1.

R2. Each Transmission Owner, Generator Owner, and Distribution Provider shall, for each BES Element with Protection System functions identified in Attachment A: *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

- Option 1: Perform a Protection System Coordination Study in a time interval not to exceed six-calendar years; or
- Option 2: Compare present Fault current values to an established Fault current baseline and perform a Protection System Coordination Study when the comparison identifies a 15 percent or greater deviation in Fault current values (either three phase or phase to ground) at a bus to which the BES Element is connected, all in a time interval not to exceed six-calendar years;[1] or,
- Option 3: Use a combination of the above.

M2. Acceptable evidence may include, but is not limited to, dated electronic or hard copy documentation to demonstrate that the responsible entity performed Protection System Coordination Study(ies) and/or Fault current comparisons in accordance with Requirement R2.

R3. Each Transmission Owner, Generator Owner, and Distribution Provider shall utilize its process established in Requirement R1 to develop new and revised Protection System settings for BES Elements. *[Violation Risk Factor: High] [Time Horizon: Operations Planning]*

[1] The initial Fault current baseline(s) shall be established by the effective date of this Reliability Standard and updated each time a Protection System Coordination Study is performed. The Fault current baseline for BES generating resources may be established at the generator, the generator step-up (GSU) transformer(s), or at the common point of connection at 100 kV or above. For dispersed power producing resources, the Fault current baseline may also be established at the BES aggregation point (total capacity greater than 75 MVA). If an initial baseline was not established by the effective date of this Reliability Standard because of the previous use of an alternate option or the installation of a new BES Element, the entity may establish the baseline by performing a Protection System Coordination Study.

M3. Acceptable evidence may include, but is not limited to, dated electronic or hard copy documentation to demonstrate that the responsible entity utilized its settings development process established in Requirement R1, as specified in Requirement R3.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority:

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The applicable entity shall keep data or evidence to show compliance, as identified below, unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

The Transmission Owner, Generator Owner, and Distribution Provider shall each keep data or evidence to show compliance with Requirements R1, R2, and R3, and Measures M1, M2, and M3 since the last audit, unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

If a Transmission Owner, Generator Owner, or Distribution Provider is found non-compliant, it shall keep information related to the non-compliance until mitigation is completed and approved, or for the time specified above, whichever is longer.

The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program

As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	N/A	The responsible entity established a process in accordance with Requirement R1, but failed to include Requirement R1, Part 1.1 or Part 1.2.	The responsible entity established a process in accordance with Requirement R1, but failed to include Requirement R1, Part 1.1 and Part 1.2.	The responsible entity established a process in accordance with Requirement R1, but failed to include Requirement R1, Part 1.3. OR The responsible entity failed to establish any process in accordance with Requirement R1.
R2.	The responsible entity performed a Protection System Coordination Study for each BES Element, in accordance with Requirement R2, Option 1, Option 2, or Option 3 but was late by less than or equal to 30 calendar days.	The responsible entity performed a Protection System Coordination Study for each BES Element, in accordance with Requirement R2, Option 1, Option 2, or Option 3, but was late by more than 30 calendar days but less than or equal to 60 calendar days.	The responsible entity performed a Protection System Coordination Study for each BES Element, in accordance with Requirement R2, Option 1, Option 2, or Option 3, but was late by more than 60 calendar days but less than or equal to 90 calendar days.	The responsible entity performed a Protection System Coordination Study for each BES Element, in accordance with Requirement R2, Option 1, Option 2, or Option 3, but was late by more than 90 calendar days. OR The responsible entity failed to perform Option 1, Option

				2, or Option 3, in accordance with Requirement R2.
R3.	N/A	N/A	N/A	The responsible entity failed to utilize the process established in accordance with Requirement R1.

D. Regional Variances

None.

E. Associated Documents

NERC System Protection and Control Subcommittee – "Power Plant and Transmission System Protection Coordination."

NERC System Protection and Control Task Force, December 7, 2006, "Assessment of Standard PRC-001-0 – System Protection Coordination."

NERC System Protection and Control Task Force, September 2006, "The Complexity of Protecting Three-Terminal Transmission Lines."

Version History

Version	Date	Action	Change Tracking
1	November 5, 2015	Adopted by NERC Board of Trustees	New standard developed under Project 2007-06

Attachment A

The following Protection System functions[2] are applicable to Requirement R2 if: (1) available Fault current levels are used to develop the settings for those Protection System functions; and (2) those Protection System functions require coordination with other Protection Systems.

21 – Distance if:

- infeed is used in determining reach (phase and ground distance), or
- zero-sequence mutual coupling is used in determining reach (ground distance).

50 – Instantaneous overcurrent

51 – AC inverse time overcurrent

67 – AC directional overcurrent if used in a non-communication-aided protection scheme

Notes:

1. The above Protection System functions utilize current in their measurement to initiate tripping of circuit breakers. Changes in the magnitude of available Fault current can impact the coordination of these functions.
2. See the PRC-027-1 Supplemental Material section for additional information.

[2] ANSI/IEEE Standard C37.2 *Standard for Electrical Power System Device Function Numbers, Acronyms, and Contact Designations*.

Purpose

The Purpose states: To maintain the coordination of Protection Systems installed to detect and isolate Faults on Bulk Electric System (BES) Elements, such that those Protection Systems operate in the intended sequence during Faults.

Coordinated Protection Systems enhance reliability by isolating faulted equipment, reducing the risk of BES instability or Cascading, and leaving the remainder of the BES operational and more capable of withstanding the next Contingency. When Faults occur, properly coordinated Protection Systems minimize the number of BES Elements that are removed from service and protect equipment from damage. This standard requires that entities establish and implement a process to coordinate their Protection Systems to operate in the intended sequence during Faults.

Applicability

Transmission Owners, Generator Owners, and Distribution Providers are included in the Applicability of PRC-027-1 because they may own Protection Systems that are installed for the purpose of detecting Faults on the Bulk Electric System (BES). It is only those Protection Systems that are under the purview of this standard.

Transmission Owners are included in the Applicability of PRC-027-1 because they own the largest number of Protection Systems installed for the purpose of detecting Faults on the BES.

Generator Owners have Protection Systems installed for the purpose of detecting Faults on the BES. It is important that those Protection Systems are coordinated with Protection Systems owned by Transmission Owners to ensure that generation Facilities do not become disconnected from the BES unnecessarily. Functions such as impedance reaches, overcurrent pickups, and time delays need to be evaluated for coordination.

A Distribution Provider may provide an electrical interconnection and path to the BES for generators that will contribute current to Faults that occur on the BES. If the Distribution Provider owns Protection Systems that operate for those Faults, it is important that those Protection Systems are coordinated with other Protection Systems that can be impacted by the current contribution to the Fault of Distribution Provider.

After the Protection Systems of Distribution Providers and Generator Owners are shown to be coordinated with other Protection Systems on the BES, there will be little future impact on the entities unless there are significant changes at or near the bus that interconnects with the Transmission Owner. The Transmission Owner, which is typically the entity maintaining the system model for Fault studies, will provide the Fault current data upon request by the Distribution Provider or Generator Owner. The Distribution Provider and Generator Owner will determine whether a change in Fault current from the baseline has occurred such that a review of coordination is necessary.

Requirement R1

The requirement states: Each Transmission Owner, Generator Owner, and Distribution Provider shall establish a process for developing new and revised Protection System settings for BES Elements, such that the Protection Systems operate in the intended sequence during Faults.

The reliability objective of this requirement is to have applicable entities establish a process to develop settings for coordinating their Protection Systems, such that they operate in the intended sequence during Faults. The parts that are included as elements of the process ensure the development of accurate settings, as well as providing internal and external checks to minimize the possibility of errors that could be introduced in the development of settings.

This standard references various publications that discuss protective relaying theory and application. The description of "coordination of protection" is from the pending revision of IEEE Standard C37.113-1999 (Reaffirmed: 2004), *Guide for Protective Relay Applications to Transmission Lines*, which reads:

> *"The process of choosing current or voltage settings, or time delay characteristics of protective relays such that their operation occurs in a specified sequence so that interruption to customers is minimized and least number of power system elements are isolated following a system fault."*

Entities may have differing technical criteria for the development of Protection System settings based on their own philosophies. These philosophies can vary based on system topology, protection technology utilized, as well as historical knowledge; as such, a single definition or criterion for "Protection System coordination" is not practical.

The coordination of some Protection Systems may seem unnecessary, such as for a line that is protected solely by dual current differential relays. However, backup Protection Systems that are enabled to operate based on current or apparent impedance with some definite or inverse time delay must be coordinated with other Protection Systems of the BES Element such that tripping does not unnecessarily occur for Faults outside of the differential zone.

Part 1.1 A review and update of short-circuit model data for the BES Elements under study.

The short-circuit study provides the necessary Fault currents used by protection engineers to develop Protection System settings for Transmission Owners, Generator Owners, and Distribution Providers. Generator Owners and Distribution Providers may not have or maintain short-circuit models; consequently, these entities would obtain the short-circuit model data from the Transmission Planners, Planning Coordinators, or Transmission Owners. Including a review and, if necessary, an update of short-circuit study information is necessary to ensure that information accurately reflects the physical power system that will form the basis of the Protection System Coordination Study and development of Protection System relay settings. The results of a short-circuit study are only as accurate as the information that its calculations are based on.

A short-circuit study is an analysis of an electrical network that determines the magnitude of the currents flowing in the network during an electrical Fault. Because the results of short-circuit studies are used as the basis for protective device coordination studies, the short-circuit model should accurately reflect the physical power system.

Reviews could include:

1. A review of applicable BES line, transformer, and generator impedances and Fault currents.

2. A review of the network model to confirm the network in the study accurately reflects the configuration of the actual System, or how the System will be configured when the proposed relay settings are installed.
3. A review, where applicable, of interconnected Transmission Owner, Generator Owner, and Distribution Provider information.

Part 1.2 A review of the developed Protection System settings.

A review of the Protection System settings prior to implementation reduces the possibility of introducing human error. A review is any systematic process of verifying the developed settings meet the technical criteria of the entity. Examples of reviews include peer reviews, automated checking programs, and entity-developed review procedures.

Part 1.3 For Protection System settings applied on BES Elements that electrically join Facilities owned by separate functional entities (Transmission Owners, Generator Owners, and Distribution Providers), provisions to:

Requirement R1, Part 1.3 addresses the coordination of Protection System settings applied on BES Elements that electrically join Facilities owned by separate functional entities. Communication among these entities is essential so potential Protection System coordination issues can be identified and addressed prior to implementation of any proposed Protection System changes.

Part 1.3.1 1.3.1. Provide the proposed Protection System settings to the owners of the electrically joined Facilities.

Requirement R1, Part 1.3.1 requires the entity to include in its process a provision to provide proposed Protection System settings to other entities. This communication ensures that the other entities have the necessary information to review the settings and determine if there are any Protection System coordination issues.

Part 1.3.2 Respond to any owner(s) that provided its proposed Protection System settings pursuant to Requirement R1, Part 1.3.1 by identifying any coordination issue(s) or affirming that no coordination issue(s) were identified.

Requirement R1, Part 1.3.2 requires the entity receiving proposed Protection System settings to include in its process a provision to respond to the entity that initiated the proposed changes. This ensures that the proposed settings are reviewed and that the initiating entity receives a response indicating Protection System coordination issues were identified, or affirmation that no issues were identified.

Part 1.3.3 Verify that identified coordination issue(s) associated with the proposed Protection System settings for the associated BES Elements are addressed prior to implementation.

Requirement R1, Part 1.3.3 requires the entity to include in their process a provision to verify that any identified coordination issue(s) associated with the proposed Protection System settings are addressed prior to implementation. This ensures that any potential impact to BES reliability is minimized.

The exclusion in PRC-001-1.1(ii), Requirement R3, R3.1 for dispersed power producing resources applies only to interconnections between different functional entities. As such, the exclusion only maps to Requirement R1, Part 1.3 in PRC-027-1. Due to the design of dispersed generation sites, the Protection Systems applied on the individual dispersed generation resources are not electrically joined Facilities owned by separate functional entities as specified in Requirement R1, Part 1.3 nor are they connected by BES Elements. Therefore Requirement R1, Part 1.3 does not apply to the Protection Systems applied on the individual dispersed generation resources. Requirement R1, Part 1.3 applies only to the Protection Systems applied on the BES Elements that electrically join Facilities owned by separate functional entities.

Note: There could be instances where coordination issues are identified and the entities agree not to mitigate all of the issues based on engineering judgment. It is also recognized that coordination issues identified during a project may not be immediately resolved if the resolution involves additional system modifications not identified in the initial project scope. Further, there could be situations where protection philosophies differ between entities, but the entities can agree that these differences do not create coordination issues.

> **Part 1.3.4** Communicate with the other owner(s) of the electrically joined Facilities regarding revised Protection System settings resulting from unforeseen circumstances that arise during implementation or commissioning, Misoperation investigations, maintenance activities, or emergency replacements required as a result of Protection System component failure.

Requirement R1, Part 1.3.4 requires the entity to communicate revisions to Protection System settings that occur due to unforeseen circumstances and differ from those developed during the planning stages of projects.

Requirement R2

This requirement states: Each Transmission Owner, Generator Owner, and Distribution Provider shall, for each BES Element with Protection System functions identified in Attachment A:

- Option 1: Perform a Protection System Coordination Study in a time interval not to exceed six-calendar years; or
- Option 2: Compare present Fault current values to an established Fault current baseline and perform a Protection System Coordination Study when the comparison identifies a 15 percent or greater deviation in Fault current values (either three phase or phase to ground) at a bus to which the BES Element is connected, all in a time interval not to exceed six-calendar years;[3] or,

[3] The initial Fault current baseline(s) shall be established by the effective date of this Reliability Standard and updated each time a Protection System Coordination Study is performed. The Fault current baseline for BES generating resources may be established at the generator, the generator step-up (GSU) transformer(s), or at the common point of connection at 100 kV or above. For dispersed power producing resources, the Fault current baseline may also be established at the BES aggregation point (total capacity greater than 75 MVA). If an initial baseline was not established by the effective date of this Reliability Standard because of the previous use of an alternate option or the installation of a new BES Element, the entity may establish the baseline by performing a Protection System Coordination Study.

- Option 3: Use a combination of the above.

Over time, incremental changes in Fault current can accumulate enough to impact the coordination of Protection System functions affected by Fault current. To minimize this risk, Requirement R2 requires responsible entities to periodically (1) perform Protection System Coordination Studies and/or (2) review available Fault currents for those Protection System functions listed in Attachment A. Two triggers were established for initiating a review of existing Protection System settings to allow for industry flexibility.

In the first option, an entity may choose a time-based methodology to review Protection System settings, thus eliminating the necessity of establishing a Fault current baseline and periodically performing Fault current comparisons. This option provides the entity the flexibility to choose an interval of up to six-calendar years for performing the Protection System Coordination Studies for those Protection System functions in Attachment A. The six-calendar-year time interval was selected as a balance between the manpower required to perform the studies and the potential reliability impacts created by incremental changes of Fault current over time.

The second option allows the entity to periodically check for a 15 percent or greater deviation in Fault current (either three-phase or phase-to-ground) from an established Fault current baseline for Protection Systems at each bus to which a BES Element is connected. Fault current baseline values can be obtained from the short-circuit studies performed by the Transmission Planners, Planning Coordinators, or Transmission Owners. This option allows the entity to choose an interval of up to six-calendar years to perform the Fault current comparisons and Protection System Coordination Studies. The six-calendar-year time interval was selected as a balance between the manpower required to perform the studies and the potential reliability impacts created by incremental changes of Fault current over time.

The accumulation of these incremental changes could affect the performance of Protection Systems during Fault conditions. A maximum Fault current deviation of 15 percent (when compared to the entity-established baseline) was established based on generally-accepted margins for setting Protection Systems in which incremental Fault current changes would not interfere with coordination. The 15 percent maximum deviation provides an entity with latitude to choose a Fault current threshold that best matches its protection philosophy, or other business considerations. The Fault current based option requires an entity to first establish a Fault current baseline to be used as a point of reference for future Fault current studies. The Fault current values used in the percent change calculation, whether three-phase or phase-to-ground Fault currents, are typically determined with all generation in service and all transmission BES Elements in their normal operating state.

As described in the footnote for Requirement R2, Option 2, an entity that elects to initially use Option 2 must establish its baseline prior to the effective date of the standard. If an initial baseline was not established by the effective date of this Reliability Standard because of the previous use of an alternate option or the installation of a new BES Element, the entity may establish the baseline upon performing a Protection System Coordination Study. The Fault current baseline values can be updated or established when a Protection System Coordination Study is performed. The baseline values at each bus to which a BES Element is connected are updated whenever a new Protection System Coordination Study is performed for the subject

Protection System. The footnote also states that the Fault current baselines may be established for BES generating resources at the generator, the BES aggregation point for dispersed power producing resources, or at the common point of connection at 100 kV or above.

> **Example:** Prior to the effective date of PRC-027-1, an entity intending to use Option 2 of Requirement R2 establishes an initial baseline; e.g., 10,000 amps at the bus to which the BES Element under study is connected. A short-circuit review performed on March 1, 2024, for example, identifies that the Fault current has increased to 11,250 amps (12.5 percent deviation); consequently, no Protection System Coordination Study is required since the increase is below the maximum 15 percent deviation. The baseline value for the next comparison (to be performed no later than December 31, 2030) remains at 10,000 amps because no study was required as a result of the initial comparison. During the next six-year interval, Fault current comparison identifies that the Fault current has increased to 11,500 (15 percent deviation); therefore, a Protection System Coordination Study is required (and must also be completed no later than December 31, 2030), and a new baseline of 11,500 amps would be established.
>
> **Note:** In the first review described above, if the entity decides to perform a Protection System Coordination Study at the 12.5 percent deviation and the results of the study indicate that the settings still meet the setting criteria of the entity, then no settings changes are required and the baseline Fault current(s) would be updated.

As a third option, an entity has the flexibility to apply a combination of the two methodologies. For example, an entity may choose the periodic Protection System review (Option 1) and review its Facilities operated above 300 kV on a six-calendar-year interval, while choosing to use the Fault current comparison (Option 2) for its Facilities operated below 300 kV.

The Protection System functions listed in Attachment A utilize AC current in their measurement to initiate tripping of circuit breakers and the coordination of these functions is susceptible to changes in the magnitude of available short-circuit Fault current. These functions are included in Attachment A based on meeting the following criteria: (1) available Fault current levels are used to develop settings, and (2) the functions require coordination with other Protection Systems. Examples of functions not included in Attachment A because they do not meet both of the criteria are differential relays and Fault detectors. The numerical identifiers in Attachment A represent general device functions according to *ANSI/IEEE Standard C37.2 Standard for Electrical Power System Device Function Numbers, Acronyms, and Contact Designations*.

The following provide additional information regarding the Protection System functions in Attachment A.

A “51 – AC inverse time overcurrent” relay connected to a CT on the neutral of a generator step-up transformer, referred to as “51N – AC Inverse Time Earth Overcurrent Relay (Neutral CT Method)” in ANSI/IEEE Standard C37.2, would be included in a Protection System Coordination Study. Also applicable, are “51 – AC Inverse time overcurrent” relays connected to CTs on the phases of an autotransformer for through-fault protection. Overcurrent functions used in conjunction with other functions are to be reviewed as well. An example is a definite-time overcurrent function, which is a “50 – Instantaneous overcurrent” function used in conjunction with a “62 – Time-delay” function.

If the functions listed in Attachment A are used in conjunction with other functions, they would be included in a Protection System Coordination Study provided they require coordination with other Protection Systems. An example of this is a time-delayed "21 – Distance" function, which is a "21 – Distance" function with a "62 – Time-delay" function. Another example would be a definite-time overcurrent function, which is a "50 – Instantaneous overcurrent" function with a "62 – Time-delay" function. A "50 – Instantaneous overcurrent" function used for supervising a "21 – Distance" function would not be included in a Protection System Coordination Study as it does not require coordination with other Protection Systems.

Reviewing "21 – Distance" functions is limited to those applied for phase and ground distance where infeed is used in determining the phase or ground distance setting when zero-sequence mutual coupling is used in determining the setting. Where infeed is not used in determining the setting, "21 – Distance" functions would not be included in a Protection System Coordination Study, as the reach is not susceptible to changes in the magnitude of available short-circuit Fault current. Where infeed is used in determining the reach, coordination can be affected by changes in the magnitude of available short-circuit Fault current. Two examples where infeed may be used in determining the reach, are protection for a transmission line with a long tap and a three-terminal transmission line. Ground distance functions are influenced by zero-sequence mutual coupling. The ground distance measurement can appear to be greater than or less than the true distance to a Fault when there is zero-sequence mutual coupling. The influence of zero-sequence mutual coupling changes with the magnitude of available short-circuit current. Therefore, "21 – Distance" functions would be included in a Protection System Coordination Study, when zero-sequence mutual coupling is used in determining the setting.

The 67 – AC directional overcurrent function utilized in Protection Systems for Transmission lines can be instantaneous overcurrent, inverse time overcurrent, or both instantaneous overcurrent and inverse time overcurrent. For example, in a communication-aided directional comparison blocking (DCB) scheme, the instantaneous overcurrent function is set very sensitive. When a single line-to-ground Fault occurs on a Transmission line, the Fault is detected by a number of Protection Systems for other Transmission lines. Signals from communication equipment are transmitted and received to block the other Protection Systems for the non-faulted Transmission lines from operating, thereby providing the coordination. A 67 – AC directional overcurrent function used in a permissive overreaching transfer trip scheme (POTT) relies on a signal from the remote end to operate and, therefore, does not require coordination with other Protection Systems.

Instantaneous overcurrent and/or inverse time overcurrent for a 67 – AC directional overcurrent function are utilized in a non-communication-aided Protection System for Transmission lines. As communication is not used to prevent operation for Faults outside a Protection System's zone of protection, coordination is necessary with other Protection Systems for buses, transformers, and other Transmission lines. The instantaneous overcurrent function should be set to not overreach the end of the Transmission line. The inverse time overcurrent function should be set to coordinate with the inverse time overcurrent function of other Protection Systems. Changes in the magnitude of available Fault current can affect the coordination.

Requirement R3

The requirement states: Each Transmission Owner, Generator Owner, and Distribution Provider shall utilize its process established in Requirement R1 to develop new and revised Protection System settings for BES Elements.

The reliability objective of this requirement is for applicable entities to utilize the process established in Requirement R1. Utilizing each of the elements of the process ensures a consistent approach to the development of accurate Protection System settings, decreases the possibility of introducing errors, and increases the likelihood of maintaining a coordinated Protection System.

Rationale

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT adoption, the text from the rationale text boxes will be moved to this section.

Rationale for Requirement R1:

Coordinated Protection Systems enhance reliability by isolating faulted equipment, thus reducing the risk of BES instability or Cascading, and leaving the remainder of the BES operational and more capable of withstanding the next Contingency. When Faults occur, properly coordinated Protection Systems minimize the number of BES Elements that are removed from service and protect equipment from damage. The stated purpose of this standard is: "To maintain the coordination of Protection Systems installed to detect and isolate Faults on Bulk Electric System (BES) Elements, such that those Protection Systems operate in the intended sequence during Faults." Requirement R1 captures this intent by requiring responsible entities establish a process that, when followed, allows for their Protection Systems to operate in the intended sequence during Faults. Requirement R1, Parts 1.1 through 1.3 are key elements to the process for developing Protection System settings.

Part 1.1 Reviewing and updating the short-circuit model data used to develop new or revised Protection System settings helps to assure that settings are developed using accurate, up-to-date information. Generator Owners and Distribution Providers may not have or maintain short-circuit models; consequently, these entities would obtain the short-circuit model data from the Transmission Planners, Planning Coordinators, or Transmission Owners.

Part 1.2 A review of the developed Protection System settings reduces the likelihood of introducing human error and verifies that the settings produced meet the technical criteria of the entity. Peer reviews, automated checking programs, and entity-developed review procedures are all examples of reviews.

Part 1.3 The coordination of Protection Systems associated with BES Elements that electrically join Facilities owned by separate functional entities (Transmission Owners, Generator Owners, and Distribution Providers) is essential to the reliability of the BES. Communication and review of proposed settings among these entities are necessary to identify potential coordination issues and address the issues prior to implementation of any proposed Protection System changes.

The exclusion in PRC-001-1.1(ii), Requirement R3, R3.1 for dispersed power producing resources applies only to interconnections between different functional entities. As such, the exclusion only maps to Requirement R1, Part 1.3 in PRC-027-1. Due to the design of dispersed generation sites, the Protection Systems applied on the individual dispersed generation resources are not electrically joined Facilities owned by separate functional entities as specified in Requirement R1, Part 1.3 nor are they connected by BES Elements. Therefore Requirement R1, Part 1.3 does not apply to the Protection Systems applied on the individual dispersed generation resources. Requirement R1, Part 1.3 applies only to the Protection Systems applied on the BES Elements that electrically join Facilities owned by separate functional entities.

Unforeseen circumstances could require immediate changes to Protection System settings. Requirement R1, Part 1.3.4 requires owners to include provisions to communicate those

unplanned settings changes after-the-fact to the other owner(s) of the electrically joined Facilities.

Note: In cases where a single protective relaying group performs coordination work for separate functional entities within an organization, the communication aspects of Requirement R1, Part 1.3 can be demonstrated by internal documentation.

Rationale for Requirement R2:
Over time, incremental changes in Fault current can accumulate enough to impact the coordination of Protection System functions affected by Fault current. To minimize this risk, Requirement R2 requires Transmission Owners, Generator Owners, and Distribution Providers to periodically (1) perform Protection System Coordination Studies and/or (2) review available Fault currents for those Protection System functions listed in Attachment A. The numerical identifiers in Attachment A represent general protective device functions per ANSI/IEEE *Standard C37.2 Standard for Electrical Power System Device Function Numbers, Acronyms, and Contact Designations*.

Requirement R2 provides entities with options to assess the state of their Protection System coordination.

Option 1 is a time-based methodology. The entity may choose to perform, at least once every six-calendar years, a Protection System Coordination Study for each of its Protection Systems identified in Attachment A. The six-calendar-year time interval was selected as a balance between the resources required to perform the studies and the potential reliability impacts created by incremental changes of Fault current over time.

Option 2 is a Fault current-based methodology. If Option 2 is initially selected, Fault current baseline(s) must be established prior to the effective date of this Reliability Standard. A baseline may be established when a new BES Element is installed or after a Protection System Coordination Study has been performed. The baseline(s) will be used as control point(s) for future Fault current comparisons. The Fault current baseline values can be obtained from the short-circuit studies performed by the Transmission Planners, Planning Coordinators, or Transmission Owners. In a time interval not to exceed six-calendar years following the effective date of this standard, an entity must perform a Fault current comparison. If the comparison identifies a deviation less than 15 percent, no further action is required for that six-year interval; however, if the comparison identifies a 15 percent or greater deviation in Fault current values (either three-phase or phase-to-ground) at each bus to which the BES Element is connected, the entity must also perform a Protection System Coordination Study during the same six-year interval. The baseline Fault current value(s) will be re-established whenever a new Protection System Coordination Study is performed. Fault current changes on the System not directly associated with BES modifications are usually small and occur gradually over time. The accumulation of these incremental changes could affect the performance of Protection System functions (identified in Attachment A of this standard) during Fault conditions. A Fault current deviation threshold of 15 percent or greater (as compared to the established baseline) and a maximum time interval of six calendar years were chosen for these evaluations. These parameters provide an entity with latitude to choose a Fault current threshold and time interval that best match its protection philosophy, Protection System maintenance schedule, or other

business considerations, without creating risk to reliability (See the Supplemental Material section for more detailed discussion).

The footnote in Option 2 describes how an entity may change from a time-based option to a Fault current-based option for existing BES Elements as well as establishing baselines for new BES Elements by performing Protection System Coordination Studies. The footnote also states that Fault current baselines for BES generating resources may be established at the generator, the generator step-up (GSU) transformer(s), or at the common point of connection at 100 kV or above. For dispersed power producing resources, the Fault current baseline may also be established at the BES aggregation point (total capacity greater than 75 MVA).

Option 3 provides the entity the choice of using both the time-based and Fault current-based methodologies. For example, the entity may choose to utilize the time-based methodology for Protection Systems at more critical Facilities and use the Fault current-based methodology for Protection Systems at other Facilities.

Rationale for Requirement R3:
Utilizing the processes established in Requirement R1 to develop new and revised Protection System settings provides a consistent approach to the development of Protection System settings and will minimize the potential for errors.

Appendix PRC-027-1-QC-1
Specific provisions applicable in Québec for standard
PRC-027-1 – Coordination of Protection Systems for Performance During Faults

This appendix establishes specific provisions for the application of the standard in Québec. Provisions of the standard and of this appendix must be read jointly for comprehension and interpretation purposes. Where the standard and appendix differ, the appendix shall prevail.

A. Introduction

1. Title: No specific provisions.

2. Number: No specific provisions.

3. Purpose: No specific provisions.

4. Applicability:

4.1. Functional Entities

No specific provisions.

4.2. Facilities

This standard only applies to Protection Systems installed to detect and isolate Faults on Main Transmission System (RTP) Elements.

5. Effective dates for Québec:

5.1. Adoption of the standard by the Régie de l'énergie: September 1st, 2022

5.2. Adoption of the appendix by the Régie de l'énergie: September 1st, 2022

5.3. Effective date of the standard and appendix for Québec: October 1st, 2024

B. Requirements and measures

All references to the terms "Bulk Electric System" or "BES" shall be replaced by the terms "Main Transmission System" or "RTP" respectively.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

In Québec, "Compliance Enforcement Authority" means the Régie de l'énergie in its roles of monitoring and enforcing compliance with respect to the Reliability Standard and to this appendix.

1.2. Evidence Retention

No specific provisions.

1.3. Compliance Monitoring and Enforcement Program

The Régie de l'énergie establishes the monitoring processes used to evaluate data or information for the purpose of determining compliance or non-compliance with the Reliability Standard and with this appendix.

Violation Severity Levels

All references to the terms "Bulk Electric System" or "BES" shall be replaced by the terms "MainTransmission System" or "RTP" respectively.

D. Regional Variances

No specific provisions.

E. Associated Documents

No specific provisions.

Attachment A

No specific provisions.

Supplemental Material

All references to the terms “Bulk Electric System” or “BES” shall be replaced by the terms “Main Transmission System” or “RTP” respectively.

Rationale

All references to the terms “Bulk Electric System” or “BES” shall be replaced by the terms “Main Transmission System” or “RTP” respectively.

Version history

Version	Date	Action	Change tracking
1	September 1st, 2022	New appendix as per decision D-2022-108.	New

A. Introduction

1. **Title:** Disturbance Monitoring and Reporting Requirements for Inverter-Based Resources

2. **Number:** PRC-028-1

3. **Purpose:** To have adequate data available from Inverter-Based Resources to evaluate Inverter-Based Resource ride-through performance during System Disturbances and to provide data for Inverter-Based Resource model validation.

4. **Applicability:**

   4.1. Functional Entities:

   4.1.1. Generator Owner

   4.2. Facilities:

   4.2.1 BES Inverter-Based Resources

   4.2.2 Non-BES Inverter-Based Resources that either have or contribute to an aggregate nameplate capacity of greater than or equal to 20 MVA, connected through a system designed primarily for delivering such capacity to a common point of connection at a voltage greater than or equal to 60 kV

5. **Effective Date:** See Implementation Plan

B. Requirements and Measures

R1. Each Generator Owner shall have sequence of event recording (SER) data for the following Elements that it owns: *[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*

1.1. Circuit breaker position (open/close) for circuit breakers associated with the main power transformer(s)[1], collector bus(es), shunt static and dynamic reactive device(s), and AC-DC and DC-AC converters, if any, in case of VSC HVDC system with a dedicated connection to Inverter-Based Resource.

1.2. For IBR units[2] in commercial operation[3] after the effective date of this standard, the following data shall be recorded when triggered by ride-through operation or tripping of an IBR unit.

[1] For the purpose of this standard, the main power transformer is the power transformer that steps up voltage from the collection system voltage to the nominal transmission/interconnecting system voltage for Inverter-Based Resources. In case of dedicated VSC HVDC system connecting to an Inverter-Based Resource, a transformer isolating the DC-AC converter from the transmission system is also considered a main power transformer.
[2] IBR unit includes the inverter, converter, wind turbine generator, or high voltage direct current converter connecting generating resource to alternating current Transmission network.
[3] Commercial operation means achievement of this designation indicating that the facility has received all approvals necessary for operation after completion of initial start-up testing.

1.2.1. All fault codes.

1.2.2. All fault alarms.

1.2.3. High and low voltage ride-through mode status.

1.2.4. High and low frequency ride-through mode status.

1.3. For IBR units in commercial operation before the effective date of this standard, if capable, the following data shall be recorded when triggered by ride-through operation or tripping of an IBR unit.

1.3.1. All fault codes.

1.3.2. All fault alarms.

1.3.3. High and low voltage ride-through mode status.

1.3.4. High and low frequency ride-through mode status.

M1. The Generator Owner has evidence (electronic or hard copy) of data, as applicable, as specified in Requirement R1. Evidence may include, but is not limited to: (1) actual data recordings; or (2) documents describing the device interconnections and configurations which may include a single design standard as representative for common installations; or (3) station or equipment drawings. The evidence to show IBR unit capability to record fault codes, alarms, or ride-through mode status may include, but is not limited to: (1) equipment specification, (2) letter from equipment manufacturer, or (3) documents describing lack of recording capability.

R2. Each Generator Owner shall have triggered fault recording (FR) data to determine the following electrical quantities for Elements that it owns: *[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*

2.1. High-side of the main power transformer FR data:

2.1.1. Phase-to-neutral voltage for each phase.

2.1.2. Each phase current and the residual or neutral current.

2.1.3. Real and Reactive Power expressed on a three-phase basis.

2.2. Collector feeder breaker FR data:

2.2.1. Phase-to-neutral voltage for each phase.

2.2.2. Each phase current and the residual or neutral current.

2.2.3. Real and Reactive Power expressed on a three-phase basis.

2.3. Shunt dynamic reactive device FR data:

2.3.1. Phase-to-neutral voltage for each phase.

2.3.2. Each phase current and the residual or neutral current.

2.3.3. Reactive Power output expressed on a three-phase basis.

M2. The Generator Owner has evidence (electronic or hard copy) of FR data that is sufficient to determine electrical quantities as specified in Requirement R2. Evidence may include, but is not limited to: (1) actual data recordings or derivations; or (2) documents describing the device specifications and configurations which may include a single design standard as representative for common installations; or (3) station or equipment drawings.

R3. Each Generator Owner shall have FR data as specified in Requirement R2 that meets the following: *[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*

3.1. High-side of the main power transformer FR data:

3.1.1. A single record or multiple records that include a pre-trigger record length of at least two cycles and a total record length of at least 2.0 seconds for the same trigger point.

3.1.2. A minimum recording rate of 64 samples per cycle.

3.1.3. Trigger settings for at least the following:

3.1.3.1. Neutral (residual) overcurrent.

3.1.3.2. AC phase overvoltage and undervoltage.

3.1.3.3. Overfrequency and underfrequency

3.2. Collector feeder breaker FR data:

3.2.1. A single record or multiple records that include a pre-trigger record length of at least two cycles and a total record length of at least 2.0 seconds for the same trigger point.

3.2.2. A minimum recording rate of 64 samples per cycle.

3.2.3. Trigger settings for at least the following:

3.2.3.1. Neutral (residual) overcurrent, if applicable.

3.2.3.2. AC phase overvoltage and undervoltage.

3.2.3.3. Overfrequency and underfrequency.

3.3. Shunt dynamic reactive device FR data:

3.3.1. A single record or multiple records that include a pre-trigger record length of at least two cycles and a total record length of at least 2.0 seconds for the same trigger point.

3.3.2. A minimum recording rate of 64 samples per cycle.

3.3.3. Trigger settings for at least the following:

3.3.3.1. Neutral (residual) overcurrent.

3.3.3.2. AC phase overvoltage and undervoltage.

M3. The Generator Owner has evidence (electronic or hard copy) that FR data meets Requirement R3. Evidence may include, but is not limited to: (1) actual data recordings or derivations, or (2) documents describing the device specification and device configuration or settings.

R4. Each Generator Owner shall have continuous dynamic disturbance recording (DDR) data and storage to determine the following electrical quantities for each main power transformer(s) it owns: *[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*

- **4.1.** One phase-to-neutral or positive sequence voltage on high-side of the main power transformer(s).
- **4.2.** The phase current for the same phase at the same voltage corresponding to the voltage in Requirement R4, Part 4.1, or the positive sequence current.
- **4.3.** Real Power and Reactive Power flows expressed on a three-phase basis corresponding to each main power transformer(s) where current measurements are required.
- **4.4.** Frequency of any one of the voltage(s) in Requirement R4, Part 4.1.

M4. The Generator Owner has evidence (electronic or hard copy) of continuous DDR data recording and storage to determine electrical quantities as specified in Requirement R4. Evidence may include, but is not limited to: (1) actual data recordings or derivations; or (2) documents describing the device specifications and configurations, which may include a single design standard as representative for common installations; or (3) station drawings.

R5. Each Generator Owner responsible for DDR data for the electrical quantities identified in Requirement R4 shall have DDR data that meet the following: *[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*

- **5.1.** Input sampling rate of at least 960 samples per second.
- **5.2.** Output recording rate of electrical quantities of at least 60 times per second.

M5. The Generator Owner has evidence (electronic or hard copy) that DDR data meets Requirement R5. Evidence may include, but is not limited to: (1) documents describing the device specification, device configuration, or settings (R5, Part 5.1; R5, Part 5.2); or (2) actual data recordings (R5, Part 5.2).

R6. Each Generator Owner shall time synchronize all SER, FR, and DDR data to meet the following: *[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*

- **6.1.** Synchronization to Coordinated Universal Time (UTC) with or without a local time offset.
- **6.2.** The IBR unit synchronized device clock accuracy within ± 100 milliseconds of UTC. For all other devices, synchronized device clock accuracy within ± 1 milliseconds of UTC.

M6. The Generator Owner has evidence (electronic or hard copy) of time synchronization described in Requirement R6. Evidence may include, but is not limited to: (1) documents describing the device specification, configuration, or setting; (2) time synchronization indication or status; or 3) station drawings.

R7. Each Generator Owner shall provide all requested SER, FR, and DDR data to its Transmission Planner, Planning Coordinator, Transmission Operator, Balancing Authority, Reliability Coordinator, Regional Entity, or NERC in accordance with the following: *[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*

7.1. Data shall be retrievable for the period of 20 calendar days, inclusive of the day the data was recorded.

7.2. Data subject to Part 7.1 shall be provided within 15 calendar days of a request unless an extension is granted by the requestor.

7.3. SER data shall be provided in ASCII[4] Comma Separated Value (CSV) format following Attachment 1.

7.4. FR data shall be provided either in CSV format with appropriate headers or in electronic files that are formatted in conformance with C37.111, IEEE Standard Common Format for Transient Data Exchange (COMTRADE), revision C37.111-1999 or later.

7.5. DDR data shall be provided either in CSV format with appropriate headers or in electronic files that are formatted in conformance with C37.111, IEEE Standard Common Format for Transient Data Exchange (COMTRADE), revision C37.111-1999 or later.

7.6. Data files shall be named in conformance with C37.232, IEEE Standard for Common Format for Naming Time Sequence Data Files (COMNAME), revision C37.232-2011 or later.

M7. The Generator Owner has evidence (electronic or hard copy) that data was submitted upon request in accordance with Requirement R7. Evidence may include, but is not limited to: (1) actual data recordings; (2) dated transmittals to the requesting entity with formatted records; or (3) documents describing data storage capability, device specification, configuration, or settings.

R8. Each Generator Owner shall, upon the discovery of a failure of the recording capability for the SER, FR, or DDR data: *[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*

- Restore the recording capability within 90 calendar days, or
- Submit a Corrective Action Plan (CAP) to the Regional Entity within 90 calendar days and then implement it according to CAP timeline.

[4] American Standard Code for Information Interchange

M8. The Generator Owner has dated evidence (electronic or hard copy) that meets Requirement R8. Evidence may include, but is not limited to: (1) dated reports of the discovery of a failure, (2) documentation noting the date the data recording was restored, (3) SCADA records, or (4) dated Corrective Action Plan transmittals to the Regional Entity and evidence of Corrective Action Plan implementation.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: "Compliance Enforcement Authority" means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Generator Owner shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation:

The Generator Owner shall retain evidence, as per Requirements R1 through R8, for three calendar years.

If a Generator Owner is found non-compliant, it shall keep information related to the non-compliance until mitigation is completed and approved or for the time specified above, whichever is longer.

The Compliance Enforcement Authority shall keep the last audit records, and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	Each Generator Owner as directed by Requirement R1 to have the required SER data had more than 80 percent, but less than 100 percent of the circuit breaker(s) identified in Requirement R1.	Each Generator Owner as directed by Requirement R1 to have the required SER data had more than 70 percent, but less than or equal to 80 percent of the circuit breaker(s) identified in Requirement R1.	Each Generator Owner as directed by Requirement R1 to have the required SER data had more than 60 percent, but less than or equal to 70 percent of the circuit breaker(s) identified in Requirement R1.	Each Generator Owner as directed by Requirement R1 to have the required SER data had less than or equal to 60 percent of the circuit breaker(s) identified in Requirement R1.
R2	The Generator Owner had FR data as directed by Requirement R2, Parts 2.1, 2.2, and 2.3 that covers more than 80 percent, but less than 100 percent of the total required electrical quantities, which is the product of the total number of monitored Elements and the number of specified electrical quantities for each Element.	The Generator Owner had FR data as directed by Requirement R2, Parts 2.1, 2.2, and 2.3 that covers more than 70 percent, but less than or equal to 80 percent of the total required electrical quantities, which is the product of the total number of monitored Elements and the number of specified electrical quantities for each Element.	The Generator Owner had FR data as directed by Requirement R2, Parts 2.1, 2.2, and 2.3 that covers more than 60 percent, but less than or equal to 70 percent of the total required electrical quantities, which is the product of the total number of monitored Elements and the number of specified electrical quantities for each Element.	The Generator Owner had FR data as directed by Requirement R2, Parts 2.1, 2.2, and 2.3 that covers less than or equal to 60 percent of the total required electrical quantities, which is the product of the total number of monitored Elements and the number of specified electrical quantities for each Element.
R3	The Generator Owner had FR data that meets more	The Generator Owner had FR data that meets more	The Generator Owner had FR data that meets more	The Generator Owner had FR data that meets less

	than 80 percent, but less than 100 percent of the total recording parameters as specified in Requirement R3.	than 70 percent, but less than or equal to 80 percent of the total recording parameters as specified in Requirement R3.	than 60 percent, but less than or equal to 70 percent of the total recording parameters as specified in Requirement R3.	than or equal to 60 percent of the total recording parameters as specified in Requirement R3.
R4	The Generator Owner had DDR data as directed by Requirement R4, Parts 4.1 through 4.4 that covered more than 80 percent, but less than 100 percent of the total required electrical quantities, which is the product of the total number of monitored Elements and the number of specified electrical quantities for each Element.	The Generator Owner had DDR data as directed by Requirement R4, Parts 4.1 through 4.4 for more than 70 percent, but less than or equal to 80 percent of the total required electrical quantities, which is the product of the total number of monitored Elements and the number of specified electrical quantities for each Element.	The Generator Owner had DDR data as directed by Requirement R4, Parts 4.1 through 4.4 for more than 60 percent, but less than or equal to 70 percent of the total required electrical quantities, which is the product of the total number of monitored Elements and the number of specified electrical quantities for each Element.	The Generator Owner had DDR data as directed by Requirement R4, Parts 4.1 through 4.4 for less than or equal to 60 percent of the total required electrical quantities, which is the product of the total number of monitored Elements and the number of specified electrical quantities for each Element.
R5	The Generator Owner had DDR data that meets more than 80 percent, but less than 100 percent of the total recording parameters as specified in Requirement R5.	The Generator Owner had DDR data that meets more than 70 percent, but less than or equal to 80 percent of the total recording properties as specified in Requirement R5.	The Generator Owner had DDR data that meets more than 60 percent, but less than or equal to 70 percent of the total recording properties as specified in Requirement R5.	The Generator Owner had DDR data that meets less than or equal to 60 percent of the total recording properties as specified in Requirement R5.

R6	The Generator Owner had time synchronized SER, FR, or DDR data per Requirement R6, Parts 6.1 and 6.2 for more than 90 percent, but less than 100 percent of the Elements.	The Generator Owner had time synchronized SER, FR, or DDR data per Requirement R6, Parts 6.1 and 6.2 for more than 80 percent, but less than or equal to 90 percent of the Elements.	The Generator Owner had time synchronized SER, FR, or DDR data per Requirement R6, Parts 6.1 and 6.2 for more than 70 percent, but less than or equal to 80 percent of the Elements.	The Generator Owner failed to have time synchronized SER, FR, or DDR data per Requirement R6, Parts 6.1 and 6.2 for less than or equal to 70 percent of the Elements.
R7	The Generator Owner as directed by Requirement R7 provided more than 90 percent, but less than 100 percent of the requested data. OR The Generator Owner as directed by Requirement R7, Part 7.2 provided the requested data one to 10 calendar days late. OR The Generator Owner as directed by Requirement R7, Parts 7.3 through 7.6 provided more than 90 percent of the data, but less than 100 percent of	The Generator Owner as directed by Requirement R7 provided more than 80 percent, but less than or equal to 90 percent of the requested data. OR The Generator Owner as directed by Requirement R7, Part 7.2 provided the requested data 11 to 20 calendar days late. OR The Generator Owner as directed by Requirement R7, Parts 7.3 through 7.6 provided more than 80 percent of the data, but less than or equal to 90 percent	The Generator Owner as directed by Requirement R7 provided more than 70 percent, but less than or equal to 80 percent of the requested data. OR The Generator Owner as directed by Requirement R7, Part 7.2 provided the requested data 21 to 30 calendar days late. OR The Generator Owner as directed by Requirement R7, Parts 7.3 through 7.6 provided more than 70 percent of the data, but less than or equal to 80	The Generator Owner as directed by Requirement R7 failed to provide less than or equal to 70 percent of the requested data. OR The Generator Owner as directed by Requirement R7, Part 7.2 provided the requested data more than 30 calendar days late. OR The Generator Owner as directed by Requirement R7, Parts 7.3 through 7.6 provided less than or equal to 70 percent of the data in the proper data format.

	the data in the proper data format.	of the data in the proper data format.	percent of the data in the proper data format.	
R8	The Generator Owner as directed by Requirement R8 was unable to restore recording capability within 90 calendar days and provided a Corrective Action Plan to the Regional Entity more than 90 calendar days, but less than or equal to 100 calendar days after discovery of the failure.	The Generator Owner as directed by Requirement R8 was unable to restore recording capability within 90 calendar days and provided a Corrective Action Plan to the Regional Entity more than 100 calendar days, but less than or equal to 110 calendar days after discovery of the failure.	The Generator Owner as directed by Requirement R8 was unable to restore recording capability within 90 calendar days and provided a Corrective Action Plan to the Regional Entity more than 110 calendar days, but less than or equal to 120 calendar days after discovery of the failure. OR The Generator Owner as directed by Requirement R8 submitted a Corrective Action Plan to the Regional Entity but failed to implement it.	The Generator Owner as directed by Requirement R8 was unable to restore recording capability within 90 calendar days and provided a Corrective Action Plan to the Regional Entity more than 120 calendar days after discovery of the failure. OR Generator Owner as directed by Requirement R8 failed to restore the recording capability within 90 calendar days and failed to submit a Corrective Action Plan to the Regional Entity.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

NERC Reliability Standard PRC-028-1: Implementation Plan.

NERC Reliability Standard PRC-028-1: Technical Rationale.

G. References

IEEE C37.111: Common format for transient data exchange (COMTRADE) for power Systems.

IEEE C37.232-2011: IEEE Standard for Common Format for Naming Time Sequence Data Files (COMNAME). Standard published 11/09/2011 by IEEE.

IEEE Std 2800-2022: IEEE Standard for Interconnection and Interoperability of Inverter-Based Resources (IBRs) Interconnecting with Associated Transmission Electric Power Systems.

Multiple Solar PV Disturbances in CAISO, Joint NERC and WECC Staff Report, April 2022.

NERC Reliability Standard PRC-002-5.

Odessa Disturbance, Texas Events: May 9, 2021 and June 26, 2021, Joint NERC and Texas RE Event Report, September 2021.

Odessa Disturbance, Texas Event: June 4, 2022, Joint NERC and Texas RE Event Report, December 2022.

Version History

Version	Date	Action	Change Tracking
1	October 8, 2024	Adopted by NERC Board of Trustees	

Attachment 1

Sequence of Events Recording (SER) Data Format

(Requirement R7, Part 7.3)

Date, Time, Local Time Code, Plant Name, Device[5], State[6]

08/27/23, 23:58:57.110, -5, Plant name 1, Breaker 1, Close

08/27/23, 23:58:57.082, -5, Plant name 2, Breaker 2, Close

08/27/23, 23:58:57.217, -5, Plant name 1, IBR unit 1, undervoltage ride-through mode

08/27/23, 23:58:57.214, -5, Plant name 2, IBR unit 2, dc overcurrent trip

[5] Device name may include specific names of breakers or IBR units as appropriate.

[6] Breaker status and any other terminology such as TRIP, TRIP TO LOCKOUT, RECLOSE, etc. is acceptable. For IBR unit level data, fault codes, alarms, change in operating mode etc., are also acceptable.

Appendix PRC-028-1-QC-1
Specific provisions applicable in Québec for standard PRC-028-1 – Disturbance Monitoring and Reporting Requirements for Inverter-Based Resources

This appendix establishes specific provisions for the application of the standard in Québec. Provisions of the standard and of this appendix must be read jointly for comprehension and interpretation purposes. Where the standard and appendix differ, the appendix shall prevail.

A. Introduction

1. Title: No specific provisions.

2. Number: No specific provisions.

3. Purpose: No specific provisions.

4. Applicability: In the application of this standard, all reference to the term "Bulk Electric System" or "BES" shall be replaced by the terms "Main Transmission System" or "RTP" respectively.

4.1. Functional Entities:

No specific provisions.

4.2. Facilities:

4.2.1 RTP Inverter-Based Ressources.

4.2.2 Non-RTP Inverter-Based Resources that either have or contribute to an aggregate nameplate capacity of greater than or equal to 50 MVA, connected through a system designed primarily for delivering such capacity to a common point of connection at a voltage greater than or equal to 44 kV.

5. Effective Date:

5.1.	Adoption of the standard by the Régie de l'énergie:	February 10, 2026
5.2.	Adoption of the appendix by the Régie de l'énergie:	February 10, 2026
5.3.	Effective date of the standard and its appendix in Québec:	July 1, 2026

Appendix PRC-028-1-QC-1
Specific provisions applicable in Québec for standard PRC-028-1 – Disturbance Monitoring and Reporting Requirements for Inverter-Based Resources

Requirements	Applicability	Date of enforcement in Québec
RTP Inverter-Based Resources		
R1 to R7	For RTP Inverter-Based Resources in commercial operation[1] on or before the effective date of PRC-028-1, entities shall comply at: • 50% of their RTP Inverter-Based Resources • 100% of their RTP Inverter-Based Resources • Entities that are required to monitor only one (1) RTP Inverter-Based Resource shall comply at 100% of their RTP Inverter-Based Resources	• Within three (3) calendar years of the effective date of PRC-028-1 • Five (5) years after PRC-028-1 approval by the Régie • Within three (3) calendar years of the effective date of PRC-028-1
	For RTP Inverter-Based Resources entering commercial operation after the effective date of PRC-028-1	Within 15 calendar months following the effective date of PRC-028-1 or the commercial operation date, whichever is later.
R8	Entities shall comply	No later than nine (9) months after the effective date of PRC-028-1

[1] Commercial operation means achievement of this designation indicating that the facility has received all approvals necessary for operation after completion of initial start-up testing.

Requirements	Applicability	Date of enforcement in Québec
Non-RTP Inverter-Based Resources		
R1 to R7	For non-RTP Inverter-Based Resources in commercial operation within 15 calendar months following approval of PRC-028-1 by the Régie, entities shall comply at 100% of their non-RTP Inverter-Based Resources	Five (5) years after approval of PRC-028-1 by the Régie
	For non-RTP Inverter-Based Resources in commercial operation after 15 calendar months following the approval by the Régie	Within 15 calendar months following the effective date of PRC-028-1 or the commercial operation date, whichever is later.
R8	Entities shall comply	Within two (2) calendar years of the effective date of PRC-028-1

Process for Requesting an Extension from Compliance Dates

Each *GO* that owns one or more applicable Inverter-Based Resources that are in commercial operation before the effective date of Reliability Standard PRC-028-1 may request an extension from the above-listed compliance dates if circumstances beyond its control prevent the installation of Disturbance Monitoring Equipment on one or more of its Inverter-Based Resources.

To request an extension, the entity shall develop and submit to its Compliance Enforcement Authority a request for extension that contains at a minimum the following information:

1. Identification of the Inverter-Based Resource(s) for which the entity requests the extension;

2. A plan for installing the Disturbance Monitoring Equipment and a timetable for completion;

3. A description of the circumstances precluding the timely installation of Disturbance Monitoring Equipment and how those circumstances are beyond the control of the entity; and

4. Any other information the entity deems relevant to the Compliance Enforcement Authority's consideration of its request.

Circumstances beyond the entity's control may include supply chain delays associated with the procurement, engineering, installation, or commissioning of disturbance monitoring equipment, inability to secure scheduled outages, or other exceptional circumstances outside the entity's control.

The entity shall provide any information requested by the Compliance Enforcement Authority to validate the information provided above, including any information specified by the Compliance Enforcement Authority in a supporting process document. If the extension request is granted, the

entity shall implement the plan in accordance with the provided timetable. Should additional time be required, the entity shall submit an updated request to its Compliance Enforcement Authority.

Requests should be submitted as soon as the entity identifies circumstances impeding the timely implementation of Reliability Standard PRC-028-1, but no later than three months prior to the compliance date for which the entity requests an extension.

B. Requirements and Measures

No specific provisions.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

In Québec, "Compliance Enforcement Authority" means the Régie de l'énergie in its roles of monitoring and enforcing compliance with respect to the Reliability Standard and to this appendix.

1.2. Evidence Retention

No specific provisions.

1.3. Compliance Monitoring and Enforcement Program

The Régie de l'énergie establishes the monitoring processes used to evaluate data or information for the purpose of determining compliance or non-compliance with the reliability standard and with this appendix.

Violation Severity Levels

No specific provisions.

D. Regional Variances

No specific provisions.

E. Interpretations

No specific provisions.

F. Associated Documents

No specific provisions.

G. References

No specific provisions.

Attachment 1

No specific provisions.

Version History

Version	Date	Action	Change Tracking
1	February 10, 2026	New Appendix as per decision D-2026-010.	New

A. Introduction

1. **Title:** Transmission Operations

2. **Number:** TOP-001-5

3. **Purpose:** To prevent instability, uncontrolled separation, or Cascading outages that adversely impact the reliability of the Interconnection by ensuring prompt action to prevent or mitigate such occurrences.

4. **Applicability:**

   4.1. Functional Entities:

   4.1.1. Balancing Authority

   4.1.2. Transmission Operator

   4.1.3. Generator Operator

   4.1.4. Distribution Provider

5. **Effective Date:** See Implementation Plan

B. Requirements and Measures

R1. Each Transmission Operator shall act to maintain the reliability of its Transmission Operator Area via its own actions or by issuing Operating Instructions. *[Violation Risk Factor: High][Time Horizon: Same-Day Operations, Real-time Operations]*

M1. Each Transmission Operator shall have and provide evidence which may include but is not limited to dated operator logs, dated records, dated and time-stamped voice recordings or dated transcripts of voice recordings, electronic communications, or equivalent documentation, that will be used to determine that it acted to maintain the reliability of its Transmission Operator Area via its own actions or by issuing Operating Instructions.

R2. Each Balancing Authority shall act to maintain the reliability of its Balancing Authority Area via its own actions or by issuing Operating Instructions. *[Violation Risk Factor: High][Time Horizon: Same-Day Operations, Real-time Operations]*

M2. Each Balancing Authority shall have and provide evidence which may include but is not limited to dated operator logs, dated records, dated and time-stamped voice recordings or dated transcripts of voice recordings, electronic communications, or equivalent documentation, that will be used to determine that it acted to maintain the reliability of its Balancing Authority Area via its own actions or by issuing Operating Instructions.

R3. Each Balancing Authority, Generator Operator, and Distribution Provider shall comply with each Operating Instruction issued by its Transmission Operator(s), unless such action cannot be physically implemented or it would violate safety, equipment, regulatory, or statutory requirements. *[Violation Risk Factor: High] [Time Horizon: Same-Day Operations, Real-Time Operations]*

M3. Each Balancing Authority, Generator Operator, and Distribution Provider shall make available upon request, evidence that it complied with each Operating Instruction issued by the Transmission Operator(s) unless such action could not be physically implemented or it would have violated safety, equipment, regulatory, or statutory requirements. Such evidence could include but is not limited to dated operator logs, voice recordings or transcripts of voice recordings, electronic communications, or other equivalent evidence in electronic or hard copy format. In such cases, the Balancing Authority, Generator Operator, and Distribution Provider shall have and provide copies of the safety, equipment, regulatory, or statutory requirements as evidence for not complying with the Transmission Operator's Operating Instruction. If such a situation has not occurred, the Balancing Authority, Generator Operator, or Distribution Provider may provide an attestation.

R4. Each Balancing Authority, Generator Operator, and Distribution Provider shall inform its Transmission Operator of its inability to comply with an Operating Instruction issued by its Transmission Operator. *[Violation Risk Factor: High] [Time Horizon: Same-Day Operations, Real-Time Operations]*

M4. Each Balancing Authority, Generator Operator, and Distribution Provider shall make available upon request, evidence which may include but is not limited to dated operator logs, voice recordings or transcripts of voice recordings, electronic communications, or equivalent evidence in electronic or hard copy format, that it informed its Transmission Operator of its inability to comply with its Operating Instruction issued. If such a situation has not occurred, the Balancing Authority, Generator Operator, or Distribution Provider may provide an attestation.

R5. Each Transmission Operator, Generator Operator, and Distribution Provider shall comply with each Operating Instruction issued by its Balancing Authority, unless such action cannot be physically implemented or it would violate safety, equipment, regulatory, or statutory requirements. *[Violation Risk Factor: High] [Time Horizon: Same-Day Operations, Real-Time Operations]*

M5. Each Transmission Operator, Generator Operator, and Distribution Provider shall make available upon request, evidence that it complied with each Operating Instruction issued by its Balancing Authority unless such action could not be physically implemented or it would have violated safety, equipment, regulatory, or statutory requirements. Such evidence could include but is not limited to dated operator logs, voice recordings or transcripts of voice recordings, electronic communications, or other equivalent evidence in electronic or hard copy format. In such cases, the Transmission Operator, Generator Operator, and Distribution Provider shall have and provide copies of the safety, equipment, regulatory, or statutory requirements as evidence for not complying with the Balancing Authority's Operating Instruction. If such a situation has not occurred, the Transmission Operator, Generator Operator, or Distribution Provider may provide an attestation.

R6. Each Transmission Operator, Generator Operator, and Distribution Provider shall inform its Balancing Authority of its inability to comply with an Operating Instruction issued by its Balancing Authority. *[Violation Risk Factor: High] [Time Horizon: Same-Day Operations, Real-Time Operations]*

M6. Each Transmission Operator, Generator Operator, and Distribution Provider shall make available upon request, evidence which may include but is not limited to dated operator logs, voice recordings or transcripts of voice recordings, electronic communications, or equivalent evidence in electronic or hard copy format, that it informed its Balancing Authority of its inability to comply with its Operating Instruction. If such a situation has not occurred, the Transmission Operator, Generator Operator, or Distribution Provider may provide an attestation.

R7. Each Transmission Operator shall assist other Transmission Operators within its Reliability Coordinator Area, if requested and able, provided that the requesting Transmission Operator has implemented its comparable Emergency procedures, unless such assistance cannot be physically implemented or would violate safety, equipment, regulatory, or statutory requirements. *[Violation Risk Factor: High] [Time Horizon: Real-Time Operations]*

M7. Each Transmission Operator shall make available upon request, evidence that comparable requested assistance, if able, was provided to other Transmission Operators within its Reliability Coordinator Area unless such assistance could not be physically implemented or would have violated safety, equipment, regulatory, or statutory requirements. Such evidence could include but is not limited to dated operator logs, voice recordings or transcripts of voice recordings, electronic communications, or other equivalent evidence in electronic or hard copy format. If no request for assistance was received, the Transmission Operator may provide an attestation.

R8. Each Transmission Operator shall inform its Reliability Coordinator, known impacted Balancing Authorities, and known impacted Transmission Operators of its actual or expected operations that result in, or could result in, an Emergency. *[Violation Risk Factor: High] [Time Horizon: Operations Planning, Same-Day Operations, Real-Time Operations]*

M8. Each Transmission Operator shall make available upon request, evidence that it informed its Reliability Coordinator, known impacted Balancing Authorities, and known impacted Transmission Operators of its actual or expected operations that result in, or could result in, an Emergency. Such evidence could include but is not limited to dated operator logs, voice recordings or transcripts of voice recordings, electronic communications, or other equivalent evidence. If no such situations have occurred, the Transmission Operator may provide an attestation.

R9. Each Balancing Authority and Transmission Operator shall notify its Reliability Coordinator and known impacted interconnected entities of all planned outages, and unplanned outages of 30 minutes or more, for telemetering and control equipment, monitoring and assessment capabilities, and associated communication channels between the affected entities. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning, Same-Day Operations, Real-Time Operations]*

M9. Each Balancing Authority and Transmission Operator shall make available upon request, evidence that it notified its Reliability Coordinator and known impacted interconnected entities of all planned outages, and unplanned outages of 30 minutes or more, for telemetering and control equipment, monitoring and assessment capabilities, and associated communication channels. Such evidence could include but is not limited to dated operator logs, voice recordings or transcripts of voice recordings, electronic communications, or other equivalent evidence. If such a situation has not occurred, the Balancing Authority or Transmission Operator may provide an attestation.

R10. Each Transmission Operator shall perform the following for determining System Operating Limit (SOL) exceedances within its Transmission Operator Area: *[Violation Risk Factor: High] [Time Horizon: Real-Time Operations]*

10.1. Monitor Facilities within its Transmission Operator Area;

10.2. Monitor the status of Remedial Action Schemes within its Transmission Operator Area;

10.3. Monitor non-BES facilities within its Transmission Operator Area identified as necessary by the Transmission Operator;

10.4. Obtain and utilize status, voltages, and flow data for Facilities outside its Transmission Operator Area identified as necessary by the Transmission Operator;

10.5. Obtain and utilize the status of Remedial Action Schemes outside its Transmission Operator Area identified as necessary by the Transmission Operator; and

10.6. Obtain and utilize status, voltages, and flow data for non-BES facilities outside its Transmission Operator Area identified as necessary by the Transmission Operator.

M10. Each Transmission Operator shall have, and provide upon request, evidence that could include but is not limited to Energy Management System description documents, computer printouts, Supervisory Control and Data Acquisition (SCADA) data collection, or other equivalent evidence that will be used to confirm that it monitored or obtained and utilized data as required to determine any System Operating Limit (SOL) exceedances within its Transmission Operator Area.

R11. Each Balancing Authority shall monitor its Balancing Authority Area, including the status of Remedial Action Schemes that impact generation or Load, in order to maintain generation-Load-interchange balance within its Balancing Authority Area and support Interconnection frequency. *[Violation Risk Factor: High] [Time Horizon: Real-Time Operations]*

M11. Each Balancing Authority shall have, and provide upon request, evidence that could include but is not limited to Energy Management System description documents, computer printouts, SCADA data collection, or other equivalent evidence that will be used to confirm that it monitors its Balancing Authority Area, including the status of Remedial Action Schemes that impact generation or Load, in order to maintain generation-Load-interchange balance within its Balancing Authority Area and support Interconnection frequency.

R12. Each Transmission Operator shall not operate outside any identified Interconnection Reliability Operating Limit (IROL) for a continuous duration exceeding its associated IROL T_V. *[Violation Risk Factor: High] [Time Horizon: Real-time Operations]*

M12. Each Transmission Operator shall make available evidence to show that for any occasion in which it operated outside any identified Interconnection Reliability Operating Limit (IROL), the continuous duration did not exceed its associated IROL T_V. Such evidence could include but is not limited to dated computer logs or reports in electronic or hard copy format specifying the date, time, duration, and details of the

excursion. If such a situation has not occurred, the Transmission Operator may provide an attestation that an event has not occurred.

R13. Each Transmission Operator shall ensure that a Real-time Assessment is performed at least once every 30 minutes. *[Violation Risk Factor: High] [Time Horizon: Real-time Operations]*

M13. Each Transmission Operator shall have, and make available upon request, evidence to show it ensured that a Real-Time Assessment was performed at least once every 30 minutes. This evidence could include but is not limited to dated computer logs showing times the assessment was conducted, dated checklists, or other evidence.

R14. Each Transmission Operator shall initiate its Operating Plan to mitigate a SOL exceedance identified as part of its Real-time monitoring or Real-time Assessment. *[Violation Risk Factor: High] [Time Horizon: Real-time Operations]*

M14. Each Transmission Operator shall have evidence that it initiated its Operating Plan for mitigating SOL exceedances identified as part of its Real-time monitoring or Real-time Assessments. This evidence could include but is not limited to dated computer logs showing times the Operating Plan was initiated, dated checklists, or other evidence.

R15. Each Transmission Operator shall inform its Reliability Coordinator of actions taken to return the System to within limits when a SOL has been exceeded. *[Violation Risk Factor: Medium] [Time Horizon: Real-Time Operations]*

M15. Each Transmission Operator shall make available evidence that it informed its Reliability Coordinator of actions taken to return the System to within limits when a SOL was exceeded. Such evidence could include but is not limited to dated operator logs, voice recordings or transcripts of voice recordings, or dated computer printouts. If such a situation has not occurred, the Transmission Operator may provide an attestation.

R16. Each Transmission Operator shall provide its System Operators with the authority to approve planned outages and maintenance of its telemetering and control equipment, monitoring and assessment capabilities, and associated communication channels between affected entities. *[Violation Risk Factor: High] [Time Horizon: Operations Planning, Same-Day Operations, Real-time Operations]*

M16. Each Transmission Operator shall have, and provide upon request, evidence that could include but is not limited to a documented procedure or equivalent evidence that will be used to confirm that the Transmission Operator has provided its System Operators with the authority to approve planned outages and maintenance of telemetering and control equipment, monitoring and assessment capabilities, and associated communication channels between affected entities.

R17. Each Balancing Authority shall provide its System Operators with the authority to approve planned outages and maintenance of its telemetering and control equipment, monitoring and assessment capabilities, and associated communication

channels between affected entities. *[Violation Risk Factor: High] [Time Horizon: Operations Planning, Same-Day Operations, Real-time Operations]*

M17. Each Balancing Authority shall have, and provide upon request, evidence that could include but is not limited to a documented procedure or equivalent evidence that will be used to confirm that the Balancing Authority has provided its System Operators with the authority to approve planned outages and maintenance of its telemetering and control equipment, monitoring and assessment capabilities, and associated communication channels between affected entities.

R18. Each Transmission Operator shall operate to the most limiting parameter in instances where there is a difference in SOLs. [*Violation Risk Factor: High] [Time Horizon: Operations Planning, Same-Day Operations, Real-time Operations]*

M18. Each Transmission Operator shall have, and provide upon request, evidence that could include but is not limited to operator logs, voice recordings, electronic communications, or equivalent evidence that will be used to determine if it operated to the most limiting parameter in instances where there is a difference in SOLs.

R19. Reserved.

M19. Reserved.

R20. Each Transmission Operator shall have data exchange capabilities, with redundant and diversely routed data exchange infrastructure within the Transmission Operator's primary Control Center, for the exchange of Real-time data with its Reliability Coordinator, Balancing Authority, and the entities it has identified it needs data from in order for it to perform its Real-time monitoring and Real-time Assessments. *[Violation Risk Factor: High] [Time Horizon: Same-Day Operations, Real-time Operations]*

M20. Each Transmission Operator shall have, and provide upon request, evidence that could include, but is not limited to, system specifications, system diagrams, or other documentation that lists its data exchange capabilities, including redundant and diversely routed data exchange infrastructure within the Transmission Operator's primary Control Center, for the exchange of Real-time data with its Reliability Coordinator, Balancing Authority, and the entities it has identified it needs data from in order to perform its Real-time monitoring and Real-time Assessments as specified in the requirement.

R21. Each Transmission Operator shall test its primary Control Center data exchange capabilities specified in Requirement R20 for redundant functionality at least once every 90 calendar days. If the test is unsuccessful, the Transmission Operator shall initiate action within two hours to restore redundant functionality. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M21. Each Transmission Operator shall have, and provide upon request, evidence that it tested its primary Control Center data exchange capabilities specified in Requirement R20 for the redundant functionality, or experienced an event that demonstrated the

redundant functionality; and, if the test was unsuccessful, initiated action within two hours to restore redundant functionality as specified in Requirement R21. Evidence could include, but is not limited to: dated and time-stamped test records, operator logs, voice recordings, or electronic communications.

R22. Reserved.

M22. Reserved.

R23. Each Balancing Authority shall have data exchange capabilities, with redundant and diversely routed data exchange infrastructure within the Balancing Authority's primary Control Center, for the exchange of Real-time data with its Reliability Coordinator, Transmission Operator, and the entities it has identified it needs data from in order for it to perform its Real-time monitoring and analysis functions. *[Violation Risk Factor: High] [Time Horizon: Same-Day Operations, Real-time Operations]*

M23. Each Balancing Authority shall have, and provide upon request, evidence that could include, but is not limited to, system specifications, system diagrams, or other documentation that lists its data exchange capabilities, including redundant and diversely routed data exchange infrastructure within the Balancing Authority's primary Control Center, for the exchange of Real-time data with its Reliability Coordinator, Transmission Operator, and the entities it has identified it needs data from in order to perform its Real-time monitoring and analysis functions as specified in the requirement.

R24. Each Balancing Authority shall test its primary Control Center data exchange capabilities specified in Requirement R23 for redundant functionality at least once every 90 calendar days. If the test is unsuccessful, the Balancing Authority shall initiate action within two hours to restore redundant functionality. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M24. Each Balancing Authority shall have, and provide upon request, evidence that it tested its primary Control Center data exchange capabilities specified in Requirement R23 for redundant functionality, or experienced an event that demonstrated the redundant functionality; and, if the test was unsuccessful, initiated action within two hours to restore redundant functionality as specified in Requirement R24. Evidence could include, but is not limited to: dated and time-stamped test records, operator logs, voice recordings, or electronic communications.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority:

"Compliance Enforcement Authority" means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention:

The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

- Each Balancing Authority, Transmission Operator, Generator Operator, and Distribution Provider shall each keep data or evidence for each applicable Requirement R1 through R11, and Measure M1 through M11, for the current calendar year and one previous calendar year, with the exception of operator logs and voice recordings which shall be retained for a minimum of 90 calendar days, unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.
- Each Transmission Operator shall retain evidence for three calendar years of any occasion in which it has exceeded an identified IROL and its associated IROL T_v as specified in Requirement R12 and Measure M12.
- Each Transmission Operator shall keep data or evidence for Requirement R13 and Measure M13 for a rolling 30-day period, unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.
- Each Transmission Operator shall retain evidence and that it initiated its Operating Plan to mitigate a SOL exceedance as specified in Requirement R14 and Measurement M14 for three calendar years.
- Each Transmission Operator and Balancing Authority shall each keep data or evidence for each applicable Requirement R15 through R18, and Measure M15 through M18 for the current calendar year and one previous calendar year, with the exception of operator logs and voice recordings which shall be retained for a minimum of 90 calendar days.

- Each Transmission Operator shall keep data or evidence for Requirement R20 and Measure M20 for the current calendar year and one previous calendar year.
- Each Transmission Operator shall keep evidence for Requirement R21 and Measure M21 for the most recent twelve calendar months, with the exception of operator logs and voice recordings which shall be retained for a minimum of 90 calendar days.
- Each Balancing Authority shall keep data or evidence for Requirement R23 and Measure M23 for the current calendar year and one previous calendar year.
- Each Balancing Authority shall keep evidence for Requirement R24 and Measure M24 for the most recent twelve calendar months, with the exception of operator logs and voice recordings which shall be retained for a minimum of 90 calendar days.

1.3. Compliance Monitoring and Enforcement Program

As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	N/A	N/A	N/A	The Transmission Operator failed to act to maintain the reliability of its Transmission Operator Area via its own actions or by issuing Operating Instructions.
R2.	N/A	N/A	N/A	The Balancing Authority failed to act to maintain the reliability of its Balancing Authority Area via its own actions or by issuing Operating Instructions.
R3.	N/A	N/A	N/A	The responsible entity did not comply with an Operating Instruction issued by the Transmission Operator, and such action could have been physically implemented and would not have violated safety, equipment, regulatory, or statutory requirements.
R4.	N/A	N/A	N/A	The responsible entity did not inform its Transmission Operator of its inability to

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				comply with an Operating Instruction issued by its Transmission Operator.
R5.	N/A	N/A	N/A	The responsible entity did not comply with an Operating Instruction issued by the Balancing Authority, and such action could have been physically implemented and would not have violated safety, equipment, regulatory, or statutory requirements.
R6.	N/A	N/A	N/A	The responsible entity did not inform its Balancing Authority of its inability to comply with an Operating Instruction issued by its Balancing Authority.
R7.	N/A	N/A	N/A	The Transmission Operator did not provide comparable assistance to other Transmission Operators within its Reliability Coordinator Area, when requested and able, and the

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				requesting entity had implemented its Emergency procedures, and such actions could have been physically implemented and would not have violated safety, equipment, regulatory, or statutory requirements.
R8.	The Transmission Operator did not inform one known impacted Transmission Operator or 5% or less of the known impacted Transmission Operators, whichever is greater, of its actual or expected operations that resulted in, or could have resulted in, an Emergency on respective Transmission Operator Areas. OR, The Transmission Operator did not inform one known impacted	The Transmission Operator did not inform two known impacted Transmission Operators or more than 5% and less than or equal to 10% of the known impacted Transmission Operators, whichever is greater, of its actual or expected operations that resulted in, or could have resulted in, an Emergency on respective Transmission Operator Areas. OR, The Transmission Operator did not inform two known impacted Balancing	The Transmission Operator did not inform three known impacted Transmission Operators or more than 10% and less than or equal to 15% of the known impacted Transmission Operators, whichever is greater, of its actual or expected operations that resulted in, or could have resulted in, an Emergency on respective Transmission Operator Areas. OR, The Transmission Operator did not inform three known impacted Balancing	The Transmission Operator did not inform its Reliability Coordinator of its actual or expected operations that resulted in, or could have resulted in, an Emergency on those respective Transmission Operator Areas. OR The Transmission Operator did not inform four or more known impacted Transmission Operators or more than 15% of the known impacted Transmission Operators of its actual or expected

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	Balancing Authorities or 5% or less of the known impacted Balancing Authorities, whichever is greater, of its actual or expected operations that resulted in, or could have resulted in, an Emergency on respective Balancing Authority Areas.	Authorities or more than 5% and less than or equal to 10% of the known impacted Balancing Authorities, whichever is greater, of its actual or expected operations that resulted in, or could have resulted in, an Emergency on respective Balancing Authority Areas.	Authorities or more than 10% and less than or equal to 15% of the known impacted Balancing Authorities, whichever is greater, of its actual or expected operations that resulted in, or could have resulted in, an Emergency on respective Balancing Authority Areas.	operations that resulted in, or could have resulted in, an Emergency on those respective Transmission Operator Areas. OR, The Transmission Operator did not inform four or more known impacted Balancing Authorities or more than 15% of the known impacted Balancing Authorities of its actual or expected operations that resulted in, or could have resulted in, an Emergency on respective Balancing Authority Areas.
R9.	The responsible entity did not notify one known impacted interconnected entity or 5% or less of the known impacted entities, whichever is greater, of a planned outage, or an unplanned outage of 30 minutes or more, for telemetering and control	The responsible entity did not notify two known impacted interconnected entities or more than 5% and less than or equal to 10% of the known impacted entities, whichever is greater, of a planned outage, or an unplanned outage of 30	The responsible entity did not notify three known impacted interconnected entities or more than 10% and less than or equal to 15% of the known impacted entities, whichever is greater, of a planned outage, or an unplanned outage of 30	The responsible entity did not notify its Reliability Coordinator of a planned outage, or an unplanned outage of 30 minutes or more, for telemetering and control equipment, monitoring and assessment capabilities, and associated communication channels.

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	equipment, monitoring and assessment capabilities, or associated communication channels between the affected entities.	minutes or more, for telemetering and control equipment, monitoring and assessment capabilities, or associated communication channels between the affected entities.	minutes or more, for telemetering and control equipment, monitoring and assessment capabilities, or associated communication channels between the affected entities.	OR, The responsible entity did not notify four or more known impacted interconnected entities or more than 15% of the known impacted entities, whichever is greater, of a planned outage, or an unplanned outage of 30 minutes or more, for telemetering and control equipment, monitoring and assessment capabilities, or associated communication channels between the affected entities.
R10.	The Transmission Operator did not monitor, obtain, or utilize one of the items required or identified as necessary by the Transmission Operator and listed in Requirement R10, Part 10.1 through 10.6.	The Transmission Operator did not monitor, obtain, or utilize two of the items required or identified as necessary by the Transmission Operator and listed in Requirement R10, Part 10.1 through 10.6.	The Transmission Operator did not monitor, obtain, or utilize three of the items required or identified as necessary by the Transmission Operator and listed in Requirement R10, Part 10.1 through 10.6.	The Transmission Operator did not monitor, obtain, or utilize four or more of the items required or identified as necessary by the Transmission Operator and listed in Requirement R10 Part 10.1 through 10.6.

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R11.	N/A	N/A	The Balancing Authority did not monitor the status of Remedial Action Schemes that impact generation or Load, in order to maintain generation-Load-interchange balance within its Balancing Authority Area and support Interconnection frequency.	The Balancing Authority did not monitor its Balancing Authority Area, in order to maintain generation-Load-interchange balance within its Balancing Authority Area and support Interconnection frequency.
R12.	N/A	N/A	N/A	The Transmission Operator exceeded an identified Interconnection Reliability Operating Limit (IROL) for a continuous duration greater than its associated IROL T_V.
R13.	For any sample 24-hour period within the 30-day retention period, the Transmission Operator's Real-time Assessment was not conducted for one 30-minute period within that 24-hour period.	For any sample 24-hour period within the 30-day retention period, the Transmission Operator's Real-time Assessment was not conducted for two 30-minute periods within that 24-hour period.	For any sample 24-hour period within the 30-day retention period, the Transmission Operator's Real-time Assessment was not conducted for three 30-minute periods within that 24-hour period.	For any sample 24-hour period within the 30-day retention period, the Transmission Operator's Real-time Assessment was not conducted for four or more 30-minute periods within that 24-hour period.
R14.	N/A	N/A	N/A	The Transmission Operator did not initiate its Operating

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				Plan for mitigating a SOL exceedance identified as part of its Real-time monitoring or Real-time Assessment
R15.	N/A	N/A	N/A	The Transmission Operator did not inform its Reliability Coordinator of actions taken to return the System to within limits when a SOL had been exceeded.
R16.	N/A	N/A	N/A	The Transmission Operator did not provide its System Operators with the authority to approve planned outages and maintenance of its telemetering and control equipment, monitoring and assessment capabilities, and associated communication channels between affected entities.
R17.	N/A	N/A	N/A	The Balancing Authority did not provide its System Operators with the

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				authority to approve planned outages and maintenance of its telemetering and control equipment, monitoring and assessment capabilities, and associated communication channels between affected entities.
R18.	N/A	N/A	N/A	The Transmission Operator failed to operate to the most limiting parameter in instances where there was a difference in SOLs.
R19. Reserved.				
R20.	N/A	N/A	The Transmission Operator had data exchange capabilities with its Reliability Coordinator, Balancing Authority, and identified entities for performing Real-time monitoring and Real-time Assessments, but did not have redundant and	The Transmission Operator did not have data exchange capabilities with its Reliability Coordinator, Balancing Authority, and identified entities for performing Real-time monitoring and Real-time Assessments as specified in the Requirement.

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			diversely routed data exchange infrastructure within the Transmission Operator's primary Control Center, as specified in the Requirement.	
R21.	The Transmission Operator tested its primary Control Center data exchange capabilities specified in Requirement R20 for redundant functionality, but did so more than 90 calendar days but less than or equal to 120 calendar days since the previous test; OR The Transmission Operator tested its primary Control Center data exchange capabilities specified in Requirement R20 for redundant functionality at least once every 90 calendar days	The Transmission Operator tested its primary Control Center data exchange capabilities specified in Requirement R20 for redundant functionality, but did so more than 120 calendar days but less than or equal to 150 calendar days since the previous test; OR The Transmission Operator tested its primary Control Center data exchange capabilities specified in Requirement R20 for redundant functionality at least once every 90 calendar days but, following an unsuccessful test, initiated action to restore the	The Transmission Operator tested its primary Control Center data exchange capabilities specified in Requirement R20 for redundant functionality, but did so more than 150 calendar days but less than or equal to 180 calendar days since the previous test; OR The Transmission Operator tested its primary Control Center data exchange capabilities specified in Requirement R20 for redundant functionality at least once every 90 calendar days but, following an unsuccessful test, initiated action to restore the	The Transmission Operator tested its primary Control Center data exchange capabilities specified in Requirement R20 for redundant functionality, but did so more than 180 calendar days since the previous test; OR The Transmission Operator did not test its primary Control Center data exchange capabilities specified in Requirement R20 for redundant functionality; OR

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	but, following an unsuccessful test, initiated action to restore the redundant functionality in more than 2 hours and less than or equal to 4 hours.	redundant functionality in more than 4 hours and less than or equal to 6 hours.	redundant functionality in more than 6 hours and less than or equal to 8 hours.	The Transmission Operator tested its primary Control Center data exchange capabilities specified in Requirement R20 for redundant functionality at least once every 90 calendar days but, following an unsuccessful test, did not initiate action within 8 hours to restore the redundant functionality.
R22. Reserved.				
R23.	N/A	N/A	The Balancing Authority had data exchange capabilities with its Reliability Coordinator, Transmission Operator, and identified entities for performing Real-time monitoring and analysis functions, but did not have redundant and diversely routed data exchange infrastructure within the Balancing	The Balancing Authority did not have data exchange capabilities with its Reliability Coordinator, Transmission Operator, and identified entities for performing Real-time monitoring and analysis functions as specified in the Requirement.

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			Authority's primary Control Center, as specified in the Requirement.	
R24.	The Balancing Authority tested its primary Control Center data exchange capabilities specified in Requirement R23 for redundant functionality, but did so more than 90 calendar days but less than or equal to 120 calendar days since the previous test; OR The Balancing Authority tested its primary Control Center data exchange capabilities specified in Requirement R23 for redundant functionality at least once every 90 calendar days but, following an unsuccessful test, initiated action to restore the redundant functionality in more than	The Balancing Authority tested its primary Control Center data exchange capabilities specified in Requirement R23 for redundant functionality, but did so more than 120 calendar days but less than or equal to 150 calendar days since the previous test; OR The Balancing Authority tested its primary Control Center data exchange capabilities specified in Requirement R23 for redundant functionality at least once every 90 calendar days but, following an unsuccessful test, initiated action to restore the redundant functionality in	The Balancing Authority tested its primary Control Center data exchange capabilities specified in Requirement R23 for redundant functionality, but did so more than 150 calendar days but less than or equal to 180 calendar days since the previous test; OR The Balancing Authority tested its primary Control Center data exchange capabilities specified in Requirement R23 for redundant functionality at least once every 90 calendar days but, following an unsuccessful test, initiated action to restore the redundant functionality in	The Balancing Authority tested its primary Control Center data exchange capabilities specified in Requirement R23 for redundant functionality, but did so more than 180 calendar days since the previous test; OR The Balancing Authority did not test its primary Control Center data exchange capabilities specified in Requirement R23 for redundant functionality; OR The Balancing Authority tested its primary Control Center data exchange capabilities specified in Requirement R23 for

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	2 hours and less than or equal to 4 hours.	more than 4 hours and less than or equal to 6 hours.	more than 6 hours and less than or equal to 8 hours.	redundant functionality at least once every 90 calendar days but, following an unsuccessful test, did not initiate action within 8 hours to restore the redundant functionality.

D. Regional Variances

None.

E. Associated Documents

The Project 2014-03 SDT has created the SOL Exceedance White Paper as guidance on SOL issues and the URL for that document is: http://www.nerc.com/pa/stand/Pages/TOP0013RI.aspx.

Operating Plan - An Operating Plan includes general Operating Processes and specific Operating Procedures. It may be an overview document which provides a prescription for an Operating Plan for the next-day, or it may be a specific plan to address a specific SOL or IROL exceedance identified in the Operational Planning Analysis (OPA). Consistent with the NERC definition, Operating Plans can be general in nature, or they can be specific plans to address specific reliability issues. The use of the term Operating Plan in the revised TOP/IRO standards allows room for both. An Operating Plan references processes and procedures, including electronic data exchange, which are available to the System Operator on a daily basis to allow the operator to reliably address conditions which may arise throughout the day. It is valid for tomorrow, the day after, and the day after that. Operating Plans should be augmented by temporary operating guides which outline prevention/mitigation plans for specific situations which are identified day-to-day in an OPA or a Real-time Assessment (RTA). As the definition in the Glossary of Terms states, a restoration plan is an example of an Operating Plan. It contains all the overarching principles that the System Operator needs to work his/her way through the restoration process. It is not a specific document written for a specific blackout scenario but rather a collection of tools consisting of processes, procedures, and automated software systems that are available to the operator to use in restoring the system. An Operating Plan can in turn be looked upon in a similar manner. It does not contain a prescription for the specific set-up for tomorrow but contains a treatment of all the processes, procedures, and automated software systems that are at the operator's disposal. The existence of an Operating Plan, however, does not preclude the need for creating specific action plans for specific SOL or IROL exceedances identified in the OPA. When a Reliability Coordinator performs an OPA, the analysis may reveal instances of possible SOL or IROL exceedances for pre- or post-Contingency conditions. In these instances, Reliability Coordinators are expected to ensure that there are plans in place to prevent or mitigate those SOLs or IROLs, should those operating conditions be encountered the next day. The Operating Plan may contain a description of the process by which specific prevention or mitigation plans for day-to-day SOL or IROL exceedances identified in the OPA are handled and communicated. This approach could alleviate any potential administrative burden associated with perceived requirements for continual day-to-day updating of "the Operating Plan document" for compliance purposes.

Version History

Version	Date	Action	Change Tracking
0	April 1, 2005	Effective Date	New
0	August 8, 2005	Removed "Proposed" from Effective Date	Errata
1	November 1, 2006	Adopted by Board of Trustees	Revised
1a	May 12, 2010	Added Appendix 1 – Interpretation of R8 approved by Board of Trustees on May 12, 2010	Interpretation
1a	September 15, 2011	FERC Order issued approved the Interpretation of R8 (FERC Order became effective November 21, 2011)	Interpretation
2	May 6, 2012	Revised under Project 2007-03	Revised
2	May 9, 2012	Adopted by Board of Trustees	Revised
3	February 12, 2015	Adopted by Board of Trustees	Revisions under Project 2014-03
3	November 19, 2015	FERC approved TOP-001-3. Docket No. RM15-16-000. Order No. 817.	Approved
4	February 9, 2017	Adopted by Board of Trustees	Revised
4	April 17, 2017	FERC letter Order approved TOP-001-4. Docket No. RD17-4-000	
5	May 9, 2019	Adopted by Board of Trustees	R19 and R22 retired under Project 2018-03 Standards Efficiency Review Retirements
5	September 17, 2020	FERC Order issued approving TOP-001-5. Docket No. RM19-16-000, RM19-17-000	

Guidelines and Technical Basis

None.

Rationale

Rationale text from the development of TOP-001-3 in Project 2014-03 and TOP-001-4 in Project 2016-01 follows. Additional information can be found on the Project 2014-03 and Project 2016-01 pages.

Rationale for Requirement R3:
The phrase 'cannot be physically implemented' means that a Transmission Operator may request something to be done that is not physically possible due to its lack of knowledge of the system involved.

Rationale for Requirement R10:
New proposed Requirement R10 is derived from approved IRO-003-2, Requirement R1, adapted to the Transmission Operator Area. This new requirement is in response to NOPR paragraph 60 concerning monitoring capabilities for the Transmission Operator. New Requirement R11 covers the Balancing Authorities. Monitoring of external systems can be accomplished via data links.

The revised requirement addresses directives for Transmission Operator (TOP) monitoring of some non-Bulk Electric System (BES) facilities as necessary for determining System Operating Limit (SOL) exceedances (FERC Order No. 817 Para 35-36). The proposed requirement corresponds with approved IRO-002-4 Requirement R4 (proposed IRO-002-5 Requirement R5), which specifies the Reliability Coordinator's (RC) monitoring responsibilities for determining SOL exceedances.

The intent of the requirement is to ensure that all facilities (i.e., BES and non-BES) that can adversely impact reliability of the BES are monitored. As used in TOP and IRO Reliability Standards, monitoring involves observing operating status and operating values in Real-time for awareness of system conditions. The facilities that are necessary for determining SOL exceedances should be either designated as part of the BES, or otherwise be incorporated into monitoring when identified by planning and operating studies such as the Operational Planning Analysis (OPA) required by TOP-002-4 Requirement R1 and IRO-008-2 Requirement R1. The SDT recognizes that not all non-BES facilities that a TOP considers necessary for its monitoring needs will need to be included in the BES.

The non-BES facilities that the TOP is required to monitor are only those that are necessary for the TOP to determine SOL exceedances within its Transmission Operator Area. TOPs perform various analyses and studies as part of their functional obligations that could lead to identification of non-BES facilities that should be monitored for determining SOL exceedances. Examples include:

- OPA;
- Real-time Assessments (RTA);

- Analysis performed by the TOP as part of BES Exception processing for including a facility in the BES; and
- Analysis which may be specified in the RC's outage coordination process that leads the TOP to identify a non-BES facility that should be temporarily monitored for determining SOL exceedances.

TOP-003-3 Requirement R1 specifies that the TOP shall develop a data specification which includes data and information needed by the TOP to support its OPAs, Real-time monitoring, and RTAs. This includes non-BES data and external network data as deemed necessary by the TOP.

The format of the proposed requirement has been changed from the approved standard to more clearly indicate which monitoring activities are required to be performed.

Rationale for Requirement R13:
The new Requirement R13 is in response to NOPR paragraphs 55 and 60 concerning Real-time analysis responsibilities for Transmission Operators and is copied from approved IRO-008-1, Requirement R2. The Transmission Operator's Operating Plan will describe how to perform the Real-time Assessment. The Operating Plan should contain instructions as to how to perform Operational Planning Analysis and Real-time Assessment with detailed instructions and timing requirements as to how to adapt to conditions where processes, procedures, and automated software systems are not available (if used). This could include instructions such as an indication that no actions may be required if system conditions have not changed significantly and that previous Contingency analysis or Real-time Assessments may be used in such a situation.

Rationale for Requirement R14:
The original Requirement R8 was deleted and original Requirements R9 and R11 were revised in order to respond to NOPR paragraph 42 which raised the issue of handling all SOLs and not just a sub-set of SOLs. The SDT has developed a white paper on SOL exceedances that explains its intent on what needs to be contained in such an Operating Plan. These Operating Plans are developed and documented in advance of Real-time and may be developed from Operational Planning Assessments required per proposed TOP-002-4 or other assessments. Operating Plans could be augmented by temporary operating guides which outline prevention/mitigation plans for specific situations which are identified day-to-day in an Operational Planning Assessment or a Real-time Assessment. The intent is to have a plan and philosophy that can be followed by an operator.

Rationale for Requirements R16 and R17:
In response to IERP Report recommendation 3 on authority.

Rationale for Requirement R18:
Moved from approved IRO-005-3.1a, Requirement R10. Transmission Service Provider, Distribution Provider, Load-Serving Entity, Generator Operator, and Purchasing-Selling Entity are deleted as those entities will receive instructions on limits from the responsible entities cited in the requirement. Note – Derived limits replaced by SOLs for clarity and specificity. SOLs include voltage, Stability, and thermal limits and are thus the most limiting factor.

Rationale for Requirements R19 and R20 (R19, R20, R22, and R23 in TOP-001-4):
[Note: Requirement R19 proposed for retirement under Project 2018-03 Standards Efficiency Review Retirements.]

The proposed changes address directives for redundancy and diverse routing of data exchange capabilities (FERC Order No. 817 Para 47).

Redundant and diversely routed data exchange capabilities consist of data exchange infrastructure components (e.g., switches, routers, servers, power supplies, and network cabling and communication paths between these components in the primary Control Center for the exchange of system operating data) that will provide continued functionality despite failure or malfunction of an individual component within the Transmission Operator's (TOP) primary Control Center. Redundant and diversely routed data exchange capabilities preclude single points of failure in primary Control Center data exchange infrastructure from halting the flow of Real-time data. Requirement R20 does not require automatic or instantaneous fail-over of data exchange capabilities. Redundancy and diverse routing may be achieved in various ways depending on the arrangement of the infrastructure or hardware within the TOP's primary Control Center.

The reliability objective of redundancy is to provide for continued data exchange functionality during outages, maintenance, or testing of data exchange infrastructure. For periods of planned or unplanned outages of individual data exchange components, the proposed requirements do not require additional redundant data exchange infrastructure components solely to provide for redundancy.

Infrastructure that is not within the TOP's primary Control Center is not addressed by the proposed requirement.

Rationale for Requirement R21:
The proposed requirement addresses directives for testing of data exchange capabilities used in primary Control Centers (FERC Order No. 817 Para 51).

A test for redundant functionality demonstrates that data exchange capabilities will continue to operate despite the malfunction or failure of an individual component (e.g., switches, routers, servers, power supplies, and network cabling and communication paths between these components in the primary Control Center for the exchange of system operating data). An entity's testing practices should, over time, examine the various failure modes of its data

exchange capabilities. When an actual event successfully exercises the redundant functionality, it can be considered a test for the purposes of the proposed requirement.

Rationale for Requirements R22 and R23:
[Note: Requirement R22 proposed for retirement under Project 2018-03 Standards Efficiency Review Retirements]

The proposed changes address directives for redundancy and diverse routing of data exchange capabilities (FERC Order No. 817 Para 47).

Redundant and diversely routed data exchange capabilities consist of data exchange infrastructure components (e.g., switches, routers, servers, power supplies, and network cabling and communication paths between these components in the primary Control Center for the exchange of system operating data) that will provide continued functionality despite failure or malfunction of an individual component within the Balancing Authority's (BA) primary Control Center. Redundant and diversely routed data exchange capabilities preclude single points of failure in primary Control Center data exchange infrastructure from halting the flow of Real-time data. Requirement R23 does not require automatic or instantaneous fail-over of data exchange capabilities. Redundancy and diverse routing may be achieved in various ways depending on the arrangement of the infrastructure or hardware within the BA's primary Control Center.

The reliability objective of redundancy is to provide for continued data exchange functionality during outages, maintenance, or testing of data exchange infrastructure. For periods of planned or unplanned outages of individual data exchange components, the proposed requirements do not require additional redundant data exchange infrastructure components solely to provide for redundancy.

Infrastructure that is not within the BA's primary Control Center is not addressed by the proposed requirement.

Rationale for Requirement R24:
The proposed requirement addresses directives for testing of data exchange capabilities used in primary Control Centers (FERC Order No. 817 Para 51).

A test for redundant functionality demonstrates that data exchange capabilities will continue to operate despite the malfunction or failure of an individual component(e.g., switches, routers, servers, power supplies, and network cabling and communication paths between these components in the primary Control Center for the exchange of system operating data). An entity's testing practices should, over time, examine the various failure modes of its data exchange capabilities. When an actual event successfully exercises the redundant functionality, it can be considered a test for the purposes of the proposed requirement.

Appendix TOP-001-5-QC-1

Specific provisions applicable in Québec for standard TOP-001-5 – Transmission Operations

This appendix establishes specific provisions for the application of the standard in Québec. Provisions of the standard and of this appendix must be read jointly for comprehension and interpretation purposes. Where the standard and appendix differ, the appendix shall prevail.

A. Introduction

1. Title: No specific provisions.

2. Number: No specific provisions.

3. Purpose: No specific provisions.

4. Applicability:

4.1. Functional Entities

No specific provisions.

The applicable facilities for Requirement R10.1 of this standard are the facilities of the Main Transmission System (RTP), and for Requirements R10.3 to R10.6, the facilities designated under these requirements.

5. Effective date:

5.1. Adoption of the standard by the Régie de l'énergie: March 10, 2022

5.2. Adoption of this appendix by the Régie de l'énergie: March 10, 2022

5.3. Effective date of the standard and of this appendix in Québec: July 1st, 2023

B. Requirements and Measures

Specific provisions applicable to Requirement R3 for Distribution Provider:

If the Operating Instruction issued to the Distribution Provider requires a load shedding, the load shedding required is equivalent to a reduction in net transfer from Québec's system to the entity's load. Depending on the load shedding required, the Distribution Provider may have to reduce net transfer to zero.

Specific provisions applicable to Requirement R10.1 and R10.3:

R10.1: The Requirements only apply to the facilities of the Main Transmission System (RTP).

R10.3: The expression "non-BES" is replaced by "non-RTP".

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

In Québec, "Compliance Enforcement Authority" means the Régie de l'énergie in its roles of monitoring and enforcing compliance with respect to the Reliability Standard and to this appendix.

1.2. Evidence Retention

No specific provisions.

1.3. Compliance Monitoring and Enforcement Program

The Régie de l'énergie establishes the monitoring processes used to evaluate data or information for the purpose of determining compliance or non-compliance with the Reliability Standard and with this appendix.

Violation Severity Levels

No specific provisions.

D. Regional Variances

No specific provisions.

E. Associated Documents

The Quebec glossary reference is the "Quebec Reliability Standards Glossary of Terms".

Guidelines and Technical Basis

No specific provisions.

Rationale

The expression "non BES" is replaced by "non RTP" only for the Facilities in Québec that are within the Transmission Operator Area.

Version history

Version	Date	Action	Change tracking
1	March 10, 2022	New appendix as per decision D-2022-031.	New

A. Introduction

1. **Title: Operations Planning**
2. **Number: TOP-002-4**
3. **Purpose:** To ensure that Transmission Operators and Balancing Authorities have plans for operating within specified limits.
4. **Applicability:**
   - **4.1.** Transmission Operator
   - **4.2.** Balancing Authority
5. **Effective Date:**

   See Implementation Plan.
6. **Background:**

   See Project 2014-03 project page.

B. Requirements and Measures

R1. Each Transmission Operator shall have an Operational Planning Analysis that will allow it to assess whether its planned operations for the next day within its Transmission Operator Area will exceed any of its System Operating Limits (SOLs). *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M1. Each Transmission Operator shall have evidence of a completed Operational Planning Analysis. Such evidence could include but is not limited to dated power flow study results.

R2. Each Transmission Operator shall have an Operating Plan(s) for next-day operations to address potential System Operating Limit (SOL) exceedances identified as a result of its Operational Planning Analysis as required in Requirement R1. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M2. Each Transmission Operator shall have evidence that it has an Operating Plan to address potential System Operating Limits (SOLs) exceedances identified as a result of the Operational Planning Analysis performed in Requirement R1. Such evidence could include but it is not limited to plans for precluding operating in excess of each SOL that was identified as a result of the Operational Planning Analysis.

R3. Each Transmission Operator shall notify entities identified in the Operating Plan(s) cited in Requirement R2 as to their role in those plan(s). *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. Each Transmission Operator shall have evidence that it notified entities identified in the Operating Plan(s) cited in Requirement R2 as to their role in the plan(s). Such evidence could include but is not limited to dated operator logs, or e-mail records.

R4. Each Balancing Authority shall have an Operating Plan(s) for the next-day that addresses: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

4.1 Expected generation resource commitment and dispatch

4.2 Interchange scheduling

4.3 Demand patterns

4.4 Capacity and energy reserve requirements, including deliverability capability

M4. Each Balancing Authority shall have evidence that it has developed a plan to operate within the criteria identified. Such evidence could include but is not limited to dated operator logs or e-mail records.

R5. Each Balancing Authority shall notify entities identified in the Operating Plan(s) cited in Requirement R4 as to their role in those plan(s). *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M5. Each Balancing Authority shall have evidence that it notified entities identified in the plan(s) cited in Requirement R4 as to their role in the plan(s). Such evidence could include but is not limited to dated operator logs or e-mail records.

R6. Each Transmission Operator shall provide its Operating Plan(s) for next-day operations identified in Requirement R2 to its Reliability Coordinator. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M6. Each Transmission Operator shall have evidence that it provided its Operating Plan(s) for next-day operations identified in Requirement R2 to its Reliability Coordinator. Such evidence could include but is not limited to dated operator logs or e-mail records.

R7. Each Balancing Authority shall provide its Operating Plan(s) for next-day operations identified in Requirement R4 to its Reliability Coordinator. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M7. Each Balancing Authority shall have evidence that it provided its Operating Plan(s) for next-day operations identified in Requirement R4 to its Reliability Coordinator. Such evidence could include but is not limited to dated operator logs or e-mail records.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Compliance Monitoring and Assessment Processes

As defined in the NERC Rules of Procedure, "Compliance Monitoring and Assessment Processes" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated reliability standard.

1.3. Data Retention

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

Each Transmission Operator and Balancing Authority shall keep data or evidence to show compliance for each applicable Requirement for a rolling 90-calendar days period for analyses, the most recent 90-calendar days for voice recordings, and 12 months for operating logs and e-mail records unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

If a Transmission Operator or Balancing Authority is found non-compliant, it shall keep information related to the non-compliance until found compliant or the time period specified above, whichever is longer.

The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records

1.4. Additional Compliance Information

None.

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	Operations Planning	Medium	N/A	N/A	N/A	The Transmission Operator did not have an Operational Planning Analysis allowing it to assess whether its planned operations for the next day within its Transmission Operator Area exceeded any of its System Operating Limits (SOLs).
R2	Operations Planning	Medium	N/A	N/A	N/A	The Transmission Operator did not have an Operating Plan to address potential System Operating Limit (SOL) exceedances identified as a result of the Operational Planning Analysis performed in Requirement R1.

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
For the Requirement R3 and R5 VSLs only, the intent of the SDT is to start with the Severe VSL first and then to work your way to the left until you find the situation that fits. In this manner, the VSL will not be discriminatory by size of entity. If a small entity has just one affected reliability entity to inform, the intent is that that situation would be a Severe violation.						
R3	Operations Planning	Medium	The Transmission Operator did not notify one impacted entity or 5% or less of the entities, whichever is greater identified in the Operating Plan(s) as to their role in the plan(s).	The Transmission Operator did not notify two entities or more than 5% and less than or equal to 10% of the impacted entities, whichever is greater, identified in the Operating Plan(s) as to their role in the plan(s).	The Transmission Operator did not notify three impacted entities or more than 10% and less than or equal to 15% of the entities, whichever is greater, identified in the Operating Plan(s) as to their role in the plan(s).	The Transmission Operator did not notify four or more entities or more than 15% of the impacted NERC identified in the Operating Plan(s) as to their role in the plan(s).
R4	Operations Planning	Medium	The Balancing Authority has an Operating Plan but it does not address one of the criteria in Requirement R4.	The Balancing Authority has an Operating Plan but it does not address two of the criteria in Requirement R4.	The Balancing Authority has an Operating Plan but it does not address three of the criteria in Requirement R4.	The Balancing Authority did not have an Operating Plan.
R5	Operations Planning	Medium	The Balancing Authority did not notify one impacted entity or 5% or less	The Balancing Authority did not notify two entities or more than 5% and	The Balancing Authority did not notify three impacted entities or	The Balancing Authority did not notify four or more entities or more than

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			of the entities, whichever is greater, identified in the Operating Plan(s) as to their role in the plan(s).	less than or equal to 10% of the impacted entities, whichever is greater, identified in the Operating Plan(s) as to their role in the plan(s).	more than 10% and less than or equal to 15% of the entities, whichever is greater, identified in the Operating Plan(s) as to their role in the plan(s).	15% of the impacted entities identified in the Operating Plan(s) as to their role in the plan(s).
R6	Operations Planning	Medium	N/A	N/A	N/A	The Transmission Operator did not provide its Operating Plan(s) for next-day operations as identified in Requirement R2 to its Reliability Coordinator.
R7	Operations Planning	Medium	N/A	N/A	N/A	The Balancing Authority did not provide its Operating Plan(s) for next-day operations as identified in Requirement R4 to its Reliability Coordinator.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

Operating Plan - An Operating Plan includes general Operating Processes and specific Operating Procedures. It may be an overview document which provides a prescription for an Operating Plan for the next-day, or it may be a specific plan to address a specific SOL or IROL exceedance identified in the Operational Planning Analysis (OPA). Consistent with the NERC definition, Operating Plans can be general in nature, or they can be specific plans to address specific reliability issues. The use of the term Operating Plan in the revised TOP/IRO standards allows room for both. An Operating Plan references processes and procedures which are available to the System Operator on a daily basis to allow the operator to reliably address conditions which may arise throughout the day. It is valid for tomorrow, the day after, and the day after that. Operating Plans should be augmented by temporary operating guides which outline prevention/mitigation plans for specific situations which are identified day-to-day in an OPA or a Real-time Assessment (RTA). As the definition in the Glossary of Terms states, a restoration plan is an example of an Operating Plan. It contains all the overarching principles that the System Operator needs to work his/her way through the restoration process. It is not a specific document written for a specific blackout scenario but rather a collection of tools consisting of processes, procedures, and automated software systems that are available to the operator to use in restoring the system. An Operating Plan can in turn be looked upon in a similar manner. It does not contain a prescription for the specific set-up for tomorrow but contains a treatment of all the processes, procedures, and automated software systems that are at the operator's disposal. The existence of an Operating Plan, however, does not preclude the need for creating specific action plans for specific SOL or IROL exceedances identified in the OPA. When a Reliability Coordinator performs an OPA, the analysis may reveal instances of possible SOL or IROL exceedances for pre- or post-Contingency conditions. In these instances, Reliability Coordinators are expected to ensure that there are plans in place to prevent or mitigate those SOLs or IROLs, should those operating conditions be encountered the next day. The Operating Plan may contain a description of the process by which specific prevention or mitigation plans for day-to-day SOL or IROL exceedances identified in the OPA are handled and communicated. This approach could alleviate any potential administrative burden associated with perceived requirements for continual day-to-day updating of "the Operating Plan document" for compliance purposes.

Version History

Version	Date	Action	Change Tracking
0	April 1, 2005	Effective Date	New
0	August 8, 2005	Removed "Proposed" from Effective Date	Errata
1	August 2, 2006	Adopted by Board of Trustees	Revised
2	November 1, 2006	Adopted by Board of Trustees	Revised
2	June 14, 2007	Fixed typo in R11., (subject to …)	Errata
2a	February 10, 2009	Added Appendix 1 – Interpretation of R11 approved by BOT on February 10, 2009	Interpretation
2a	December 2, 2009	Interpretation of R11 approved by FERC on December 2, 2009	Same Interpretation
2b	November 4, 2010	Added Appendix 2 – Interpretation of R10 adopted by the Board of Trustees	
2b	October 20, 2011	FERC Order issued approving the Interpretation of R10 (FERC's Order became effective on October 20, 2011)	
2.1b	March 8, 2012	Errata adopted by Standards Committee; (Removed unnecessary language from the Effective Date section. Deleted retired sub-requirements from Requirement R14)	Errata
2.1b	April 11, 2012	Additional errata adopted by Standards Committee; (Deleted language from retired sub-requirement from Measure M7)	Errata
2.1b	September 13, 2012	FERC approved	Errata
3	May 6, 2012	Revisions under Project 2007-03	Revised

3	May 9, 2012	Adopted by Board of Trustees	Revised
4	April 2014	Revisions under Project 2014-03	Revised
4	November 13, 2014	Adopted by NERC Board of Trustees	Revisions under Project 2014-03

Guidelines and Technical Basis

Rationale:

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for Definitions:
Changes made to the proposed definitions were made in order to respond to issues raised in NOPR paragraphs 55, 73, and 74 dealing with analysis of SOLs in all time horizons, questions on Protection Systems and Special Protection Systems in NOPR paragraph 78, and recommendations on phase angles from the SW Outage Report (recommendation 27). The intent of such changes is to ensure that Real-time Assessments contain sufficient details to result in an appropriate level of situational awareness. Some examples include: 1) analyzing phase angles which may result in the implementation of an Operating Plan to adjust generation or curtail transactions so that a Transmission facility may be returned to service, or 2) evaluating the impact of a modified Contingency resulting from the status change of a Special Protection Scheme from enabled/in-service to disabled/out-of-service.

Rationale for R1:
Terms deleted in Requirement R1 as they are now contained in the revised definition of Operational Planning Analysis

Rationale for R2:
The change to Requirement R2 is in response to NOPR paragraph 42 and in concert with proposed changes made to proposed TOP-001-4

Rationale for R3:
Changes in response to IERP recommendation

Rationale for R4 and R5:
These Requirements were added to address IERP recommendations

Rationale for R6 and R7:
Added in response to SW Outage Report recommendation 1

Appendix QC-TOP-002-4
Provisions specific to the standard TOP-002-4 applicable in Québec

This appendix establishes specific provisions for the application of the standard in Québec. Provisions of the standard and of its appendix must be read together for the purposes of understanding and interpretation. Where the standard and appendix differ, the appendix shall prevail.

A. Introduction

1. Title: **Operations Planning**

2. Number: TOP-002-4

3. Purpose: No specific provision

4. Applicability:

Functions

No specific provision

Facilities

This standard only applies to the facilities of the Main Transmission System (RTP).

5. Effective Date:

5.1. Adoption of the standard by the Régie de l'énergie: June 16, 2017

5.2. Adoption of the appendix by the Régie de l'énergie: June 16, 2017

5.3. Effective date of the standard and its appendix in Québec: July 1st 2017

6. Background :

No specific provision

B. Requirements and Measures

No specific provision

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

The Régie de l'énergie is responsible, in Québec, for compliance monitoring with respect to the reliability standard and its appendix that it adopts.

1.2. Compliance Monitoring and Assessment Processes

Compliance Audit

Self-Certification

Spot Check

Compliance Investigation

Non-Compliance Self-Reporting

Periodic Data Submittal

Exception Reporting

Investigation following a complaint

1.3. Data Retention

No specific provision

1.4. Additional Compliance Information

No specific provision

2. Table of Compliance Elements

No specific provision

D. Regional Variances

No specific provision

E. Interpretations

No specific provision

F. Associated Documents

The Quebec glossary reference is the "Quebec Reliability Standards Glossary of Terms"

Guidelines and Technical Basis

No specific provision

Revision History

Revision	Date	Action	Change Tracking
0	June 16, 2017	New appendix	New

A. Introduction

1. **Title:** Transmission Operator and Balancing Authority Data and Information Specification and Collection

2. **Number:** TOP-003-6.1

3. **Purpose:** To ensure that each Transmission Operator and Balancing Authority has the data and information it needs to plan, monitor, and assess the operation of its Transmission Operator Area or Balancing Authority Area.

4. **Applicability:**

   4.1 Functional Entities:

   4.1.1 Transmission Operator

   4.1.2 Balancing Authority

   4.1.3 Generator Owner

   4.1.4 Generator Operator

   4.1.5 Transmission Owner

   4.1.6 Distribution Provider

5. **Effective Date:** See Implementation Plan for Project 2021-06.

B. Requirements and Measures

R1. Each Transmission Operator shall maintain documented specification(s) for the data and information necessary for it to perform its Operational Planning Analyses, Real-time monitoring, and Real-time Assessments. The specification shall include, but not be limited to: *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

1.1. A list of data and information needed by the Transmission Operator to support its Operational Planning Analyses, Real-time monitoring, and Real-time Assessments including non-BES data and information, external network data and information, and identification of the entities responsible for responding to the specification as deemed necessary by the Transmission Operator.

1.2. Provisions for notification of current Protection System and Remedial Action Scheme (RAS) status or degradation that impacts System reliability.

1.3. Provisions for notification of BES generating unit(s) during local forecasted cold weather to include:

1.3.1. Operating limitations based on:

1.3.1.1. capability and availability;

1.3.1.2. fuel supply and inventory concerns;

1.3.1.3. fuel switching capabilities; and

1.3.1.4. environmental constraints

1.3.2. Generating unit(s) minimum:

1.3.2.1. design temperature; or

1.3.2.2. historical operating temperature; or

1.3.2.3. current cold weather performance temperature determined by an engineering analysis.

1.4. Identification of a mutually agreeable process for resolving conflicts.

1.5. Method(s) for the entity identified in Part 1.1 to provide the data and information that includes at a minimum the following.

1.5.1. Specified deadlines or periodicity which data and information is to be provided;

1.5.2. Performance criteria for the availability and accuracy of data and information as applicable;

1.5.3. Provisions to update or correct data and information, as applicable or necessary;

1.5.4. A mutually agreeable format;

1.5.5. Mutually agreeable method(s) for securely transferring data and information.

M1. Each Transmission Operator shall make available its dated, current, in force documented specification(s) for data and information.

R2. Each Balancing Authority shall maintain documented specification(s) for the data and information necessary for it to perform its analysis functions and Real-time monitoring. The data specification shall include, but not be limited to: *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

2.1. A list of data and information needed by the Balancing Authority to support its analysis functions and Real-time monitoring including non-Bulk Electric System data and information, and external network data and information, as deemed necessary by the Balancing Authority, and identification of the entity responsible for responding to the specification.

2.2. Provisions for notification of current Protection System and Remedial Action Scheme status or degradation that impacts System reliability.

2.3. Provisions for notification of BES generating unit(s) status during local forecasted cold weather to include:

2.3.1. Operating limitations based on:

2.3.1.1. capability and availability;

2.3.1.2. fuel supply and inventory concerns;

2.3.1.3. fuel switching capabilities; and

2.3.1.4. environmental constraints.

2.3.2. Generating unit(s) minimum:

2.3.2.1. design temperature; or

2.3.2.2. historical operating temperature; or

2.3.2.3. current cold weather performance temperature determined by an engineering analysis.

2.4. Identification of a mutually agreeable process in resolving conflicts

2.5. Methods for the entity identified in Part 2.1 to provide data and information that includes at a minimum the following.

2.5.1. Specific deadlines or periodicity in which data and information is to be provided;

2.5.2. Performance criteria for the availability and accuracy of data and information, as applicable;

2.5.3. Provisions to update or correct data and information, as applicable or necessary.

2.5.4. A mutually agreeable format.

2.5.5. A mutually agreeable method(s) for securely transferring data and information.

M2. Each Balancing Authority shall make available its dated, current, in force documented specification(s) for data and information.

R3. Each Transmission Operator shall distribute its data and information specification(s) to entities that have data and information required by the Transmission Operator's Operational Planning Analyses, Real- time monitoring, and Real-time Assessments. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M3. Each Transmission Operator shall make available evidence that it has distributed its data specification(s) to entities that have data and information required by the Transmission Operator's Operational Planning Analyses, Real-time monitoring, and Real-time Assessments.

Such evidence could include but is not limited to web postings with an electronic notice of the posting, dated operator logs, voice recordings, postal receipts showing the recipient, date and contents, or e-mail records.

R4. Each Balancing Authority shall distribute its data and information specification(s) to entities that have data and information required by the Balancing Authority's analysis functions and Real-time monitoring. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M4. Each Balancing Authority shall make available evidence that it has distributed its data specification(s) to entities that have data and information required by the Balancing Authority's analysis functions and Real-time monitoring. Such evidence could include but is not limited to web postings with an electronic notice of the posting, dated operator logs, voice recordings, postal receipts showing the recipient, or e-mail records.

R5. Each Transmission Operator, Balancing Authority, Generator Owner, Generator Operator, Transmission Owner, and Distribution Provider receiving a data and information specification(s) in Requirement R3 or R4 shall satisfy the obligations of the documented specifications. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning, Same-Day Operations, Real-time Operations]*

M5. Each Transmission Operator, Balancing Authority, Generator Owner, Generator Operator, Transmission Owner, and Distribution Provider receiving a specification(s) in Requirement R3 or R4 shall make available evidence that it has satisfied the obligations of the documented specification. Such evidence could include, but is not limited to, electronic or hard copies of data transmittals or attestations of receiving entities.

C. Compliance

1. Compliance Monitoring Process

4.1.1 Compliance Enforcement Authority: "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

4.1.2 Evidence Retention: The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

Each responsible entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation.

Each Transmission Operator shall retain its dated, current, in force, documented specification for the data and information necessary for it to perform its Operational Planning Analyses, Real-time monitoring, and Real-time Assessments in accordance with Requirement R1 and Measurement M1 as well as any documents in force since the last compliance audit.

Each Balancing Authority shall retain its dated, current, in force, documented specification(s) for the data and information necessary for it to perform its analysis functions and Real-time monitoring in accordance with Requirement R2 and Measurement M2 as well as any documents in force since the last compliance audit.

Each Transmission Operator shall retain evidence for three calendar years that it has distributed its specification(s) to entities that have data required by the Transmission Operator's Operational Planning Analyses, Real-time monitoring, and Real-time Assessments in accordance with Requirement R3 and Measurement M3.

Each Balancing Authority shall retain evidence for three calendar years that it has distributed its specification(s) to entities that have data required by the Balancing Authority's analysis functions and Real-time monitoring in accordance with Requirement R4 and Measurement M4.

Each Balancing Authority, Generator Owner, Generator Operator, Transmission Operator, Transmission Owner, and Distribution Provider receiving a specification(s) in Requirement R3 or R4 shall retain evidence for the most

recent 90-calendar days that it has satisfied the obligations of the documented specifications in accordance with Requirement R5 and Measurement M5.

4.1.3 Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated reliability standard.

Violation Severity Levels

R#	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	Operations Planning	Lower	The Transmission Operator did not include one or two of the parts (Part 1.1 through Part 1.5) of the documented specification(s) for the data and information necessary for it to perform its Operational Planning Analyses, Real-time monitoring, and Real- time Assessments.	The Transmission Operator did not include three of the parts (Part 1.1 through Part 1.5) of the documented specification(s) for the data and information necessary for it to perform its Operational Planning Analyses, Real-time monitoring, and Real- time Assessments.	The Transmission Operator did not include four of the parts (Part 1.1 through Part 1.5) of the documented specification(s) for the data and information necessary for it to perform its Operational Planning Analyses, Real-time monitoring, and Real-time Assessments.	The Transmission Operator did not include any of the parts (Part 1.1 through Part 1.5) of the documented specification(s) for the data and information necessary for it to perform its Operational Planning Analyses, Real-time monitoring, and Real- time Assessments. OR, The Transmission Operator did not have a documented specification(s) for the data and information necessary for it to perform its Operational Planning Analyses, Real-time monitoring, and Real- time Assessments.
R2	Operations Planning	Lower	The Balancing Authority did not include two or fewer of the parts (Part 2.1 through Part 2.5) of the documented specification(s) for the data and information necessary for it to perform its analysis functions and Real- time monitoring.	The Balancing Authority did not include three of the parts (Part 2.1 through Part 2.5) of the documented specification(s) for the data and information necessary for it to perform its analysis functions and Real- time	The Balancing Authority did not include four of the parts (Part 2.1 through Part 2.5) of the documented specification(s) for the data and information necessary for it to perform its analysis functions and Real- time monitoring.	The Balancing Authority did not include any of the parts (Part 2.1 through Part 2.5) of the documented specification(s) for the data and information necessary for it to perform its analysis functions and Real- time monitoring.

R#	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				monitoring.		OR, The Balancing Authority did not have a documented specification(s) for the data and information necessary for it to perform its analysis functions and Real- time monitoring.
For the Requirement R3 and R4 VSLs only, the intent of the SDT is to start with the Severe VSL first and then to work your way to the left until you find the situation that fits. In this manner, the VSL will not be discriminatory by size of entity. If a small entity has just one affected reliability entity to inform, the intent is that that situation would be a Severe violation.						
R3	Operations Planning	Lower	The Transmission Operator did not distribute its Specification(s) to one entity, or 5% or less of the entities, whichever is greater, that have data and information required by the Transmission Operator's Operational Planning Analyses, Real-time monitoring, and Real-time Assessments.	The Transmission Operator did not distribute its Specification(s) to two entities, or more than 5% and less than or equal to10% of the reliability entities, whichever is greater, that have data and information required by the Transmission Operator's Operational Planning Analyses, Real-time monitoring, and Real-time Assessments.	The Transmission Operator did not distribute its Specification(s) to three entities, or more than 10% and less than or equal to 15% of the reliability entities, whichever is greater, that have data and information required by the Transmission Operator's Operational Planning Analyses, Real-time monitoring, and Real-time Assessments.	The Transmission Operator did not distribute its Specification(s) to four or more entities, or more than 15% of the entities that have data and information required by the Transmission Operator's Operational Planning Analyses, Real-time monitoring, and Real-time Assessments.
R4	Operations Planning	Lower	The Balancing Authority did not distribute its Specification(s) to one entity, or 5% or less of the entities, whichever is greater, that have data and information required	The Balancing Authority did not distribute its Specification(s) to two entities, or more than 5% and less than or equal to 10% of the entities, whichever is greater, that	The Balancing Authority did not distribute its Specification(s) to three entities, or more than10% and less than or equal to 15% of the entities, whichever is greater, that	The Balancing Authority did not distribute its Specification(s) to four or more entities, or more than 15% of the entities that have data and information required by

R#	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			by the Balancing Authority's analysis functions and Real-time monitoring.	have data and information required by the Balancing Authority's analysis functions and Real-time monitoring.	have data and information required by the Balancing Authority's analysis functions and Real-time monitoring.	the Balancing Authority's analysis functions and Real-time monitoring.
R5	Operations Planning, Same-Day Operations, Real-time Operations	Medium	The responsible entity receiving a specification(s) in Requirement R3 or R4 satisfied the obligations in the specification but failed to meet one of the parts in Requirement R1 Part1.5 or Requirement R2 Part 2.5.	The responsible entity receiving a specification(s) in Requirement R3 or R4 satisfied the obligations in the specification but failed to meet two of the parts in Requirement R1 Part 1.5 or Requirement R2 Part 2.5.	The responsible entity receiving a specification(s) in Requirement R3 or R4 satisfied the obligations in the specification but failed to meet three or more of the parts in Requirement R1 Part 1.5 or Requirement R2 Part 2.5.	The responsible entity receiving a specification(s) in Requirement R3 or R4 did not satisfy the obligations of the documented specifications.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
0	April 1, 2005	Effective Date	New
0	August 8, 2005	Removed “Proposed” from Effective Date	Errata
1		Modified R1.2 Modified M1 Replaced Levels of Non-compliance with the Feb 28, BOT approved Violation Severity Levels (VSLs)	Revised
1	October 17, 2008	Adopted by NERC Board of Trustees	
1	March 17, 2011	Order issued by FERC approving TOP- 003-1 (approval effective 5/23/11)	
2	May 6, 2012	Revised under Project 2007-03	Revised
2	May 9, 2012	Adopted by Board of Trustees	Revised
3	April 2014	Changes pursuant to Project 2014-03	Revised
3	November 13, 2014	Adopted by Board of Trustees	Revisions under Project 2014-03
3	November 19, 2015	FERC approved TOP-003-3. Docket No. RM15-16-000, Order No. 817	
4	February 6, 2020	Adopted by NERC Board of Trustees	Revisions under Project 2017-07
4	October 30, 2020	FERC approved TOP-003-4. Docket No. RD20-4-000	
5	May 2021	Changes pursuant to Project 2019-06	Revised
5	June 11, 2021	Board approved	Project 2019-06 Cold Weather
5	August 24, 2021	FERC approved TOP –003-5 Docket No. RD21-5-000, Order 176	
6	TBD	Adopted by NERC Board of Trustees	Revisions under project 2021-06
6.1	Errata	Approved by the Standards Committee	August 23,2023
6.1	November 2, 2023	FERC Approved TOP-003-6.1 Docket No.RD23-6-000,	

6.1	November 3, 2023	Effective Date	July 1, 2025

Appendix TOP-003-6.1-QC-1
Specific provisions applicable in Québec for standard TOP-003-6.1 – Transmission Operator and Balancing Authority Data and Information Specification and Collection

This appendix establishes specific provisions for the application of the standard in Québec. Provisions of the standard and of this appendix must be read together jointly for comprehension and interpretation purposes. Where the standard and appendix differ, the appendix shall prevail.

A. Introduction

1. Title: No specific provision.

2. Number: No specific provision.

3. Purpose: No specific provision.

4. Applicability:

This standard applies to the facilities of the Main Transmission System (RTP) and, for the requirements R1 and R2, to the facilities designated under this requirement.

5. Effective Date:

5.1. Adoption of the standard by the Régie de l'énergie: September 13, 2024

5.2. Adoption of the appendix by the Régie de l'énergie: September 13, 2024

5.3. Effective date of the standard and of its appendix in Québec: April 1, 2026

B. Requirements and Measures

Specific provisions applicable to requirement R1 & R2 (1.1 and 2.1):
The expression “non BES” is replaced by “non RTP”.

Specific provisions applicable to requirements R1 & R2 (1.3 and 2.3):
The expression “BES” is replaced by “RTP”.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Process

In Québec, “Compliance Enforcement Authority” means the Régie de l’énergie in its roles of monitoring and enforcing compliance with respect to the Reliability Standard and to this appendix.

1.2. Evidence Retention

No specific provision.

1.3. Compliance Monitoring and Enforcement Program

The Régie de l’énergie establishes the monitoring processes used to evaluate data or information for the purpose of determining compliance or non-compliance with the Reliability Standard and with this appendix.

Violation Severity Levels

No specific provision.

D. Regional Variances

No specific provision.

E. Interpretations

No specific provision.

F. Associated Documents

No specific provision.

Version history

Version	Date	Action	Change Tracking
1	September 13, 2024	New appendix as per decision D-2024-096.	New

A. Introduction

1. **Title:** **Real-time Reliability Monitoring and Analysis Capabilities**
2. **Number:** **TOP-010-1(i)**
3. **Purpose:** Establish requirements for Real-time monitoring and analysis capabilities to support reliable System operations.
4. **Applicability:**
   - **4.1. Functional Entities:**
     - **4.1.1.** Transmission Operators
     - **4.1.2.** Balancing Authorities
5. **Effective Date:** See Implementation Plan

B. Requirements and Measures

R1. Each Transmission Operator shall implement an Operating Process or Operating Procedure to address the quality of the Real-time data necessary to perform its Real-time monitoring and Real-time Assessments. The Operating Process or Operating Procedure shall include: *[Violation Risk Factor: High] [Time Horizon: Real-time Operations]*

- **1.1.** Criteria for evaluating the quality of Real-time data;
- **1.2.** Provisions to indicate the quality of Real-time data to the System Operator; and
- **1.3.** Actions to address Real-time data quality issues with the entity(ies) responsible for providing the data when data quality affects Real-time Assessments.

M1. Each Transmission Operator shall have evidence that it implemented its Operating Process or Operating Procedure to address the quality of the Real-time data necessary to perform its Real-time monitoring and Real-time Assessments. This evidence could include, but is not limited to: 1) an Operating Process or Operating Procedure in electronic or hard copy format meeting all provisions of Requirement R1; and 2) evidence the Transmission Operator implemented the Operating Process or Operating Procedure as called for in the Operating Process or Operating Procedure, such as dated operator logs, dated checklists, voice recordings, voice transcripts, or other evidence.

R2. Each Balancing Authority shall implement an Operating Process or Operating Procedure to address the quality of the Real-time data necessary to perform its analysis functions and Real-time monitoring. The Operating Process or Operating Procedure shall include: *[Violation Risk Factor: High] [Time Horizon: Real-time Operations]*

- **2.1.** Criteria for evaluating the quality of Real-time data;
- **2.2.** Provisions to indicate the quality of Real-time data to the System Operator; and

2.3. Actions to address Real-time data quality issues with the entity(ies) responsible for providing the data when data quality affects its analysis functions.

M2. Each Balancing Authority shall have evidence that it implemented its Operating Process or Operating Procedure to address the quality of the Real-time data necessary to perform its analysis functions and Real-time monitoring. This evidence could include, but is not limited to: 1) an Operating Process or Operating Procedure in electronic or hard copy format meeting all provisions of Requirement R2; and 2) evidence the Balancing Authority implemented the Operating Process or Operating Procedure as called for in the Operating Process or Operating Procedure, such as dated operator logs, dated checklists, voice recordings, voice transcripts, or other evidence.

R3. Each Transmission Operator shall implement an Operating Process or Operating Procedure to address the quality of analysis used in its Real-time Assessments. The Operating Process or Operating Procedure shall include: *[Violation Risk Factor: Medium] [Time Horizon: Real-time Operations]*

3.1. Criteria for evaluating the quality of analysis used in its Real-time Assessments;

3.2. Provisions to indicate the quality of analysis used in its Real-time Assessments; and

3.3. Actions to address analysis quality issues affecting its Real-time Assessments.

M3. Each Transmission Operator shall have evidence it implemented its Operating Process or Operating Procedure to address the quality of analysis used in its Real-time Assessments as specified in Requirement R3. This evidence could include, but is not limited to: 1) an Operating Process or Operating Procedure in electronic or hard copy format meeting all provisions of Requirement R3; and 2) evidence the Transmission Operator implemented the Operating Process or Operating Procedure as called for in the Operating Process or Operating Procedure, such as dated operator logs, dated checklists, voice recordings, voice transcripts, or other evidence.

R4. Each Transmission Operator and Balancing Authority shall have an alarm process monitor that provides notification(s) to its System Operators when a failure of its Real-time monitoring alarm processor has occurred. *[Violation Risk Factor: Medium] [Time Horizon: Real-time Operations]*

M4. Each Transmission Operator and Balancing Authority shall have evidence of an alarm process monitor that provides notification(s) to its System Operators when a failure of its Real-time monitoring alarm processor has occurred. This evidence could include, but is not limited to, operator logs, computer printouts, system specifications, or other evidence.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority:

"Compliance Enforcement Authority" means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention:

The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show it was compliant for the full-time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

The applicable entity shall retain evidence of compliance for Requirements R1, R2, and R4, and Measures M1, M2, and M4 for the current calendar year and one previous calendar year, with the exception of operator logs and voice recordings which shall be retained for a minimum of 90 calendar days, unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

The Transmission Operator shall retain evidence of compliance for Requirement R3 and Measure M3 for a rolling 30-day period, unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

If an applicable entity is found non-compliant it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.

1.3. Compliance Monitoring and Enforcement Program

As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	N/A	The Transmission Operator's Operating Process or Operating Procedure to address the quality of the Real-time data necessary to perform its Real-time monitoring and Real-time Assessments did not include one of the elements listed in Part 1.1 through Part 1.3.	The Transmission Operator's Operating Process or Operating Procedure to address the quality of the Real-time data necessary to perform its Real-time monitoring and Real-time Assessments did not include two of the elements listed in Part 1.1 through Part 1.3.	The Transmission Operator's Operating Process or Operating Procedure to address the quality of the Real-time data necessary to perform its Real-time monitoring and Real-time Assessments did not include any of the elements listed in Part 1.1 through Part 1.3; OR The Transmission Operator did not implement an Operating Process or Operating Procedure to address the quality of the Real-time data necessary to perform its Real-time monitoring and Real-time Assessments.
R2.	N/A	The Balancing Authority's Operating Process or Operating Procedure to address the quality of the	The Balancing Authority's Operating Process or Operating Procedure to address the quality of the	The Balancing Authority's Operating Process or Operating Procedure to address the quality of the

		Real-time data necessary to perform its analysis functions and Real-time monitoring did not include one of the elements listed in Part 2.1 through Part 2.3.	Real-time data necessary to perform its analysis functions and Real-time monitoring did not include two of the elements listed in Part 2.1 through Part 2.3.	Real-time data necessary to perform its analysis functions and Real-time monitoring did not include any of the elements listed in Part 2.1 through Part 2.3; OR The Balancing Authority did not implement an Operating Process or Operating Procedure to address the quality of the Real-time data necessary to perform its analysis functions and Real-time monitoring.
R3.	N/A	The Transmission Operator's Operating Process or Operating Procedure to address the quality of analysis used in its Real-time Assessments did not include one of the elements listed in Part 3.1 through Part 3.3.	The Transmission Operator's Operating Process or Operating Procedure to address the quality of analysis used in its Real-time Assessments did not include two of the elements listed in Part 3.1 through Part 3.3.	The Transmission Operator's Operating Process or Operating Procedure to address the quality of analysis used in its Real-time Assessments did not include any of the elements listed in Part 3.1 through Part 3.3; OR The Transmission Operator did not implement an Operating Process or Operating Procedure to address the quality of

				analysis used in its Real-time Assessments.
R4.	N/A	N/A	The responsible entity has an alarm process monitor but the alarm process monitor did not provide notification(s) to its System Operators when a failure of its Real-time monitoring alarm processor occurred.	The responsible entity does not have an alarm process monitor that provides notification(s) to its System Operators when a failure of its Real-time monitoring alarm processor has occurred.

D. Regional Variances

None.

E. Associated Documents

- Implementation Plan

Version History

Version	Date	Action	Change Tracking
1	October 30, 2015	New standard developed in Project 2009-02 to respond to recommendations in Real-time Best Practices Task Force Report and FERC directives.	N/A
1	May 5, 2016	Adopted by the Board of Trustees	New
1	September 22, 2016	FERC Order issued approving TOP-010-1. Docket No. RD16-6-000	

1(i)	September 22, 2016	FERC directive to change Requirement 1 and Requirement 2 from 'medium' to 'high'. Docket No. RD16-6-000	Revised
1(i)	November 2, 2016	Adopted by the Board of Trustees	New
1(i)	December 14, 2016	FERC letter Order approving revisions to the VRF for R1 and R2 from 'medium' to 'high'. Docket No. RD16-6-001.	

Guidelines and Technical Basis

Real-time monitoring, or *monitoring* the Bulk Electric System (BES) in Real-time, is a primary function of Reliability Coordinators (RCs), Transmission Operators (TOPs), and Balancing Authorities (BAs) as required by TOP and IRO Reliability Standards. As used in TOP and IRO Reliability Standards, monitoring involves observing operating status and operating values in Real-time for awareness of system conditions. Real-time monitoring may include the following activities performed in Real-time:

- Acquisition of operating data;
- Display of operating data as needed for visualization of system conditions;
- Audible or visual alerting when warranted by system conditions; and
- Audible or visual alerting when monitoring and analysis capabilities degrade or become unavailable.

Requirement R1

The TOP uses a set of Real-time data identified in TOP-003-3 Requirement R1 to perform its Real-time monitoring and Real-time Assessments. Functional requirements to perform monitoring and Real-time Assessments appear in other Reliability Standards.

The TOP's Operating Process or Operating Procedure must contain criteria for evaluating the quality of Real-time data as specified in proposed TOP-010-1 Requirement R1 Part 1.1. The criteria support identification of applicable data quality issues, which may include:

- Data outside of a prescribed data range;
- Analog data not updated within a predetermined time period;
- Data entered manually to override telemetered information; or
- Data otherwise identified as invalid or suspect.

The Operating Process or Operating Procedure must include provisions for indicating the quality of Real-time data to operating personnel. Descriptions of quality indicators such as display color codes, data quality flags, or other such indicators as found in Real-time monitoring specifications could be used.

Requirement R1 Part 1.3 specifies the TOP shall include actions to address Real-time data quality issues with the entity(ies) responsible for providing the data when data quality affects Real-time Assessments. Requirement R1 Part 1.3 is focused on addressing data point quality issues affecting Real-time Assessments. Other data quality issues of a lower priority are addressed according to an entity's operating practices and are not covered under Requirement R1 Part 1.3.

The TOP's actions to address data quality issues are steps within existing authorities and capabilities that provide awareness and enable the TOP to meet its obligations for performing the Real-time Assessment. Examples of actions to address data quality issues include, but are not limited to, the following:

- Notifying entities that provide Real-time data to the TOP;
- Following processes established for resolving data conflicts as specified in TOP-003-3, or other applicable Reliability Standards;
- Taking corrective actions on the TOP's own data;
- Changing data sources or other inputs so that the data quality issue no longer affects the TOP's Real-time Assessment; and
- Inputting data manually and updating as necessary.

The Operating Process or Operating Procedure must clearly identify to operating personnel how to determine the data that affects the quality of the Real-time Assessment so that effective actions can be taken to address data quality issues in an appropriate timeframe.

Requirement R2

The BA uses a set of Real-time data identified in TOP-003-3 Requirement R2 to perform its analysis functions and Real-time monitoring. Requirements to perform monitoring appear in other Reliability Standards.

The BA's Operating Process or Operating Procedure must contain criteria for evaluating the quality of Real-time data as specified in proposed TOP-010-1 Requirement R2 Part 2.1. The criteria supports identification of applicable data quality issues, which may include:

- Data outside of a prescribed data range;
- Analog data not updated within a predetermined time period;
- Data entered manually to override telemetered information; or
- Data otherwise identified as invalid or suspect.

The Operating Process or Operating Procedure must include provisions for indicating the quality of Real-time data to operating personnel. Descriptions of quality indicators such as display color codes, data quality flags, or other such indicators as found in Real-time monitoring specifications could be used.

Requirement R2 Part 2.3 specifies the BA shall include in its Operating Process or Operating Procedure actions to address Real-time data quality issues when data quality affects its analysis functions. Requirement R2 Part 2.3 is focused on addressing data point quality issues affecting analysis functions. Other data quality issues of a lower priority are addressed according to an entity's operating practices and are not covered under Requirement R2 Part 2.3.

The BA's actions to address data quality issues are steps within existing authorities and capabilities that provide awareness and enable the BA to meet its obligations for performing its analysis functions. Examples of actions to address data quality issues include, but are not limited to, the following:

- Notifying entities that provide Real-time data to the BA;

- Following processes established for resolving data conflicts as specified in TOP-003-3 or other applicable Reliability Standards;
- Taking corrective actions on the BA's own data;
- Changing data sources or other inputs so that the data quality issue no longer affects the BA's analysis functions; and
- Inputting data manually and updating as necessary.

The Operating Process or Operating Procedure must clearly identify to operating personnel how to determine the data that affects the analysis quality so that effective actions can be taken to address data quality issues in an appropriate timeframe.

Requirement R3

Requirement R3 ensures TOPs have procedures to address issues related to the quality of the analysis results used for Real-time Assessments. Requirements to perform Real-time Assessments appear in other Reliability Standards. Examples of the types of analysis used in Real-time Assessments may include, as applicable, state estimation, Real-time Contingency analysis, Stability analysis or other studies used for Real-time Assessments.

Examples of the types of criteria used to evaluate the quality of analysis used in Real-time Assessments may include solution tolerances, mismatches with Real-time data, convergences, etc.

The Operating Process or Operating Procedure must describe how the quality of analysis results used in Real-time Assessment will be shown to operating personnel.

Requirement R4

Requirement R4 addresses recommendation S7 of the Real-time Best Practices Task Force report concerning operator awareness of alarm availability.

An alarm process monitor could be an application within a Real-time monitoring system or it could be a separate system. 'Heartbeat' or 'watchdog' monitors are examples of an alarm process monitor. An alarm process monitor should be designed and implemented such that a stall of the Real-time monitoring alarm processor does not cause a failure of the alarm process monitor.

Rationale

Rationale for Requirement R1: The Transmission Operator (TOP) uses a set of Real-time data identified in TOP-003-3 Requirement R1 to perform its Real-time monitoring and Real-time Assessments. Functional requirements to perform Real-time monitoring and Real-time Assessments appear in other Reliability Standards.

The Operating Process or Operating Procedure must include provisions for indicating the quality of Real-time data to operating personnel. Descriptions of quality indicators such as display color codes, data quality flags, or other such indicators as found in Real-time monitoring specifications could be used.

Requirement R1 Part 1.3 of this standard specifies the TOP shall include actions to address Real-time data quality issues affecting its Real-time Assessments in its Operating Process or Operating Procedure. Examples of actions to address Real-time data quality issues are provided in the Guidelines and Technical Basis section. These actions could be the same as the process used to resolve data conflicts required by TOP-003-3 Requirement R5 Part 5.2, provided that this process addresses Real-time data quality issues.

The revision in Part 1.3 to address Real-time data quality issues *when data quality affects Real-time Assessments* clarifies the scope of data points that must be covered by the Operating Process or Operating Procedure.

Rationale for Requirement R2: The Balancing Authority (BA) uses a set of Real-time data identified in TOP-003-3 Requirement R2 to perform its analysis functions and Real-time monitoring. Requirements to perform monitoring appear in other Reliability Standards.

The Operating Process or Operating Procedure must include provisions for indicating the quality of Real-time data to operating personnel. Descriptions of quality indicators such as display color codes, data quality flags, or other such indicators as found in Real-time monitoring specifications could be used.

Requirement R2 Part 2.3 of this standard specifies the BA shall include actions to address Real-time data quality issues affecting its analysis functions in its Operating Process or Operating Procedure. Examples of actions to address Real-time data quality issues are provided in the Guidelines and Technical Basis section. These actions could be the same as the process to resolve data conflicts required by TOP-003-3 Requirement R5 Part 5.2 provided that this process addresses Real-time data quality issues.

The revision in Part 2.3 to address Real-time data quality issues *when data quality affects its analysis functions* clarifies the scope of data points that must be covered by the Operating Process or Operating Procedure.

Rationale for Requirement R3: Requirement R3 ensures TOPs have procedures to address issues related to the quality of the analysis results used for Real-time Assessments. Requirements to perform Real-time Assessments appear in other Reliability Standards. Examples of the types of analysis used in Real-time Assessments include, as applicable, state

estimation, Real-time Contingency analysis, Stability analysis or other studies used for Real-time Assessments.

The Operating Process or Operating Procedure must include provisions for how the quality of analysis results used in Real-time Assessment will be shown to operating personnel. Operating personnel includes System Operators and staff responsible for supporting Real-time operations.

Rationale for Requirement R4: The requirement addresses recommendation S7 of the Real-time Best Practices Task Force report concerning operator awareness of alarm availability.

The requirement in Draft Two of the proposed standard has been revised for clarity by removing the term *independent*. The alarm process monitor must be able to provide notification of failure of the Real-time monitoring alarm processor. This capability could be provided by an application within a Real-time monitoring system or by a separate component used by the System Operator. The alarm process monitor must not fail with a simultaneous failure of the Real-time monitoring alarm processor.

Appendix TOP-010-1(i)-QC-1

Specific provisions applicable in Québec for standard TOP-010-1(i) – Real-time Reliability Monitoring and Analysis Capabilities

This appendix establishes specific provisions for the application of the standard in Québec. Provisions of the standard and of this appendix must be read jointly for comprehension and interpretation purposes. Where the standard and appendix differ, the appendix shall prevail.

A. Introduction

1. Title: No specific provisions.

2. Number: No specific provisions.

3. Purpose: No specific provisions.

4. Applicability:

4.1. Functional Entities

No specific provisions.

5. Effective date:

5.1.	Adoption of the standard by the Régie de l'énergie:	June 9, 2020
5.2.	Adoption of this appendix by the Régie de l'énergie:	June 9, 2020
5.3.	Effective date of the standard and of this appendix in Québec:	January 1, 2022

B. Requirements and Measures

No specific provisions.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

In Québec, "Compliance Enforcement Authority" means the Régie de l'énergie in its roles of monitoring and enforcing compliance with respect to the Reliability Standard and to this appendix.

1.2. Evidence Retention

No specific provisions.

1.3. Compliance Monitoring and Enforcement Program

The Régie de l'énergie establishes the monitoring processes used to evaluate data or information for the purpose of determining compliance or non-compliance with the Reliability Standard and with this appendix.

Violation Severity Levels

No specific provisions.

D. Regional Variances

No specific provisions.

E. Associated Documents

No specific provisions.

Appendix TOP-010-1(i)-QC-1

Specific provisions applicable in Québec for standard TOP-010-1(i) – Real-time Reliability Monitoring and Analysis Capabilities

Guidelines and Technical Basis

No specific provisions.

Rationale

No specific provisions.

Version history

Version	Date	Action	Change tracking
1	June 9, 2020	New appendix	New

A. Introduction

1. **Title:** **Transmission System Planning Performance Requirements**

2. **Number:** **TPL-001-4**

3. **Purpose:** Establish Transmission system planning performance requirements within the planning horizon to develop a Bulk Electric System (BES) that will operate reliably over a broad spectrum of System conditions and following a wide range of probable Contingencies.

4. **Applicability:**

   4.1. Functional Entity

   4.1.1. Planning Coordinator.

   4.1.2. Transmission Planner.

5. **Effective Date:** Requirements R1 and R7 as well as the definitions shall become effective on the first day of the first calendar quarter, 12 months after applicable regulatory approval. In those jurisdictions where regulatory approval is not required, Requirements R1 and R7 become effective on the first day of the first calendar quarter, 12 months after Board of Trustees adoption or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

   Except as indicated below, Requirements R2 through R6 and Requirement R8 shall become effective on the first day of the first calendar quarter, 24 months after applicable regulatory approval. In those jurisdictions where regulatory approval is not required, all requirements, except as noted below, go into effect on the first day of the first calendar quarter, 24 months after Board of Trustees adoption or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

   For 84 calendar months beginning the first day of the first calendar quarter following applicable regulatory approval, or in those jurisdictions where regulatory approval is not required on the first day of the first calendar quarter 84 months after Board of Trustees adoption or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities, Corrective Action Plans applying to the following categories of Contingencies and events identified in TPL-001-4, Table 1 are allowed to include Non-Consequential Load Loss and curtailment of Firm Transmission Service (in accordance with Requirement R2, Part 2.7.3.) that would not otherwise be permitted by the requirements of TPL-001-4:

   - P1-2 (for controlled interruption of electric supply to local network customers connected to or supplied by the Faulted element)
   - P1-3 (for controlled interruption of electric supply to local network customers connected to or supplied by the Faulted element)
   - P2-1
   - P2-2 (above 300 kV)
   - P2-3 (above 300 kV)
   - P3-1 through P3-5
   - P4-1 through P4-5 (above 300 kV)
   - P5 (above 300 kV)

B. Requirements

R1. Each Transmission Planner and Planning Coordinator shall maintain System models within its respective area for performing the studies needed to complete its Planning Assessment. The models shall use data consistent with that provided in accordance with the MOD-010 and MOD-012 standards, supplemented by other sources as needed, including items represented in the Corrective Action Plan, and shall represent projected System conditions. This establishes Category P0 as the normal System condition in Table 1. *[Violation Risk Factor: High] [Time Horizon: Long-term Planning]*

1.1. System models shall represent:

1.1.1. Existing Facilities

1.1.2. Known outage(s) of generation or Transmission Facility(ies) with a duration of at least six months.

1.1.3. New planned Facilities and changes to existing Facilities

1.1.4. Real and reactive Load forecasts

1.1.5. Known commitments for Firm Transmission Service and Interchange

1.1.6. Resources (supply or demand side) required for Load

R2. Each Transmission Planner and Planning Coordinator shall prepare an annual Planning Assessment of its portion of the BES. This Planning Assessment shall use current or qualified past studies (as indicated in Requirement R2, Part 2.6), document assumptions, and document summarized results of the steady state analyses, short circuit analyses, and Stability analyses. *[Violation Risk Factor: High] [Time Horizon: Long-term Planning]*

2.1. For the Planning Assessment, the Near-Term Transmission Planning Horizon portion of the steady state analysis shall be assessed annually and be supported by current annual studies or qualified past studies as indicated in Requirement R2, Part 2.6. Qualifying studies need to include the following conditions:

2.1.1. System peak Load for either Year One or year two, and for year five.

2.1.2. System Off-Peak Load for one of the five years.

2.1.3. P1 events in Table 1, with known outages modeled as in Requirement R1, Part 1.1.2, under those System peak or Off-Peak conditions when known outages are scheduled.

2.1.4. For each of the studies described in Requirement R2, Parts 2.1.1 and 2.1.2, sensitivity case(s) shall be utilized to demonstrate the impact of changes to the basic assumptions used in the model. To accomplish this, the sensitivity analysis in the Planning Assessment must vary one or more of the following conditions by a sufficient amount to stress the System within a range of credible conditions that demonstrate a measurable change in System response :

- Real and reactive forecasted Load.
- Expected transfers.
- Expected in service dates of new or modified Transmission Facilities.
- Reactive resource capability.
- Generation additions, retirements, or other dispatch scenarios.

- Controllable Loads and Demand Side Management.
- Duration or timing of known Transmission outages.

2.1.5. When an entity's spare equipment strategy could result in the unavailability of major Transmission equipment that has a lead time of one year or more (such as a transformer), the impact of this possible unavailability on System performance shall be studied. The studies shall be performed for the P0, P1, and P2 categories identified in Table 1 with the conditions that the System is expected to experience during the possible unavailability of the long lead time equipment.

2.2. For the Planning Assessment, the Long-Term Transmission Planning Horizon portion of the steady state analysis shall be assessed annually and be supported by the following annual current study, supplemented with qualified past studies as indicated in Requirement R2, Part 2.6:

2.2.1. A current study assessing expected System peak Load conditions for one of the years in the Long-Term Transmission Planning Horizon and the rationale for why that year was selected.

2.3. The short circuit analysis portion of the Planning Assessment shall be conducted annually addressing the Near-Term Transmission Planning Horizon and can be supported by current or past studies as qualified in Requirement R2, Part 2.6. The analysis shall be used to determine whether circuit breakers have interrupting capability for Faults that they will be expected to interrupt using the System short circuit model with any planned generation and Transmission Facilities in service which could impact the study area.

2.4. For the Planning Assessment, the Near-Term Transmission Planning Horizon portion of the Stability analysis shall be assessed annually and be supported by current or past studies as qualified in Requirement R2, Part2.6. The following studies are required:

2.4.1. System peak Load for one of the five years. System peak Load levels shall include a Load model which represents the expected dynamic behavior of Loads that could impact the study area, considering the behavior of induction motor Loads. An aggregate System Load model which represents the overall dynamic behavior of the Load is acceptable.

2.4.2. System Off-Peak Load for one of the five years.

2.4.3. For each of the studies described in Requirement R2, Parts 2.4.1 and 2.4.2, sensitivity case(s) shall be utilized to demonstrate the impact of changes to the basic assumptions used in the model. To accomplish this, the sensitivity analysis in the Planning Assessment must vary one or more of the following conditions by a sufficient amount to stress the System within a range of credible conditions that demonstrate a measurable change in performance:

- Load level, Load forecast, or dynamic Load model assumptions.
- Expected transfers.
- Expected in service dates of new or modified Transmission Facilities.
- Reactive resource capability.
- Generation additions, retirements, or other dispatch scenarios.

2.5. For the Planning Assessment, the Long-Term Transmission Planning Horizon portion of the Stability analysis shall be assessed to address the impact of proposed material generation additions or changes in that timeframe and be supported by current or past studies as qualified in Requirement R2, Part2.6 and shall include documentation to support the technical rationale for determining material changes.

2.6. Past studies may be used to support the Planning Assessment if they meet the following requirements:

2.6.1. For steady state, short circuit, or Stability analysis: the study shall be five calendar years old or less, unless a technical rationale can be provided to demonstrate that the results of an older study are still valid.

2.6.2. For steady state, short circuit, or Stability analysis: no material changes have occurred to the System represented in the study. Documentation to support the technical rationale for determining material changes shall be included.

2.7. For planning events shown in Table 1, when the analysis indicates an inability of the System to meet the performance requirements in Table 1, the Planning Assessment shall include Corrective Action Plan(s) addressing how the performance requirements will be met. Revisions to the Corrective Action Plan(s) are allowed in subsequent Planning Assessments but the planned System shall continue to meet the performance requirements in Table 1. Corrective Action Plan(s) do not need to be developed solely to meet the performance requirements for a single sensitivity case analyzed in accordance with Requirements R2, Parts 2.1.4 and 2.4.3. The Corrective Action Plan(s) shall:

2.7.1. List System deficiencies and the associated actions needed to achieve required System performance. Examples of such actions include:

- Installation, modification, retirement, or removal of Transmission and generation Facilities and any associated equipment.
- Installation, modification, or removal of Protection Systems or Special Protection Systems
- Installation or modification of automatic generation tripping as a response to a single or multiple Contingency to mitigate Stability performance violations.
- Installation or modification of manual and automatic generation runback/tripping as a response to a single or multiple Contingency to mitigate steady state performance violations.
- Use of Operating Procedures specifying how long they will be needed as part of the Corrective Action Plan.
- Use of rate applications, DSM, new technologies, or other initiatives.

2.7.2. Include actions to resolve performance deficiencies identified in multiple sensitivity studies or provide a rationale for why actions were not necessary.

2.7.3. If situations arise that are beyond the control of the Transmission Planner or Planning Coordinator that prevent the implementation of a Corrective Action Plan in the required timeframe, then the Transmission Planner or Planning Coordinator is permitted to utilize Non-Consequential Load Loss and curtailment of Firm Transmission Service to correct the situation that would normally not be permitted in Table 1, provided that the Transmission Planner

or Planning Coordinator documents that they are taking actions to resolve the situation. The Transmission Planner or Planning Coordinator shall document the situation causing the problem, alternatives evaluated, and the use of Non-Consequential Load Loss or curtailment of Firm Transmission Service.

2.7.4. Be reviewed in subsequent annual Planning Assessments for continued validity and implementation status of identified System Facilities and Operating Procedures.

2.8. For short circuit analysis, if the short circuit current interrupting duty on circuit breakers determined in Requirement R2, Part 2.3 exceeds their Equipment Rating, the Planning Assessment shall include a Corrective Action Plan to address the Equipment Rating violations. The Corrective Action Plan shall:

2.8.1. List System deficiencies and the associated actions needed to achieve required System performance.

2.8.2. Be reviewed in subsequent annual Planning Assessments for continued validity and implementation status of identified System Facilities and Operating Procedures.

R3. For the steady state portion of the Planning Assessment, each Transmission Planner and Planning Coordinator shall perform studies for the Near-Term and Long-Term Transmission Planning Horizons in Requirement R2, Parts 2.1, and 2.2. The studies shall be based on computer simulation models using data provided in Requirement R1. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

3.1. Studies shall be performed for planning events to determine whether the BES meets the performance requirements in Table 1 based on the Contingency list created in Requirement R3, Part 3.4.

3.2. Studies shall be performed to assess the impact of the extreme events which are identified by the list created in Requirement R3, Part 3.5.

3.3. Contingency analyses for Requirement R3, Parts 3.1 & 3.2 shall:

3.3.1. Simulate the removal of all elements that the Protection System and other automatic controls are expected to disconnect for each Contingency without operator intervention. The analyses shall include the impact of subsequent:

3.3.1.1. Tripping of generators where simulations show generator bus voltages or high side of the generation step up (GSU) voltages are less than known or assumed minimum generator steady state or ride through voltage limitations. Include in the assessment any assumptions made.

3.3.1.2. Tripping of Transmission elements where relay loadability limits are exceeded.

3.3.2. Simulate the expected automatic operation of existing and planned devices designed to provide steady state control of electrical system quantities when such devices impact the study area. These devices may include equipment such as phase-shifting transformers, load tap changing transformers, and switched capacitors and inductors.

3.4. Those planning events in Table 1, that are expected to produce more severe System impacts on its portion of the BES, shall be identified and a list of those Contingencies

to be evaluated for System performance in Requirement R3, Part 3.1 created. The rationale for those Contingencies selected for evaluation shall be available as supporting information.

3.4.1. The Planning Coordinator and Transmission Planner shall coordinate with adjacent Planning Coordinators and Transmission Planners to ensure that Contingencies on adjacent Systems which may impact their Systems are included in the Contingency list.

3.5. Those extreme events in Table 1 that are expected to produce more severe System impacts shall be identified and a list created of those events to be evaluated in Requirement R3, Part 3.2. The rationale for those Contingencies selected for evaluation shall be available as supporting information. If the analysis concludes there is Cascading caused by the occurrence of extreme events, an evaluation of possible actions designed to reduce the likelihood or mitigate the consequences and adverse impacts of the event(s) shall be conducted.

R4. For the Stability portion of the Planning Assessment, as described in Requirement R2, Parts 2.4 and 2.5, each Transmission Planner and Planning Coordinator shall perform the Contingency analyses listed in Table 1. The studies shall be based on computer simulation models using data provided in Requirement R1. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

4.1. Studies shall be performed for planning events to determine whether the BES meets the performance requirements in Table 1 based on the Contingency list created in Requirement R4, Part 4.4.

4.1.1. For planning event P1: No generating unit shall pull out of synchronism. A generator being disconnected from the System by fault clearing action or by a Special Protection System is not considered pulling out of synchronism.

4.1.2. For planning events P2 through P7: When a generator pulls out of synchronism in the simulations, the resulting apparent impedance swings shall not result in the tripping of any Transmission system elements other than the generating unit and its directly connected Facilities.

4.1.3. For planning events P1 through P7: Power oscillations shall exhibit acceptable damping as established by the Planning Coordinator and Transmission Planner.

4.2. Studies shall be performed to assess the impact of the extreme events which are identified by the list created in Requirement R4, Part 4.5.

4.3. Contingency analyses for Requirement R4, Parts 4.1 and 4.2 shall :

4.3.1. Simulate the removal of all elements that the Protection System and other automatic controls are expected to disconnect for each Contingency without operator intervention. The analyses shall include the impact of subsequent:

4.3.1.1. Successful high speed (less than one second) reclosing and unsuccessful high speed reclosing into a Fault where high speed reclosing is utilized.

4.3.1.2. Tripping of generators where simulations show generator bus voltages or high side of the GSU voltages are less than known or assumed generator low voltage ride through capability. Include in the assessment any assumptions made.

4.3.1.3. Tripping of Transmission lines and transformers where transient swings cause Protection System operation based on generic or actual relay models.

4.3.2. Simulate the expected automatic operation of existing and planned devices designed to provide dynamic control of electrical system quantities when such devices impact the study area. These devices may include equipment such as generation exciter control and power system stabilizers, static var compensators, power flow controllers, and DC Transmission controllers.

4.4. Those planning events in Table 1 that are expected to produce more severe System impacts on its portion of the BES, shall be identified, and a list created of those Contingencies to be evaluated in Requirement R4, Part 4.1. The rationale for those Contingencies selected for evaluation shall be available as supporting information.

4.4.1. Each Planning Coordinator and Transmission Planner shall coordinate with adjacent Planning Coordinators and Transmission Planners to ensure that Contingencies on adjacent Systems which may impact their Systems are included in the Contingency list.

4.5. Those extreme events in Table 1 that are expected to produce more severe System impacts shall be identified and a list created of those events to be evaluated in Requirement R4, Part 4.2. The rationale for those Contingencies selected for evaluation shall be available as supporting information. If the analysis concludes there is Cascading caused by the occurrence of extreme events, an evaluation of possible actions designed to reduce the likelihood or mitigate the consequences of the event(s) shall be conducted.

R5. Each Transmission Planner and Planning Coordinator shall have criteria for acceptable System steady state voltage limits, post-Contingency voltage deviations, and the transient voltage response for its System. For transient voltage response, the criteria shall at a minimum, specify a low voltage level and a maximum length of time that transient voltages may remain below that level. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

R6. Each Transmission Planner and Planning Coordinator shall define and document, within their Planning Assessment, the criteria or methodology used in the analysis to identify System instability for conditions such as Cascading, voltage instability, or uncontrolled islanding. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

R7. Each Planning Coordinator, in conjunction with each of its Transmission Planners, shall determine and identify each entity's individual and joint responsibilities for performing the required studies for the Planning Assessment. *[Violation Risk Factor: Low] [Time Horizon: Long-term Planning]*

R8. Each Planning Coordinator and Transmission Planner shall distribute its Planning Assessment results to adjacent Planning Coordinators and adjacent Transmission Planners within 90 calendar days of completing its Planning Assessment, and to any functional entity that has a reliability related need and submits a written request for the information within 30 days of such a request. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

8.1. If a recipient of the Planning Assessment results provides documented comments on the results, the respective Planning Coordinator or Transmission Planner shall provide a documented response to that recipient within 90 calendar days of receipt of those comments.

Table 1 – Steady State & Stability Performance Planning Events

Steady State & Stability:

a. The System shall remain stable. Cascading and uncontrolled islanding shall not occur.

b. Consequential Load Loss as well as generation loss is acceptable as a consequence of any event excluding P0.

c. Simulate the removal of all elements that Protection Systems and other controls are expected to automatically disconnect for each event.

d. Simulate Normal Clearing unless otherwise specified.

e. Planned System adjustments such as Transmission configuration changes and re-dispatch of generation are allowed if such adjustments are executable within the time duration applicable to the Facility Ratings.

Steady State Only:

f. Applicable Facility Ratings shall not be exceeded.

g. System steady state voltages and post-Contingency voltage deviations shall be within acceptable limits as established by the Planning Coordinator and the Transmission Planner.

h. Planning event P0 is applicable to steady state only.

i. The response of voltage sensitive Load that is disconnected from the System by end-user equipment associated with an event shall not be used to meet steady state performance requirements.

Stability Only:

j. Transient voltage response shall be within acceptable limits established by the Planning Coordinator and the Transmission Planner.

Category	Initial Condition	Event [1]	Fault Type [2]	BES Level [3]	Interruption of Firm Transmission Service Allowed [4]	Non-Consequential Load Loss Allowed
P0 No Contingency	Normal System	None	N/A	EHV, HV	No	No
P1 Single Contingency	Normal System	Loss of one of the following: 1. Generator 2. Transmission Circuit 3. Transformer [5] 4. Shunt Device [6]	3Ø	EHV, HV	No[9]	No[12]
		5. Single Pole of a DC line	SLG			
P2 Single Contingency	Normal System	1. Opening of a line section w/o a fault [7]	N/A	EHV, HV	No[9]	No[12]
		2. Bus Section Fault	SLG	EHV	No[9]	No
				HV	Yes	Yes
		3. Internal Breaker Fault [8] (non-Bus-tie Breaker)	SLG	EHV	No[9]	No
				HV	Yes	Yes
		4. Internal Breaker Fault (Bus-tie Breaker) [8]	SLG	EHV, HV	Yes	Yes

Category	Initial Condition	Event [1]	Fault Type [2]	BES Level [3]	Interruption of Firm Transmission Service Allowed [4]	Non-Consequential Load Loss Allowed
P3 Multiple Contingency	Loss of generator unit followed by System adjustments[9]	Loss of one of the following: 1. Generator 2. Transmission Circuit 3. Transformer [5] 4. Shunt Device [6]	3Ø	EHV, HV	No[9]	No[12]
		5. Single pole of a DC line	SLG			
P4 Multiple Contingency *(Fault plus stuck breaker[10])*	Normal System	Loss of multiple elements caused by a stuck breaker [10](non-Bus-tie Breaker) attempting to clear a Fault on one of the following: 1. Generator 2. Transmission Circuit 3. Transformer [5] 4. Shunt Device [6] 5. Bus Section	SLG	EHV	No[9]	No
				HV	Yes	Yes
		6. Loss of multiple elements caused by a stuck breaker[10] (Bus-tie Breaker) attempting to clear a Fault on the associated bus	SLG	EHV, HV	Yes	Yes
P5 Multiple Contingency *(Fault plus relay failure to operate)*	Normal System	Delayed Fault Clearing due to the failure of a non-redundant relay[13] protecting the Faulted element to operate as designed, for one of the following: 1. Generator 2. Transmission Circuit 3. Transformer [5] 4. Shunt Device [6] 5. Bus Section	SLG	EHV	No[9]	No
				HV	Yes	Yes
P6 Multiple Contingency *(Two overlapping singles)*	Loss of one of the following followed by System adjustments.[9] 1. Transmission Circuit 2. Transformer [5] 3. Shunt Device[6] 4. Single pole of a DC line	Loss of one of the following: 1. Transmission Circuit 2. Transformer [5] 3. Shunt Device [6]	3Ø	EHV, HV	Yes	Yes
		4. Single pole of a DC line	SLG	EHV, HV	Yes	Yes

Category	Initial Condition	Event [1]	Fault Type [2]	BES Level [3]	Interruption of Firm Transmission Service Allowed [4]	Non-Consequential Load Loss Allowed
P7 Multiple Contingency *(Common Structure)*	Normal System	The loss of: 1. Any two adjacent (vertically or horizontally) circuits on common structure [11] 2. Loss of a bipolar DC line	SLG	EHV, HV	Yes	Yes

Table 1 – Steady State & Stability Performance Extreme Events

Steady State & Stability

For all extreme events evaluated:

a. Simulate the removal of all elements that Protection Systems and automatic controls are expected to disconnect for each Contingency.

b. Simulate Normal Clearing unless otherwise specified.

Steady State

1. Loss of a single generator, Transmission Circuit, single pole of a DC Line, shunt device, or transformer forced out of service followed by another single generator, Transmission Circuit, single pole of a different DC Line, shunt device, or transformer forced out of service prior to System adjustments.
2. Local area events affecting the Transmission System such as:
   a. Loss of a tower line with three or more circuits.[11]
   b. Loss of all Transmission lines on a common Right-of-Way[11].
   c. Loss of a switching station or substation (loss of one voltage level plus transformers).
   d. Loss of all generating units at a generating station.
   e. Loss of a large Load or major Load center.
3. Wide area events affecting the Transmission System based on System topology such as:
   a. Loss of two generating stations resulting from conditions such as:
      i. Loss of a large gas pipeline into a region or multiple regions that have significant gas-fired generation.
      ii. Loss of the use of a large body of water as the cooling source for generation.
      iii. Wildfires.
      iv. Severe weather, e.g., hurricanes, tornadoes, etc.
      v. A successful cyber attack.
      vi. Shutdown of a nuclear power plant(s) and related facilities for a day or more for common causes such as problems with similarly designed plants.
   b. Other events based upon operating experience that may result in wide area disturbances.

Stability

1. With an initial condition of a single generator, Transmission circuit, single pole of a DC line, shunt device, or transformer forced out of service, apply a 3Ø fault on another single generator, Transmission circuit, single pole of a different DC line, shunt device, or transformer prior to System adjustments.
2. Local or wide area events affecting the Transmission System such as:
   a. 3Ø fault on generator with stuck breaker[10] or a relay failure[13] resulting in Delayed Fault Clearing.
   b. 3Ø fault on Transmission circuit with stuck breaker[10] or a relay failure[13] resulting in Delayed Fault Clearing.
   c. 3Ø fault on transformer with stuck breaker[10] or a relay failure[13] resulting in Delayed Fault Clearing.
   d. 3Ø fault on bus section with stuck breaker[10] or a relay failure[13] resulting in Delayed Fault Clearing.
   e. 3Ø internal breaker fault.
   f. Other events based upon operating experience, such as consideration of initiating events that experience suggests may result in wide area disturbances

Table 1 – Steady State & Stability Performance Footnotes (Planning Events and Extreme Events)
1. If the event analyzed involves BES elements at multiple System voltage levels, the lowest System voltage level of the element(s) removed for the analyzed event determines the stated performance criteria regarding allowances for interruptions of Firm Transmission Service and Non-Consequential Load Loss.
2. Unless specified otherwise, simulate Normal Clearing of faults. Single line to ground (SLG) or three-phase (3Ø) are the fault types that must be evaluated in Stability simulations for the event described. A 3Ø or a double line to ground fault study indicating the criteria are being met is sufficient evidence that a SLG condition would also meet the criteria.
3. Bulk Electric System (BES) level references include extra-high voltage (EHV) Facilities defined as greater than 300kV and high voltage (HV) Facilities defined as the 300kV and lower voltage Systems. The designation of EHV and HV is used to distinguish between stated performance criteria allowances for interruption of Firm Transmission Service and Non-Consequential Load Loss.
4. Curtailment of Conditional Firm Transmission Service is allowed when the conditions and/or events being studied formed the basis for the Conditional Firm Transmission Service.
5. For non-generator step up transformer outage events, the reference voltage, as used in footnote 1, applies to the low-side winding (excluding tertiary windings). For generator and Generator Step Up transformer outage events, the reference voltage applies to the BES connected voltage (high-side of the Generator Step Up transformer). Requirements which are applicable to transformers also apply to variable frequency transformers and phase shifting transformers.
6. Requirements which are applicable to shunt devices also apply to FACTS devices that are connected to ground.
7. Opening one end of a line section without a fault on a normally networked Transmission circuit such that the line is possibly serving Load radial from a single source point.
8. An internal breaker fault means a breaker failing internally, thus creating a System fault which must be cleared by protection on both sides of the breaker.
9. An objective of the planning process should be to minimize the likelihood and magnitude of interruption of Firm Transmission Service following Contingency events. Curtailment of Firm Transmission Service is allowed both as a System adjustment (as identified in the column entitled 'Initial Condition') and a corrective action when achieved through the appropriate re-dispatch of resources obligated to re-dispatch, where it can be demonstrated that Facilities, internal and external to the Transmission Planner's planning region, remain within applicable Facility Ratings and the re-dispatch does not result in any Non-Consequential Load Loss. Where limited options for re-dispatch exist, sensitivities associated with the availability of those resources should be considered.
10. A stuck breaker means that for a gang-operated breaker, all three phases of the breaker have remained closed. For an independent pole operated (IPO) or an independent pole tripping (IPT) breaker, only one pole is assumed to remain closed. A stuck breaker results in Delayed Fault Clearing.
11. Excludes circuits that share a common structure (Planning event P7, Extreme event steady state 2a) or common Right-of-Way (Extreme event, steady state 2b) for 1 mile or less.
12. An objective of the planning process is to minimize the likelihood and magnitude of Non-Consequential Load Loss following planning events. In limited circumstances, Non-Consequential Load Loss may be needed throughout the planning horizon to ensure that BES performance requirements are met. However, when Non-Consequential Load Loss is utilized under footnote 12 within the Near-Term Transmission Planning Horizon to address BES performance requirements, such interruption is limited to circumstances where the Non-Consequential Load Loss meets the conditions shown in Attachment 1. In no case can the planned Non-Consequential Load Loss under footnote 12 exceed 75 MW for US registered entities. The amount of planned Non-Consequential Load Loss for a non-US Registered Entity should be implemented in a manner that is consistent with, or under the direction of, the applicable governmental authority or its agency in the non-US jurisdiction.
13. Applies to the following relay functions or types: pilot (#85), distance (#21), differential (#87), current (#50, 51, and 67), voltage (#27 & 59), directional (#32, &

Table 1 – Steady State & Stability Performance Footnotes (Planning Events and Extreme Events)
67), and tripping (#86, & 94).

Attachment 1

I. Stakeholder Process

During each Planning Assessment before the use of Non-Consequential Load Loss under footnote 12 is allowed as an element of a Corrective Action Plan in the Near-Term Transmission Planning Horizon of the Planning Assessment, the Transmission Planner or Planning Coordinator shall ensure that the utilization of footnote 12 is reviewed through an open and transparent stakeholder process. The responsible entity can utilize an existing process or develop a new process. .The process must include the following:

1. Meetings must be open to affected stakeholders including applicable regulatory authorities or governing bodies responsible for retail electric service issues
2. Notice must be provided in advance of meetings to affected stakeholders including applicable regulatory authorities or governing bodies responsible for retail electric service issues and include an agenda with:
    a. Date, time, and location for the meeting
    b. Specific location(s) of the planned Non-Consequential Load Loss under footnote 12
    c. Provisions for a stakeholder comment period
3. Information regarding the intended purpose and scope of the proposed Non-Consequential Load Loss under footnote 12 (as shown in Section II below) must be made available to meeting participants
4. A procedure for stakeholders to submit written questions or concerns and to receive written responses to the submitted questions and concerns
5. A dispute resolution process for any question or concern raised in #4 above that is not resolved to the stakeholder's satisfaction

An entity does not have to repeat the stakeholder process for a specific application of footnote 12 utilization with respect to subsequent Planning Assessments unless conditions spelled out in Section II below have materially changed for that specific application.

II. Information for Inclusion in Item #3 of the Stakeholder Process

The responsible entity shall document the planned use of Non-Consequential Load Loss under footnote 12 which must include the following:

1. Conditions under which Non-Consequential Load Loss under footnote 12 would be necessary:
    a. System Load level and estimated annual hours of exposure at or above that Load level
    b. Applicable Contingencies and the Facilities outside their applicable rating due to that Contingency
2. Amount of Non-Consequential Load Loss with:
    a. The estimated number and type of customers affected

   b. An explanation of the effect of the use of Non-Consequential Load Loss under footnote 12 on the health, safety, and welfare of the community
3. Estimated frequency of Non-Consequential Load Loss under footnote 12 based on historical performance
4. Expected duration of Non-Consequential Load Loss under footnote 12 based on historical performance
5. Future plans to alleviate the need for Non-Consequential Load Loss under footnote 12
6. Verification that TPL Reliability Standards performance requirements will be met following the application of footnote 12
7. Alternatives to Non-Consequential Load Loss considered and the rationale for not selecting those alternatives under footnote 12
8. Assessment of potential overlapping uses of footnote 12 including overlaps with adjacent Transmission Planners and Planning Coordinators

III. Instances for which Regulatory Review of Non-Consequential Load Loss under Footnote 12 is Required

Before a Non-Consequential Load Loss under footnote 12 is allowed as an element of a Corrective Action Plan in Year One of the Planning Assessment, the Transmission Planner or Planning Coordinator must ensure that the applicable regulatory authorities or governing bodies responsible for retail electric service issues do not object to the use of Non-Consequential Load Loss under footnote 12 if either:

1. The voltage level of the Contingency is greater than 300 kV
   a. If the Contingency analyzed involves BES Elements at multiple System voltage levels, the lowest System voltage level of the element(s) removed for the analyzed Contingency determines the stated performance criteria regarding allowances for Non-Consequential Load Loss under footnote 12, or
   b. For a non-generator step up transformer outage Contingency, the 300 kV limit applies to the low-side winding (excluding tertiary windings). For a generator or generator step up transformer outage Contingency, the 300 kV limit applies to the BES connected voltage (high-side of the Generator Step Up transformer)
2. The planned Non-Consequential Load Loss under footnote 12 is greater than or equal to 25 MW

Once assurance has been received that the applicable regulatory authorities or governing bodies responsible for retail electric service issues do not object to the use of Non-Consequential Load Loss under footnote 12, the Planning Coordinator or Transmission Planner must submit the information outlined in items II.1 through II.8 above to the ERO for a determination of whether there are any Adverse Reliability Impacts caused by the request to utilize footnote 12 for Non-Consequential Load Loss.

C. Measures

M1. Each Transmission Planner and Planning Coordinator shall provide evidence, in electronic or hard copy format, that it is maintaining System models within their respective area, using data consistent with MOD-010 and MOD-012, including items represented in the Corrective Action Plan, representing projected System conditions, and that the models represent the required information in accordance with Requirement R1.

M2. Each Transmission Planner and Planning Coordinator shall provide dated evidence, such as electronic or hard copies of its annual Planning Assessment, that it has prepared an annual Planning Assessment of its portion of the BES in accordance with Requirement R2.

M3. Each Transmission Planner and Planning Coordinator shall provide dated evidence, such as electronic or hard copies of the studies utilized in preparing the Planning Assessment, in accordance with Requirement R3.

M4. Each Transmission Planner and Planning Coordinator shall provide dated evidence, such as electronic or hard copies of the studies utilized in preparing the Planning Assessment in accordance with Requirement R4.

M5. Each Transmission Planner and Planning Coordinator shall provide dated evidence such as electronic or hard copies of the documentation specifying the criteria for acceptable System steady state voltage limits, post-Contingency voltage deviations, and the transient voltage response for its System in accordance with Requirement R5.

M6. Each Transmission Planner and Planning Coordinator shall provide dated evidence, such as electronic or hard copies of documentation specifying the criteria or methodology used in the analysis to identify System instability for conditions such as Cascading, voltage instability, or uncontrolled islanding that was utilized in preparing the Planning Assessment in accordance with Requirement R6.

M7. Each Planning Coordinator, in conjunction with each of its Transmission Planners, shall provide dated documentation on roles and responsibilities, such as meeting minutes, agreements, and e-mail correspondence that identifies that agreement has been reached on individual and joint responsibilities for performing the required studies and Assessments in accordance with Requirement R7.

M8. Each Planning Coordinator and Transmission Planner shall provide evidence, such as email notices, documentation of updated web pages, postal receipts showing recipient and date; or a demonstration of a public posting, that it has distributed its Planning Assessment results to adjacent Planning Coordinators and adjacent Transmission Planners within 90 days of having completed its Planning Assessment, and to any functional entity who has indicated a reliability need within 30 days of a written request and that the Planning Coordinator or Transmission Planner has provided a documented response to comments received on Planning Assessment results within 90 calendar days of receipt of those comments in accordance with Requirement R8.

D. Compliance

1. Compliance Monitoring Process

1.1 Compliance Enforcement Authority

Regional Entity

1.2 Compliance Monitoring Period and Reset Timeframe

Not applicable.

1.3 Compliance Monitoring and Enforcement Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4 Data Retention

The Transmission Planner and Planning Coordinator shall each retain data or evidence to show compliance as identified unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation:

- The models utilized in the current in-force Planning Assessment and one previous Planning Assessment in accordance with Requirement R1 and Measure M1.
- The Planning Assessments performed since the last compliance audit in accordance with Requirement R2 and Measure M2.
- The studies performed in support of its Planning Assessments since the last compliance audit in accordance with Requirement R3 and Measure M3.
- The studies performed in support of its Planning Assessments since the last compliance audit in accordance with Requirement R4 and Measure M4.
- The documentation specifying the criteria for acceptable System steady state voltage limits, post-Contingency voltage deviations, and transient voltage response since the last compliance audit in accordance with Requirement R5 and Measure M5.
- The documentation specifying the criteria or methodology utilized in the analysis to identify System instability for conditions such as Cascading, voltage instability, or uncontrolled islanding in support of its Planning Assessments since the last compliance audit in accordance with Requirement R6 and Measure M6.
- The current, in force documentation for the agreement(s) on roles and responsibilities, as well as documentation for the agreements in force since the last compliance audit, in accordance with Requirement R7 and Measure M7.

The Planning Coordinator shall retain data or evidence to show compliance as identified unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation:

- Three calendar years of the notifications employed in accordance with Requirement R8 and Measure M8.

If a Transmission Planner or Planning Coordinator is found non-compliant, it shall keep information related to the non-compliance until found compliant or the time periods specified above, whichever is longer.

1.5 Additional Compliance Information

None

2. Violation Severity Levels

	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	The responsible entity's System model failed to represent one of the Requirement R1, Parts 1.1.1 through 1.1.6.	The responsible entity's System model failed to represent two of the Requirement R1, Parts 1.1.1 through 1.1.6.	The responsible entity's System model failed to represent three of the Requirement R1, Parts 1.1.1 through 1.1.6.	The responsible entity's System model failed to represent four or more of the Requirement R1, Parts 1.1.1 through 1.1.6. OR The responsible entity's System model did not represent projected System conditions as described in Requirement R1. OR The responsible entity's System model did not use data consistent with that provided in accordance with the MOD-010 and MOD-012 standards and other sources, including items represented in the Corrective Action Plan.
R2	The responsible entity failed to comply with Requirement R2, Part 2.6.	The responsible entity failed to comply with Requirement R2, Part 2.3 or Part 2.8.	The responsible entity failed to comply with one of the following Parts of Requirement R2: Part 2.1, Part 2.2, Part 2.4, Part 2.5, or Part 2.7.	The responsible entity failed to comply with two or more of the following Parts of Requirement R2: Part 2.1, Part 2.2, Part 2.4, or Part 2.7. OR The responsible entity does not have a completed annual Planning Assessment.
R3	The responsible entity did not identify planning events as described in Requirement R3, Part 3.4 or extreme events as described in Requirement R3, Part 3.5.	The responsible entity did not perform studies as specified in Requirement R3, Part 3.1 to determine that the BES meets the performance requirements for one of the categories (P2 through P7) in Table 1.	The responsible entity did not perform studies as specified in Requirement R3, Part 3.1 to determine that the BES meets the performance requirements for two of the categories (P2 through P7) in	The responsible entity did not perform studies as specified in Requirement R3, Part 3.1 to determine that the BES meets the performance requirements for three or more of the categories (P2 through P7) in Table 1.

	Lower VSL	Moderate VSL	High VSL	Severe VSL
		OR The responsible entity did not perform studies as specified in Requirement R3, Part 3.2 to assess the impact of extreme events.	Table 1. OR The responsible entity did not perform Contingency analysis as described in Requirement R3, Part 3.3.	OR The responsible entity did not perform studies to determine that the BES meets the performance requirements for the P0 or P1 categories in Table 1. OR The responsible entity did not base its studies on computer simulation models using data provided in Requirement R1.
R4	The responsible entity did not identify planning events as described in Requirement R4, Part 4.4 or extreme events as described in Requirement R4, Part 4.5.	The responsible entity did not perform studies as specified in Requirement R4, Part 4.1 to determine that the BES meets the performance requirements for one of the categories (P1 through P7) in Table 1. OR The responsible entity did not perform studies as specified in Requirement R4, Part 4.2 to assess the impact of extreme events.	The responsible entity did not perform studies as specified in Requirement R4, Part 4.1 to determine that the BES meets the performance requirements for two of the categories (P1 through P7) in Table 1. OR The responsible entity did not perform Contingency analysis as described in Requirement R4, Part 4.3.	The responsible entity did not perform studies as specified in Requirement R4, Part 4.1 to determine that the BES meets the performance requirements for three or more of the categories (P1 through P7) in Table 1. OR The responsible entity did not base its studies on computer simulation models using data provided in Requirement R1.
R5	N/A	N/A	N/A	The responsible entity does not have criteria for acceptable System steady state voltage limits, post-Contingency voltage deviations, or the transient voltage response for its System.
R6	N/A	N/A	N/A	The responsible entity failed to define and document the criteria or methodology for System instability used within its analysis as described in Requirement R6.

	Lower VSL	Moderate VSL	High VSL	Severe VSL
R7	N/A	N/A	N/A	The Planning Coordinator, in conjunction with each of its Transmission Planners, failed to determine and identify individual or joint responsibilities for performing required studies.
R8	The responsible entity distributed its Planning Assessment results to adjacent Planning Coordinators and adjacent Transmission Planners but it was more than 90 days but less than or equal to 120 days following its completion. OR, The responsible entity distributed its Planning Assessment results to functional entities having a reliability related need who requested the Planning Assessment in writing but it was more than 30 days but less than or equal to 40 days following the request.	The responsible entity distributed its Planning Assessment results to adjacent Planning Coordinators and adjacent Transmission Planners but it was more than 120 days but less than or equal to 130 days following its completion. OR, The responsible entity distributed its Planning Assessment results to functional entities having a reliability related need who requested the Planning Assessment in writing but it was more than 40 days but less than or equal to 50 days following the request.	The responsible entity distributed its Planning Assessment results to adjacent Planning Coordinators and adjacent Transmission Planners but it was more than 130 days but less than or equal to 140 days following its completion. OR, The responsible entity distributed its Planning Assessment results to functional entities having a reliability related need who requested the Planning Assessment in writing but it was more than 50 days but less than or equal to 60 days following the request.	The responsible entity distributed its Planning Assessment results to adjacent Planning Coordinators and adjacent Transmission Planners but it was more than 140 days following its completion. OR The responsible entity did not distribute its Planning Assessment results to adjacent Planning Coordinators and adjacent Transmission Planners. OR The responsible entity distributed its Planning Assessment results to functional entities having a reliability related need who requested the Planning Assessment in writing but it was more than 60 days following the request. OR The responsible entity did not distribute its Planning Assessment results to functional entities having a reliability related need who requested the Planning Assessment in writing.

E. Regional Variances

None.

Version History

Version	Date	Action	Change Tracking
0	April 1, 2005	Effective Date	New
0	February 8, 2005	BOT Approval	Revised
0	June 3, 2005	Fixed reference in M1 to read TPL-001-0 R2.1 and TPL-001-0 R2.2	Errata
0	July 24, 2007	Corrected reference in M1. to read TPL-001-0 R1 and TPL-001-0 R2.	Errata
0.1	October 29, 2008	BOT adopted errata changes; updated version number to "0.1"	Errata
0.1	May 13, 2009	FERC Approved – Updated Effective Date and Footer	Revised
1	Approved by Board of Trustees February 17, 2011	Revised footnote 'b' pursuant to FERC Order RM06-16-009	Revised (Project 2010-11)
2	August 4, 2011	Revision of TPL-001-1; includes merging and upgrading requirements of TPL-001-0, TPL-002-0, TPL-003-0, and TPL-004-0 into one, single, comprehensive, coordinated standard: TPL-001-2; and retirement of TPL-005-0 and TPL-006-0.	Project 2006-02 – complete revision
2	August 4, 2011	Adopted by Board of Trustees	
1	April 19, 2012	FERC issued Order 762 remanding TPL-001-1, TPL-002-1b, TPL-003-1a, and TPL-004-1. FERC also issued a NOPR proposing to remand TPL-001-2. NERC has been directed to revise footnote 'b' in accordance with the directives of Order Nos. 762 and 693.	
3	February 7, 2013	Adopted by the NERC Board of Trustees. TPL-001-3 was created after the Board of Trustees approved the revised footnote 'b' in TPL-002-2b, which was balloted and appended to: TPL-001-0.1, TPL-002-0b, TPL-003-0a, and TPL-004-0.	
4	February 7, 2013	Adopted by the NERC Board of Trustees. TPL-001-4 was adopted by the Board of Trustees as TPL-001-3, but a discrepancy in numbering was identified and corrected prior to filing with the regulatory agencies.	
4	October 17, 2013	FERC Order issued approving TPL-001-4 (Order effective December 23, 2013).	
4	May 7, 2014	NERC Board of Trustees adopted change to VRF in Requirement 1 from Medium to High.	

Appendix QC-TPL-001-4
Provisions specific to the standard TPL-001-4 applicable in Québec

This appendix establishes specific provisions for the application of the standard in Québec. Provisions of the standard and of its appendix must be read together for the purposes of understanding and interpretation. Where the standard and appendix differ, the appendix shall prevail.

A. Introduction

1. Title: **Transmission System Planning Performance Requirements**

2. Number: TPL-001-4

3. Purpose: No specific provision

4. Applicability:

4.1. Functional entities

No specific provision

Facilities

This standard only applies to the facilities of the Bulk Power System (BPS)

5. Effective Date:

5.1. Adoption of the standard by the Régie de l'énergie: September 27, 2017

5.2. Adoption of the appendix by the Régie de l'énergie: September 27, 2017

5.3. Effective date of the standard and its appendix in Québec: October 1st, 2017. However, before January 1, 2022, Corrective Action Plans applying to the following categories of Contingencies and events identified in TPL-001-4, Table 1 are allowed to include Non-Consequential Load Loss and curtailment of Firm Transmission Service (in accordance with Requirement R2, Part 2.7.3) that would not otherwise be permitted by the requirements of TPL-001-4 :

- P1-2 (for controlled interruption of electric supply to local network customers connected to or supplied by the Faulted element)
- P1-3 (for controlled interruption of electric supply to local network customers connected to or supplied by the Faulted element)
- P2-1
- P2-2 (above 300 kV)
- P2-3 (above 300 kV)
- P3-1 through P3-5
- P4-1 through P4-5 (above 300 kV)
- P5 (above 300 kV)

B. Requirements

Specific provision applicable to requirement E1 : Every reference to the standards MOD-010 and MOD-012 is replaced by reference to the standard MOD-032-1.

C. Measures

No specific provision

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

The Régie de l'énergie is responsible, in Québec, for compliance monitoring with respect to the reliability standard and its appendix that it adopts.

1.2. Compliance Monitoring Period and Reset Timeframe

No specific provision

1.3. Compliance Monitoring and Enforcement Processes:

No specific provision

1.4. Data Retention

No specific provision

1.5. Additional Compliance Information

No specific provision

2. Violation Severity Levels

No specific provision

E. Regional Variances

No specific provision

Table 1

This table only applies to the facilities of the Bulk Power System (BPS) for:

- Categories
- Contingencies
- System Limits or Impacts

Attachment 1

No specific provision

Revision History

Version	Date	Action	Change Tracking
0	September 27, 2017	New appendix	New

A. Introduction

1. **Title:** Transmission System Planned Performance for Geomagnetic Disturbance Events

2. **Number:** TPL-007-4

3. **Purpose:** Establish requirements for Transmission system planned performance during geomagnetic disturbance (GMD) events.

4. **Applicability:**

   4.1. Functional Entities:

   4.1.1. Planning Coordinator with a planning area that includes a Facility or Facilities specified in 4.2;

   4.1.2. Transmission Planner with a planning area that includes a Facility or Facilities specified in 4.2;

   4.1.3. Transmission Owner who owns a Facility or Facilities specified in 4.2; and

   4.1.4. Generator Owner who owns a Facility or Facilities specified in 4.2.

   4.2. Facilities:

   4.2.1. Facilities that include power transformer(s) with a high side, wye-grounded winding with terminal voltage greater than 200 kV.

5. **Effective Date:** See Implementation Plan for TPL-007-4.

6. **Background:** During a GMD event, geomagnetically-induced currents (GIC) may cause transformer hot-spot heating or damage, loss of Reactive Power sources, increased Reactive Power demand, and Misoperation(s), the combination of which may result in voltage collapse and blackout.

B. Requirements and Measures

R1. Each Planning Coordinator, in conjunction with its Transmission Planner(s), shall identify the individual and joint responsibilities of the Planning Coordinator and Transmission Planner(s) in the Planning Coordinator's planning area for maintaining models, performing the study or studies needed to complete benchmark and supplemental GMD Vulnerability Assessments, and implementing process(es) to obtain GMD measurement data as specified in this standard. *[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*

M1. Each Planning Coordinator, in conjunction with its Transmission Planners, shall provide documentation on roles and responsibilities, such as meeting minutes, agreements, copies of procedures or protocols in effect between entities or between departments of a vertically integrated system, or email correspondence that identifies an agreement has been reached on individual and joint responsibilities for maintaining models, performing the study or studies needed to complete benchmark and supplemental GMD Vulnerability Assessments, and implementing process(es) to obtain GMD measurement data in accordance with Requirement R1.

R2. Each responsible entity, as determined in Requirement R1, shall maintain System models and GIC System models of the responsible entity's planning area for performing the study or studies needed to complete benchmark and supplemental GMD Vulnerability Assessments*. [Violation Risk Factor: High] [Time Horizon: Long-term Planning]*

M2. Each responsible entity, as determined in Requirement R1, shall have evidence in either electronic or hard copy format that it is maintaining System models and GIC System models of the responsible entity's planning area for performing the study or studies needed to complete benchmark and supplemental GMD Vulnerability Assessments.

R3. Each responsible entity, as determined in Requirement R1, shall have criteria for acceptable System steady state voltage performance for its System during the GMD events described in Attachment 1*. [Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

M3. Each responsible entity, as determined in Requirement R1, shall have evidence, such as electronic or hard copies of the criteria for acceptable System steady state voltage performance for its System in accordance with Requirement R3.

Benchmark GMD Vulnerability Assessment(s)

R4. Each responsible entity, as determined in Requirement R1, shall complete a benchmark GMD Vulnerability Assessment of the Near-Term Transmission Planning Horizon at least once every 60 calendar months. This benchmark GMD Vulnerability Assessment shall use a study or studies based on models identified in Requirement R2, document assumptions, and document summarized results of the steady state analysis. *[Violation Risk Factor: High] [Time Horizon: Long-term Planning]*

4.1. The study or studies shall include the following conditions:

4.1.1. System On-Peak Load for at least one year within the Near-Term Transmission Planning Horizon; and

4.1.2. System Off-Peak Load for at least one year within the Near-Term Transmission Planning Horizon.

4.2. The study or studies shall be conducted based on the benchmark GMD event described in Attachment 1 to determine whether the System meets the performance requirements for the steady state planning benchmark GMD event contained in Table 1.

4.3. The benchmark GMD Vulnerability Assessment shall be provided: (i) to the responsible entity's Reliability Coordinator, adjacent Planning Coordinators, and adjacent Transmission Planners within 90 calendar days of completion, and (ii) to any functional entity that submits a written request and has a reliability-related need within 90 calendar days of receipt of such request or within 90 calendar days of completion of the benchmark GMD Vulnerability Assessment, whichever is later.

4.3.1. If a recipient of the benchmark GMD Vulnerability Assessment provides documented comments on the results, the responsible entity shall provide a documented response to that recipient within 90 calendar days of receipt of those comments.

M4. Each responsible entity, as determined in Requirement R1, shall have dated evidence such as electronic or hard copies of its benchmark GMD Vulnerability Assessment meeting all of the requirements in Requirement R4. Each responsible entity, as determined in Requirement R1, shall also provide evidence, such as email records, web postings with an electronic notice of posting, or postal receipts showing recipient and date, that it has distributed its benchmark GMD Vulnerability Assessment: (i) to the responsible entity's Reliability Coordinator, adjacent Planning Coordinators, and adjacent Transmission Planners within 90 calendar days of completion, and (ii) to any functional entity that submits a written request and has a reliability-related need within 90 calendar days of receipt of such request or within 90 calendar days of completion of the benchmark GMD Vulnerability Assessment, whichever is later, as specified in Requirement R4. Each responsible entity, as determined in Requirement R1, shall also provide evidence, such as email notices or postal receipts showing recipient and date, that it has provided a documented response to comments received on its benchmark GMD Vulnerability Assessment within 90 calendar days of receipt of those comments in accordance with Requirement R4.

R5. Each responsible entity, as determined in Requirement R1, shall provide GIC flow information to be used for the benchmark thermal impact assessment of transformers specified in Requirement R6 to each Transmission Owner and Generator Owner that owns an applicable Bulk Electric System (BES) power transformer in the planning area. The GIC flow information shall include: *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

5.1. The maximum effective GIC value for the worst case geoelectric field orientation for the benchmark GMD event described in Attachment 1. This value shall be provided to the Transmission Owner or Generator Owner that owns each applicable BES power transformer in the planning area.

5.2. The effective GIC time series, GIC(t), calculated using the benchmark GMD event described in Attachment 1 in response to a written request from the Transmission Owner or Generator Owner that owns an applicable BES power transformer in the planning area. GIC(t) shall be provided within 90 calendar days of receipt of the written request and after determination of the maximum effective GIC value in Part 5.1.

M5. Each responsible entity, as determined in Requirement R1, shall provide evidence, such as email records, web postings with an electronic notice of posting, or postal receipts showing recipient and date, that it has provided the maximum effective GIC values to the Transmission Owner and Generator Owner that owns each applicable BES power transformer in the planning area as specified in Requirement R5, Part 5.1. Each responsible entity, as determined in Requirement R1, shall also provide evidence, such as email records, web postings with an electronic notice of posting, or postal receipts showing recipient and date, that it has provided GIC(t) in response to a written request from the Transmission Owner or Generator Owner that owns an applicable BES power transformer in the planning area.

R6. Each Transmission Owner and Generator Owner shall conduct a benchmark thermal impact assessment for its solely and jointly owned applicable BES power transformers where the maximum effective GIC value provided in Requirement R5, Part 5.1, is 75 A per phase or greater. The benchmark thermal impact assessment shall: *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

6.1. Be based on the effective GIC flow information provided in Requirement R5;

6.2. Document assumptions used in the analysis;

6.3. Describe suggested actions and supporting analysis to mitigate the impact of GICs, if any; and

6.4. Be performed and provided to the responsible entities, as determined in Requirement R1, within 24 calendar months of receiving GIC flow information specified in Requirement R5, Part 5.1.

M6. Each Transmission Owner and Generator Owner shall have evidence such as electronic or hard copies of its benchmark thermal impact assessment for all of its solely and jointly owned applicable BES power transformers where the maximum effective GIC value provided in Requirement R5, Part 5.1, is 75 A per phase or greater, and shall have evidence such as email records, web postings with an electronic notice of posting, or postal receipts showing recipient and date, that it has provided its thermal impact assessment to the responsible entities as specified in Requirement R6.

R7. Each responsible entity, as determined in Requirement R1, that concludes through the benchmark GMD Vulnerability Assessment conducted in Requirement R4 that their System does not meet the performance requirements for the steady state planning benchmark GMD event contained in Table 1, shall develop a Corrective

Action Plan (CAP) addressing how the performance requirements will be met. The CAP shall: *[Violation Risk Factor: High] [Time Horizon: Long-term Planning]*

7.1. List System deficiencies and the associated actions needed to achieve required System performance. Examples of such actions include:

- Installation, modification, retirement, or removal of Transmission and generation Facilities and any associated equipment.
- Installation, modification, or removal of Protection Systems or Remedial Action Schemes.
- Use of Operating Procedures, specifying how long they will be needed as part of the CAP.
- Use of Demand-Side Management, new technologies, or other initiatives.

7.2. Be developed within one year of completion of the benchmark GMD Vulnerability Assessment.

7.3. Include a timetable, subject to approval for any extension sought under Part 7.4, for implementing the selected actions from Part 7.1. The timetable shall:

7.3.1. Specify implementation of non-hardware mitigation, if any, within two years of development of the CAP; and

7.3.2. Specify implementation of hardware mitigation, if any, within four years of development of the CAP.

7.4. Be submitted to the Compliance Enforcement Authority (CEA) with a request for extension of time if the responsible entity is unable to implement the CAP within the timetable provided in Part 7.3. The submitted CAP shall document the following:

7.4.1. Circumstances causing the delay for fully or partially implementing the selected actions in Part 7.1 and how those circumstances are beyond the control of the responsible entity;

7.4.2. Revisions to the selected actions in Part 7.1, if any, including utilization of Operating Procedures, if applicable; and

7.4.3. Updated timetable for implementing the selected actions in Part 7.1.

7.5. Be provided: (i) to the responsible entity's Reliability Coordinator, adjacent Planning Coordinator(s), adjacent Transmission Planner(s), and functional entities referenced in the CAP within 90 calendar days of development or revision, and (ii) to any functional entity that submits a written request and has a reliability-related need within 90 calendar days of receipt of such request or within 90 calendar days of development or revision, whichever is later.

7.5.1. If a recipient of the CAP provides documented comments on the CAP, the responsible entity shall provide a documented response to that recipient within 90 calendar days of receipt of those comments.

M7. Each responsible entity, as determined in Requirement R1, that concludes, through the benchmark GMD Vulnerability Assessment conducted in Requirement R4, that the responsible entity's System does not meet the performance requirements for the steady state planning benchmark GMD event contained in Table 1 shall have evidence such as dated electronic or hard copies of its CAP including timetable for implementing selected actions, as specified in Requirement R7. Each responsible entity, as determined in Requirement R1, shall also provide evidence, such as email records or postal receipts showing recipient and date, that it submitted a request for extension to the CEA if the responsible entity is unable to implement the CAP within the timetable provided in Part 7.3. Each responsible entity, as determined in Requirement R1, shall also provide evidence, such as email records, web postings with an electronic notice of posting, or postal receipts showing recipient and date, that it has distributed its CAP or relevant information, if any, (i) to the responsible entity's Reliability Coordinator, adjacent Planning Coordinator(s), adjacent Transmission Planner(s), and functional entities referenced in the CAP within 90 calendar days of development or revision, and (ii) to any functional entity that submits a written request and has a reliability-related need within 90 calendar days of receipt of such request or within 90 calendar days of development or revision, whichever is later as specified in Requirement R7. Each responsible entity, as determined in Requirement R1, shall also provide evidence, such as email notices or postal receipts showing recipient and date, that it has provided a documented response to comments received on its CAP within 90 calendar days of receipt of those comments, in accordance with Requirement R7.

Supplemental GMD Vulnerability Assessment(s)

R8. Each responsible entity, as determined in Requirement R1, shall complete a supplemental GMD Vulnerability Assessment of the Near-Term Transmission Planning Horizon at least once every 60 calendar months. This supplemental GMD Vulnerability Assessment shall use a study or studies based on models identified in Requirement R2, document assumptions, and document summarized results of the steady state analysis. *[Violation Risk Factor: High] [Time Horizon: Long-term Planning]*

8.1. The study or studies shall include the following conditions:

8.1.1. System On-Peak Load for at least one year within the Near-Term Transmission Planning Horizon; and

8.1.2. System Off-Peak Load for at least one year within the Near-Term Transmission Planning Horizon.

8.2. The study or studies shall be conducted based on the supplemental GMD event described in Attachment 1 to determine whether the System meets the performance requirements for the steady state planning supplemental GMD event contained in Table 1.

8.3. The supplemental GMD Vulnerability Assessment shall be provided: (i) to the responsible entity's Reliability Coordinator, adjacent Planning Coordinators, adjacent Transmission Planners within 90 calendar days of completion, and (ii) to any functional entity that submits a written request and has a reliability-related need within 90 calendar days of receipt of such request or within 90 calendar days of completion of the supplemental GMD Vulnerability Assessment, whichever is later.

8.3.1. If a recipient of the supplemental GMD Vulnerability Assessment provides documented comments on the results, the responsible entity shall provide a documented response to that recipient within 90 calendar days of receipt of those comments.

M8. Each responsible entity, as determined in Requirement R1, shall have dated evidence such as electronic or hard copies of its supplemental GMD Vulnerability Assessment meeting all of the requirements in Requirement R8. Each responsible entity, as determined in Requirement R1, shall also provide evidence, such as email records, web postings with an electronic notice of posting, or postal receipts showing recipient and date, that it has distributed its supplemental GMD Vulnerability Assessment: (i) to the responsible entity's Reliability Coordinator, adjacent Planning Coordinators, adjacent Transmission Planners within 90 calendar days of completion, and (ii) to any functional entity that submits a written request and has a reliability-related need within 90 calendar days of receipt of such request or within 90 calendar days of completion of the supplemental GMD Vulnerability Assessment, whichever is later, as specified in Requirement R8. Each responsible entity, as determined in Requirement R1, shall also provide evidence, such as email notices or postal receipts showing recipient and date, that it has provided a documented response to comments received on its supplemental GMD Vulnerability Assessment within 90 calendar days of receipt of those comments in accordance with Requirement R8.

R9. Each responsible entity, as determined in Requirement R1, shall provide GIC flow information to be used for the supplemental thermal impact assessment of transformers specified in Requirement R10 to each Transmission Owner and Generator Owner that owns an applicable Bulk Electric System (BES) power transformer in the planning area. The GIC flow information shall include: *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

9.1. The maximum effective GIC value for the worst case geoelectric field orientation for the supplemental GMD event described in Attachment 1. This value shall be provided to the Transmission Owner or Generator Owner that owns each applicable BES power transformer in the planning area.

9.2. The effective GIC time series, GIC(t), calculated using the supplemental GMD event described in Attachment 1 in response to a written request from the Transmission Owner or Generator Owner that owns an applicable BES power transformer in the planning area. GIC(t) shall be provided within 90 calendar days of receipt of the written request and after determination of the maximum effective GIC value in Part 9.1.

M9. Each responsible entity, as determined in Requirement R1, shall provide evidence, such as email records, web postings with an electronic notice of posting, or postal receipts showing recipient and date, that it has provided the maximum effective GIC values to the Transmission Owner and Generator Owner that owns each applicable BES power transformer in the planning area as specified in Requirement R9, Part 9.1. Each responsible entity, as determined in Requirement R1, shall also provide evidence, such as email records, web postings with an electronic notice of posting, or postal receipts showing recipient and date, that it has provided GIC(t) in response to a written request from the Transmission Owner or Generator Owner that owns an applicable BES power transformer in the planning area.

R10. Each Transmission Owner and Generator Owner shall conduct a supplemental thermal impact assessment for its solely and jointly owned applicable BES power transformers where the maximum effective GIC value provided in Requirement R9, Part 9.1, is 85 A per phase or greater. The supplemental thermal impact assessment shall: *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

10.1. Be based on the effective GIC flow information provided in Requirement R9;

10.2. Document assumptions used in the analysis;

10.3. Describe suggested actions and supporting analysis to mitigate the impact of GICs, if any; and

10.4. Be performed and provided to the responsible entities, as determined in Requirement R1, within 24 calendar months of receiving GIC flow information specified in Requirement R9, Part 9.1.

M10. Each Transmission Owner and Generator Owner shall have evidence such as electronic or hard copies of its supplemental thermal impact assessment for all of its solely and jointly owned applicable BES power transformers where the maximum effective GIC value provided in Requirement R9, Part 9.1, is 85 A per phase or greater, and shall have evidence such as email records, web postings with an electronic notice of posting, or postal receipts showing recipient and date, that it has provided its supplemental thermal impact assessment to the responsible entities as specified in Requirement R10.

R11. Each responsible entity, as determined in Requirement R1, that concludes through the supplemental GMD Vulnerability Assessment conducted in Requirement R8 that their System does not meet the performance requirements for the steady state planning supplemental GMD event contained in Table 1, shall develop a Corrective

Action Plan (CAP) addressing how the performance requirements will be met. The CAP shall: *[Violation Risk Factor: High] [Time Horizon: Long-term Planning]*

11.1. List System deficiencies and the associated actions needed to achieve required System performance. Examples of such actions include:

- Installation, modification, retirement, or removal of Transmission and generation Facilities and any associated equipment.
- Installation, modification, or removal of Protection Systems or Remedial Action Schemes.
- Use of Operating Procedures, specifying how long they will be needed as part of the CAP.
- Use of Demand-Side Management, new technologies, or other initiatives.

11.2. Be developed within one year of completion of the supplemental GMD Vulnerability Assessment.

11.3. Include a timetable, subject to approval for any extension sought under Part 11.4, for implementing the selected actions from Part 11.1. The timetable shall:

11.3.1. Specify implementation of non-hardware mitigation, if any, within two years of development of the CAP; and

11.3.2. Specify implementation of hardware mitigation, if any, within four years of development of the CAP.

11.4. Be submitted to the CEA with a request for extension of time if the responsible entity is unable to implement the CAP within the timetable provided in Part 11.3. The submitted CAP shall document the following:

11.4.1. Circumstances causing the delay for fully or partially implementing the selected actions in Part 11.1 and how those circumstances are beyond the control of the responsible entity;

11.4.2. Revisions to the selected actions in Part 11.1, if any, including utilization of Operating Procedures, if applicable; and

11.4.3. Updated timetable for implementing the selected actions in Part 11.1.

11.5. Be provided: (i) to the responsible entity's Reliability Coordinator, adjacent Planning Coordinator(s), adjacent Transmission Planner(s), and functional entities referenced in the CAP within 90 calendar days of development or revision, and (ii) to any functional entity that submits a written request and has a reliability-related need within 90 calendar days of receipt of such request or within 90 calendar days of development or revision, whichever is later.

11.5.1. If a recipient of the CAP provides documented comments on the CAP, the responsible entity shall provide a documented response to that recipient within 90 calendar days of receipt of those comments.

M11. Each responsible entity, as determined in Requirement R1, that concludes, through the supplemental GMD Vulnerability Assessment conducted in Requirement R8, that the responsible entity's System does not meet the performance requirements for the steady state planning supplemental GMD event contained in Table 1 shall have evidence such as dated electronic or hard copies of its CAP including timetable for implementing selected actions, as specified in Requirement R11. Each responsible entity, as determined in Requirement R1, shall also provide evidence, such as email records or postal receipts showing recipient and date, that it submitted a request for extension to the CEA if the responsible entity is unable to implement the CAP within the timetable provided in Part 11.3. Each responsible entity, as determined in Requirement R1, shall also provide evidence, such as email records, web postings with an electronic notice of posting, or postal receipts showing recipient and date, that it has distributed its CAP or relevant information, if any, (i) to the responsible entity's Reliability Coordinator, adjacent Planning Coordinator(s), adjacent Transmission Planner(s), and functional entities referenced in the CAP within 90 calendar days of development or revision, and (ii) to any functional entity that submits a written request and has a reliability-related need within 90 calendar days of receipt of such request or within 90 calendar days of development or revision, whichever is later as specified in Requirement R11. Each responsible entity, as determined in Requirement R1, shall also provide evidence, such as email notices or postal receipts showing recipient and date, that it has provided a documented response to comments received on its CAP within 90 calendar days of receipt of those comments, in accordance with Requirement R11.

GMD Measurement Data Processes

R12. Each responsible entity, as determined in Requirement R1, shall implement a process to obtain GIC monitor data from at least one GIC monitor located in the Planning Coordinator's planning area or other part of the system included in the Planning Coordinator's GIC System model. *[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*

M12. Each responsible entity, as determined in Requirement R1, shall have evidence such as electronic or hard copies of its GIC monitor location(s) and documentation of its process to obtain GIC monitor data in accordance with Requirement R12.

R13. Each responsible entity, as determined in Requirement R1, shall implement a process to obtain geomagnetic field data for its Planning Coordinator's planning area. *[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*

M13. Each responsible entity, as determined in Requirement R1, shall have evidence such as electronic or hard copies of its process to obtain geomagnetic field data for its Planning Coordinator's planning area in accordance with Requirement R13.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: "Compliance Enforcement Authority" means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

- For Requirements R1, R2, R3, R5, R6, R9, and R10, each responsible entity shall retain documentation as evidence for five years.
- For Requirements R4 and R8, each responsible entity shall retain documentation of the current GMD Vulnerability Assessment and the preceding GMD Vulnerability Assessment.
- For Requirement R7 and R11, each responsible entity shall retain documentation as evidence for five years or until all actions in the Corrective Action Plan are completed, whichever is later.
- For Requirements R12 and R13, each responsible entity shall retain documentation as evidence for three years.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Table 1: Steady State Planning GMD Event

Steady State:

a. Voltage collapse, Cascading and uncontrolled islanding shall not occur.
b. Generation loss is acceptable as a consequence of the steady state planning GMD events.
c. Planned System adjustments such as Transmission configuration changes and re-dispatch of generation are allowed if such adjustments are executable within the time duration applicable to the Facility Ratings.

Category	Initial Condition	Event	Interruption of Firm Transmission Service Allowed	Load Loss Allowed
Benchmark GMD Event – GMD Event with Outages	1. System as may be postured in response to space weather information[1], and then 2. GMD event[2]	Reactive Power compensation devices and other Transmission Facilities removed as a result of Protection System operation or Misoperation due to harmonics during the GMD event	Yes[3]	Yes[3]
Supplemental GMD Event – GMD Event with Outages	1. System as may be postured in response to space weather information[1], and then 2. GMD event[2]	Reactive Power compensation devices and other Transmission Facilities removed as a result of Protection System operation or Misoperation due to harmonics during the GMD event	Yes	Yes

Table 1: Steady State Performance Footnotes

1. The System condition for GMD planning may include adjustments to posture the System that are executable in response to space weather information.
2. The GMD conditions for the benchmark and supplemental planning events are described in Attachment 1.
3. Load loss as a result of manual or automatic Load shedding (e.g., UVLS) and/or curtailment of Firm Transmission Service may be used to meet BES performance requirements during studied GMD conditions. The likelihood and magnitude of Load loss or curtailment of Firm Transmission Service should be minimized.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	N/A	N/A	N/A	The Planning Coordinator, in conjunction with its Transmission Planner(s), failed to determine and identify individual or joint responsibilities of the Planning Coordinator and Transmission Planner(s) in the Planning Coordinator's planning area for maintaining models, performing the study or studies needed to complete benchmark and supplemental GMD Vulnerability Assessments, and implementing process(es) to obtain GMD measurement data as specified in this standard.
R2.	N/A	N/A	The responsible entity did not maintain either System models or GIC System models of the responsible entity's planning area for performing the studies	The responsible entity did not maintain both System models and GIC System models of the responsible entity's planning area for performing the studies

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			needed to complete benchmark and supplemental GMD Vulnerability Assessments.	needed to complete benchmark and supplemental GMD Vulnerability Assessments.
R3.	N/A	N/A	N/A	The responsible entity did not have criteria for acceptable System steady state voltage performance for its System during the GMD events described in Attachment 1 as required.
R4.	The responsible entity completed a benchmark GMD Vulnerability Assessment, but it was more than 60 calendar months and less than or equal to 64 calendar months since the last benchmark GMD Vulnerability Assessment.	The responsible entity's completed benchmark GMD Vulnerability Assessment failed to satisfy one of the elements listed in Requirement R4, Parts 4.1 through 4.3; OR The responsible entity completed a benchmark GMD Vulnerability Assessment, but it was more than 64 calendar months and less than or equal to 68 calendar months since the	The responsible entity's completed benchmark GMD Vulnerability Assessment failed to satisfy two of the elements listed in Requirement R4, Parts 4.1 through 4.3; OR The responsible entity completed a benchmark GMD Vulnerability Assessment, but it was more than 68 calendar months and less than or equal to 72 calendar months since the	The responsible entity's completed benchmark GMD Vulnerability Assessment failed to satisfy three of the elements listed in Requirement R4, Parts 4.1 through 4.3; OR The responsible entity completed a benchmark GMD Vulnerability Assessment, but it was more than 72 calendar months since the last benchmark

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		last benchmark GMD Vulnerability Assessment.	last benchmark GMD Vulnerability Assessment.	GMD Vulnerability Assessment; OR The responsible entity does not have a completed benchmark GMD Vulnerability Assessment.
R5.	The responsible entity provided the effective GIC time series, GIC(t), in response to written request, but did so more than 90 calendar days and less than or equal to 100 calendar days after receipt of a written request.	The responsible entity provided the effective GIC time series, GIC(t), in response to written request, but did so more than 100 calendar days and less than or equal to 110 calendar days after receipt of a written request.	The responsible entity provided the effective GIC time series, GIC(t), in response to written request, but did so more than 110 calendar days after receipt of a written request.	The responsible entity did not provide the maximum effective GIC value to the Transmission Owner and Generator Owner that owns each applicable BES power transformer in the planning area; OR The responsible entity did not provide the effective GIC time series, GIC(t), upon written request.
R6.	The responsible entity failed to conduct a benchmark thermal impact assessment for 5% or less or one of its solely owned and jointly owned applicable BES power	The responsible entity failed to conduct a benchmark thermal impact assessment for more than 5% up to (and including) 10% or two of its solely owned and jointly	The responsible entity failed to conduct a benchmark thermal impact assessment for more than 10% up to (and including) 15% or three of its solely owned and	The responsible entity failed to conduct a benchmark thermal impact assessment for more than 15% or more than three of its solely owned and jointly owned

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	transformers (whichever is greater) where the maximum effective GIC value provided in Requirement R5, Part 5.1, is 75 A or greater per phase; OR The responsible entity conducted a benchmark thermal impact assessment for its solely owned and jointly owned applicable BES power transformers where the maximum effective GIC value provided in Requirement R5, Part 5.1, is 75 A or greater per phase but did so more than 24 calendar months and less than or equal to 26 calendar months of receiving GIC flow information specified in Requirement R5, Part 5.1.	owned applicable BES power transformers (whichever is greater) where the maximum effective GIC value provided in Requirement R5, Part 5.1, is 75 A or greater per phase; OR The responsible entity conducted a benchmark thermal impact assessment for its solely owned and jointly owned applicable BES power transformers where the maximum effective GIC value provided in Requirement R5, Part 5.1, is 75 A or greater per phase but did so more than 26 calendar months and less than or equal to 28 calendar months of receiving GIC flow information specified in Requirement R5, Part 5.1; OR The responsible entity failed to include one of the	jointly owned applicable BES power transformers (whichever is greater) where the maximum effective GIC value provided in Requirement R5, Part 5.1, is 75 A or greater per phase; OR The responsible entity conducted a benchmark thermal impact assessment for its solely owned and jointly owned applicable BES power transformers where the maximum effective GIC value provided in Requirement R5, Part 5.1, is 75 A or greater per phase but did so more than 28 calendar months and less than or equal to 30 calendar months of receiving GIC flow information specified in Requirement R5, Part 5.1; OR The responsible entity failed to include two of the	applicable BES power transformers (whichever is greater) where the maximum effective GIC value provided in Requirement R5, Part 5.1, is 75 A or greater per phase; OR The responsible entity conducted a benchmark thermal impact assessment for its solely owned and jointly owned applicable BES power transformers where the maximum effective GIC value provided in Requirement R5, Part 5.1, is 75 A or greater per phase but did so more than 30 calendar months of receiving GIC flow information specified in Requirement R5, Part 5.1; OR The responsible entity failed to include three of the required elements as listed

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		required elements as listed in Requirement R6, Parts 6.1 through 6.3.	required elements as listed in Requirement R6, Parts 6.1 through 6.3.	in Requirement R6, Parts 6.1 through 6.3.
R7.	The responsible entity's Corrective Action Plan failed to comply with one of the elements in Requirement R7, Parts 7.1 through 7.5.	The responsible entity's Corrective Action Plan failed to comply with two of the elements in Requirement R7, Parts 7.1 through 7.5.	The responsible entity's Corrective Action Plan failed to comply with three of the elements in Requirement R7, Parts 7.1 through 7.5.	The responsible entity's Corrective Action Plan failed to comply with four or more of the elements in Requirement R7, Parts 7.1 through 7.5; OR The responsible entity did not develop a Corrective Action Plan as required by Requirement R7.
R8.	The responsible entity completed a supplemental GMD Vulnerability Assessment, but it was more than 60 calendar months and less than or equal to 64 calendar months since the last supplemental GMD Vulnerability Assessment.	The responsible entity's completed supplemental GMD Vulnerability Assessment failed to satisfy one of the elements listed in Requirement R8, Parts 8.1 through 8.3; OR The responsible entity completed a supplemental GMD Vulnerability Assessment, but it was more	The responsible entity's completed supplemental GMD Vulnerability Assessment failed to satisfy two of the elements listed in Requirement R8, Parts 8.1 through 8.3; OR The responsible entity completed a supplemental GMD Vulnerability Assessment, but it was more	The responsible entity's completed supplemental GMD Vulnerability Assessment failed to satisfy three of the elements listed in Requirement R8, Parts 8.1 through 8.3; OR The responsible entity completed a supplemental GMD Vulnerability Assessment, but it was more

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		than 64 calendar months and less than or equal to 68 calendar months since the last supplemental GMD Vulnerability Assessment.	than 68 calendar months and less than or equal to 72 calendar months since the last supplemental GMD Vulnerability Assessment.	than 72 calendar months since the last supplemental GMD Vulnerability Assessment; OR The responsible entity does not have a completed supplemental GMD Vulnerability Assessment.
R9.	The responsible entity provided the effective GIC time series, GIC(t), in response to written request, but did so more than 90 calendar days and less than or equal to 100 calendar days after receipt of a written request.	The responsible entity provided the effective GIC time series, GIC(t), in response to written request, but did so more than 100 calendar days and less than or equal to 110 calendar days after receipt of a written request.	The responsible entity provided the effective GIC time series, GIC(t), in response to written request, but did so more than 110 calendar days after receipt of a written request.	The responsible entity did not provide the maximum effective GIC value to the Transmission Owner and Generator Owner that owns each applicable BES power transformer in the planning area; OR The responsible entity did not provide the effective GIC time series, GIC(t), upon written request.
R10.	The responsible entity failed to conduct a supplemental thermal impact assessment for 5% or less or one of its	The responsible entity failed to conduct a supplemental thermal impact assessment for more than 5% up to (and	The responsible entity failed to conduct a supplemental thermal impact assessment for more than 10% up to	The responsible entity failed to conduct a supplemental thermal impact assessment for more than 15% or more

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	solely owned and jointly owned applicable BES power transformers (whichever is greater) where the maximum effective GIC value provided in Requirement R9, Part 9.1, is 85 A or greater per phase; OR The responsible entity conducted a supplemental thermal impact assessment for its solely owned and jointly owned applicable BES power transformers where the maximum effective GIC value provided in Requirement R9, Part 9.1, is 85 A or greater per phase but did so more than 24 calendar months and less than or equal to 26 calendar months of receiving GIC flow information specified in Requirement R9, Part 9.1.	including) 10% or two of its solely owned and jointly owned applicable BES power transformers (whichever is greater) where the maximum effective GIC value provided in Requirement R9, Part 9.1, is 85 A or greater per phase; OR The responsible entity conducted a supplemental thermal impact assessment for its solely owned and jointly owned applicable BES power transformers where the maximum effective GIC value provided in Requirement R9, Part 9.1, is 85 A or greater per phase but did so more than 26 calendar months and less than or equal to 28 calendar months of receiving GIC flow information specified in Requirement R9, Part 9.1 OR	(and including) 15% or three of its solely owned and jointly owned applicable BES power transformers (whichever is greater) where the maximum effective GIC value provided in Requirement R9, Part 9.1, is 85 A or greater per phase; OR The responsible entity conducted a supplemental thermal impact assessment for its solely owned and jointly owned applicable BES power transformers where the maximum effective GIC value provided in Requirement R9, Part 9.1, is 85 A or greater per phase but did so more than 28 calendar months and less than or equal to 30 calendar months of receiving GIC flow information specified in Requirement R9, Part 9.1; OR	than three of its solely owned and jointly owned applicable BES power transformers (whichever is greater) where the maximum effective GIC value provided in Requirement R9, Part 9.1, is 85 A or greater per phase; OR The responsible entity conducted a supplemental thermal impact assessment for its solely owned and jointly owned applicable BES power transformers where the maximum effective GIC value provided in Requirement R9, Part 9.1, is 85 A or greater per phase but did so more than 30 calendar months of receiving GIC flow information specified in Requirement R9, Part 9.1; OR

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		The responsible entity failed to include one of the required elements as listed in Requirement R10, Parts 10.1 through 10.3.	The responsible entity failed to include two of the required elements as listed in Requirement R10, Parts 10.1 through 10.3.	The responsible entity failed to include three of the required elements as listed in Requirement R10, Parts 10.1 through 10.3.
R11.	The responsible entity's Corrective Action Plan failed to comply with one of the elements in Requirement R11, Parts 11.1 through 11.5.	The responsible entity's Corrective Action Plan failed to comply with two of the elements in Requirement R11, Parts 11.1 through 11.5.	The responsible entity's Corrective Action Plan failed to comply with three of the elements in Requirement R11, Parts 11.1 through 11.5.	The responsible entity's Corrective Action Plan failed to comply with four or more of the elements in Requirement R11, Parts 11.1 through 11.5; OR The responsible entity did not develop a Corrective Action Plan as required by Requirement R11.

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R12.	N/A	N/A	N/A	The responsible entity did not implement a process to obtain GIC monitor data from at least one GIC monitor located in the Planning Coordinator's planning area or other part of the system included in the Planning Coordinator's GIC System Model.
R13.	N/A	N/A	N/A	The responsible entity did not implement a process to obtain geomagnetic field data for its Planning Coordinator's planning area.

D. Regional Variances

D.A. Regional Variance for Canadian Jurisdictions

This Variance shall be applicable in those Canadian jurisdictions where the Variance has been approved for use by the applicable governmental authority or has otherwise become effective in the jurisdiction.

This variance replaces all references to "Attachment 1" in the standard with "Attachment 1 or Attachment 1-CAN."

In addition, this Variance replaces Requirement R7, Part 7.3 through Part 7.5 and Requirement R11, Part 11.3 through Part 11.5 with the following:

D.A.7.3. Include a timetable, subject to revision by the responsible entity in Part D.A.7.4, for implementing the selected actions from Part 7.1. The timetable shall:

D.A.7.3.1. Specify implementation of non-hardware mitigation, if any, within two years of the later of the development of the CAP or receipt of regulatory approvals, if required; and

D.A.7.3.2. Specify implementation of hardware mitigation, if any, within four years of the later of the development of the CAP or receipt of regulatory approvals, if required.

D.A.7.4. Be revised if the responsible entity is unable to implement the CAP within the timetable for implementation provided in Part D.A.7.3. The revised CAP shall document the following:

D.A.7.4.1 Circumstances causing the delay for fully or partially implementing the selected actions in Part 7.1 and how those circumstances are beyond the control of the responsible entity;

D.A.7.4.2 Revisions to the selected actions in Part 7.1, if any, including utilization of Operating Procedures if applicable; and

D.A.7.4.3 Updated timetable for implementing the selected actions in Part 7.1.

D.A.7.5. Be provided: (i) to the responsible entity's Reliability Coordinator, adjacent Planning Coordinator(s), adjacent Transmission Planner(s), and functional entities referenced in the CAP within 90 calendar days of development or revision, (ii) to any functional entity that submits a written request and has a reliability-related need within 90 calendar days of receipt of such request or within 90 calendar days of development or revision, whichever is later, and (iii) to the Compliance Enforcement Authority or Applicable Governmental Authority when revised under D.A.7.4 within 90 calendar days of revision.

D.A.7.5.1 If a recipient of the CAP provides documented comments on the CAP, the responsible entity shall provide a documented response to that recipient within 90 calendar days of receipt of those comments.

D.A.M.7. Each responsible entity, as determined in Requirement R1, that concludes, through the benchmark GMD Vulnerability Assessment conducted in Requirement R4, that the responsible entity's System does not meet the performance requirements for the steady state planning benchmark GMD event contained in Table 1 shall have evidence such as dated electronic or hard copies of its CAP including timetable for implementing selected actions, as specified in Requirement R7. Each responsible entity, as determined in Requirement R1, shall also provide evidence, such as email records or postal receipts showing recipient and date, that it has revised its CAP if situations beyond the responsible entity's control prevent implementation of the CAP within the timetable specified. Each responsible entity, as determined in Requirement R1, shall also provide evidence, such as email records, web postings with an electronic notice of posting, or postal receipts showing recipient and date, that it has distributed its CAP or relevant information, if any, (i) to the responsible entity's Reliability Coordinator, adjacent Planning Coordinator(s), adjacent Transmission Planner(s), and functional entities referenced in the CAP within 90 calendar days of development or revision, (ii) to any functional entity that submits a written request and has a reliability-related need within 90 calendar days of receipt of such request or within 90 calendar days of development or revision, whichever is later as specified in Requirement R7, and (iii) to the Compliance Enforcement Authority or Applicable Governmental Authority when revised under D.A.7.4 within 90 calendar days of revision. Each responsible entity, as determined in Requirement R1, shall also provide evidence, such as email notices or postal receipts showing recipient and date, that it has provided a documented response to comments received on its CAP within 90 calendar days of receipt of those comments, in accordance with Requirement R7.

D.A.11.3. Include a timetable, subject to revision by the responsible entity in Part D.A.11.4, for implementing the selected actions from Part 11.1. The timetable shall:

D.A.11.3.1. Specify implementation of non-hardware mitigation, if any, within two years of the later of the development of the CAP or receipt of regulatory approvals, if required; and

D.A.11.3.2. Specify implementation of hardware mitigation, if any, within four years of the later of the development of the CAP or receipt of regulatory approvals, if required.

D.A.11.4. Be revised if the responsible entity is unable to implement the CAP within the timetable for implementation provided in Part D.A.11.3. The revised CAP shall document the following:

D.A.11.4.1 Circumstances causing the delay for fully or partially implementing the selected actions in Part 11.1 and how those circumstances are beyond the control of the responsible entity;

D.A.11.4.2 Revisions to the selected actions in Part 11.1, if any, including utilization of Operating Procedures if applicable; and

D.A.11.4.3 Updated timetable for implementing the selected actions in Part 11.1.

D.A.11.5. Be provided: (i) to the responsible entity's Reliability Coordinator, adjacent Planning Coordinator(s), adjacent Transmission Planner(s), and functional entities referenced in the CAP within 90 calendar days of development or revision, (ii) to any functional entity that submits a written request and has a reliability-related need within 90 calendar days of receipt of such request or within 90 calendar days of development or revision, whichever is later, and (iii) to the Compliance Enforcement Authority or Applicable Governmental Authority when revised under D.A.11.4 within 90 calendar days of revision.

D.A.11.5.1. If a recipient of the CAP provides documented comments on the CAP, the responsible entity shall provide a documented response to that recipient within 90 calendar days of receipt of those comments.

D.A.M.11. Each responsible entity, as determined in Requirement R1, that concludes, through the supplemental GMD Vulnerability Assessment conducted in Requirement R8, that the responsible entity's System does not meet the performance requirements for the steady state planning supplemental GMD event contained in Table 1 shall have evidence such as dated electronic or hard copies of its CAP including timetable for implementing selected actions, as specified in Requirement R11. Each responsible entity, as determined in Requirement R1, shall also provide evidence, such as email records or postal receipts showing recipient and date, that it has revised its CAP if situations beyond the responsible entity's control prevent implementation of the CAP within the timetable specified. Each responsible entity, as determined in Requirement R1, shall also provide evidence, such as email records, web postings with an electronic notice of posting, or postal receipts showing recipient and date, that it has distributed its CAP or relevant information, if any, (i) to the responsible entity's Reliability Coordinator, adjacent Planning Coordinator(s), adjacent Transmission Planner(s), and functional entities referenced in the CAP within 90 calendar days of development or revision, (ii) to any functional entity that submits a written request and has a reliability-related need within 90 calendar days of receipt of such request or within 90 calendar days of development or revision, whichever is later as specified in Requirement R11, and (iii) to the Compliance Enforcement Authority or Applicable Governmental Authority when revised under D.A.11.4 within 90 calendar days of revision. Each responsible entity, as determined in Requirement R1, shall also provide evidence, such as email notices or postal receipts showing recipient and date, that it has provided a documented response to comments received on its CAP within 90 calendar days of receipt of those comments, in accordance with Requirement R11.

E. Associated Documents

Attachment 1

Attachment 1-CAN

Version History

Version	Date	Action	Change Tracking
1	December 17, 2014	Adopted by the NERC Board of Trustees	New
2	November 9, 2017	Adopted by the NERC Board of Trustees	Revised to respond to directives in FERC Order No. 830.
2	November 25, 2018	FERC Order issued approving TPL-007-2. Docket No. RM18-8-000	
3	February 7, 2019	Adopted by the NERC Board of Trustees	Canadian Variance
4	February 6, 2020	Adopted by the NERC Board of Trustees	Revised to respond to directives in FERC Order. 851
4	March 19, 2020	FERC Order issued approving TPL-007-4. Docket No. RD20-3-000	

Attachment 1

Calculating Geoelectric Fields for the Benchmark and Supplemental GMD Events

The benchmark GMD event[1] defines the geoelectric field values used to compute GIC flows that are needed to conduct a benchmark GMD Vulnerability Assessment. It is composed of the following elements: (1) a reference peak geoelectric field amplitude of 8 V/km derived from statistical analysis of historical magnetometer data; (2) scaling factors to account for local geomagnetic latitude; (3) scaling factors to account for local earth conductivity; and (4) a reference geomagnetic field time series or waveform to facilitate time-domain analysis of GMD impact on equipment.

The supplemental GMD event is composed of similar elements as described above, except (1) the reference peak geoelectric field amplitude is 12 V/km over a localized area; and (2) the geomagnetic field time series or waveform includes a local enhancement in the waveform.[2]

The regional geoelectric field peak amplitude used in GMD Vulnerability Assessment, E_{peak}, can be obtained from the reference geoelectric field value of 8 V/km for the benchmark GMD event (1) or 12 V/km for the supplemental GMD event (2) using the following relationships:

$$E_{peak} = 8 \times \alpha \times \beta_b \, (V/km) \quad (1)$$

$$E_{peak} = 12 \times \alpha \times \beta_s \, (V/km) \quad (2)$$

where, α is the scaling factor to account for local geomagnetic latitude, and β is a scaling factor to account for the local earth conductivity structure. Subscripts *b* and *s* for the β scaling factor denote association with the benchmark or supplemental GMD events, respectively.

Scaling the Geomagnetic Field

The benchmark and supplemental GMD events are defined for geomagnetic latitude of 60° and must be scaled to account for regional differences based on geomagnetic latitude. Table 2 provides a scaling factor correlating peak geoelectric field to geomagnetic latitude. Alternatively, the scaling factor α is computed with the empirical expression:

$$\alpha = 0.001 \times e^{(0.115 \times L)} \quad (3)$$

where, L is the geomagnetic latitude in degrees and $0.1 \leq \alpha \leq 1$.

[1] The Benchmark Geomagnetic Disturbance Event Description, May 2016 is available on the Related Information webpage for TPL-007-1: http://www.nerc.com/pa/Stand/TPL0071RD/Benchmark_clean_May12_complete.pdf.

[2] The extent of local enhancements is on the order of 100 km in North-South (latitude) direction but longer in East-West (longitude) direction. The local enhancement in the geomagnetic field occurs over the time period of 2-5 minutes. Additional information is available in the Supplemental Geomagnetic Disturbance Event Description, October 2017 white paper on the Project 2013-03 Geomagnetic Disturbance Mitigation project webpage: http://www.nerc.com/pa/Stand/Pages/Project-2013-03-Geomagnetic-Disturbance-Mitigation.aspx.

For large planning areas that cover more than one scaling factor from Table 2, the GMD Vulnerability Assessment should be based on a peak geoelectric field that is:

- calculated by using the most conservative (largest) value for α; or
- calculated assuming a non-uniform or piecewise uniform geomagnetic field.

Table 2: Geomagnetic Field Scaling Factors for the Benchmark and Supplemental GMD Events

Geomagnetic Latitude (Degrees)	Scaling Factor1 (α)
≤ 40	0.10
45	0.2
50	0.3
54	0.5
56	0.6
57	0.7
58	0.8
59	0.9
≥ 60	1.0

Scaling the Geoelectric Field

The benchmark GMD event is defined for the reference Quebec earth model described in Table 4. The peak geoelectric field, E_{peak}, used in a GMD Vulnerability Assessment may be obtained by either:

- Calculating the geoelectric field for the ground conductivity in the planning area and the reference geomagnetic field time series scaled according to geomagnetic latitude, using a procedure such as the plane wave method described in the NERC GMD Task Force GIC Application Guide;[3] or
- Using the earth conductivity scaling factor β from Table 3 that correlates to the ground conductivity map in Figure 1 or Figure 2. Along with the scaling factor α from equation (3) or Table 2, β is applied to the reference geoelectric field using equation (1 or 2, as applicable) to obtain the regional geoelectric field peak amplitude E_{peak} to be used in GMD Vulnerability Assessments. When a ground conductivity model is not available, the responsible entity should use the largest β factor of adjacent physiographic regions or a technically justified value.

[3] Available at the NERC GMD Task Force project webpage: http://www.nerc.com/comm/PC/Pages/Geomagnetic-Disturbance-Task-Force-(GMDTF)-2013.aspx.

The earth models used to calculate Table 3 for the United States were obtained from publicly available information published on the U. S. Geological Survey website.[4] The models used to calculate Table 3 for Canada were obtained from Natural Resources Canada (NRCan) and reflect the average structure for large regions. A planner can also use specific earth model(s) with documented justification and the reference geomagnetic field time series to calculate the β factor(s) as follows:

$$\beta_b = E/8 \text{ for the benchmark GMD event} \quad (4)$$

$$\beta_s = E/12 \text{ for the supplemental GMD} \quad (5)$$

where, *E* is the absolute value of peak geoelectric in V/km obtained from the technically justified earth model and the reference geomagnetic field time series.

For large planning areas that span more than one β scaling factor, the most conservative (largest) value for β may be used in determining the peak geoelectric field to obtain conservative results. Alternatively, a planner could perform analysis using a non-uniform or piecewise uniform geoelectric field.

Applying the Localized Peak Geoelectric Field in the Supplemental GMD Event

The peak geoelectric field of the supplemental GMD event occurs in a localized area.[5] Planners have flexibility to determine how to apply the localized peak geoelectric field over the planning area in performing GIC calculations. Examples of approaches are:

- Apply the peak geoelectric field (12 V/km scaled to the planning area) over the entire planning area;
- Apply a spatially limited (12 V/km scaled to the planning area) peak geoelectric field (e.g., 100 km in North-South latitude direction and 500 km in East-West longitude direction) over a portion(s) of the system, and apply the benchmark GMD event over the rest of the system; or
- Other methods to adjust the benchmark GMD event analysis to account for the localized geoelectric field enhancement of the supplemental GMD event.

[4] Available at http://geomag.usgs.gov/conductivity/.

[5] See the Supplemental Geomagnetic Disturbance Description white paper located on the Project 2013-03 Geomagnetic Disturbance Mitigation project webpage: http://www.nerc.com/pa/Stand/Pages/Project-2013-03-Geomagnetic-Disturbance-Mitigation.aspx.

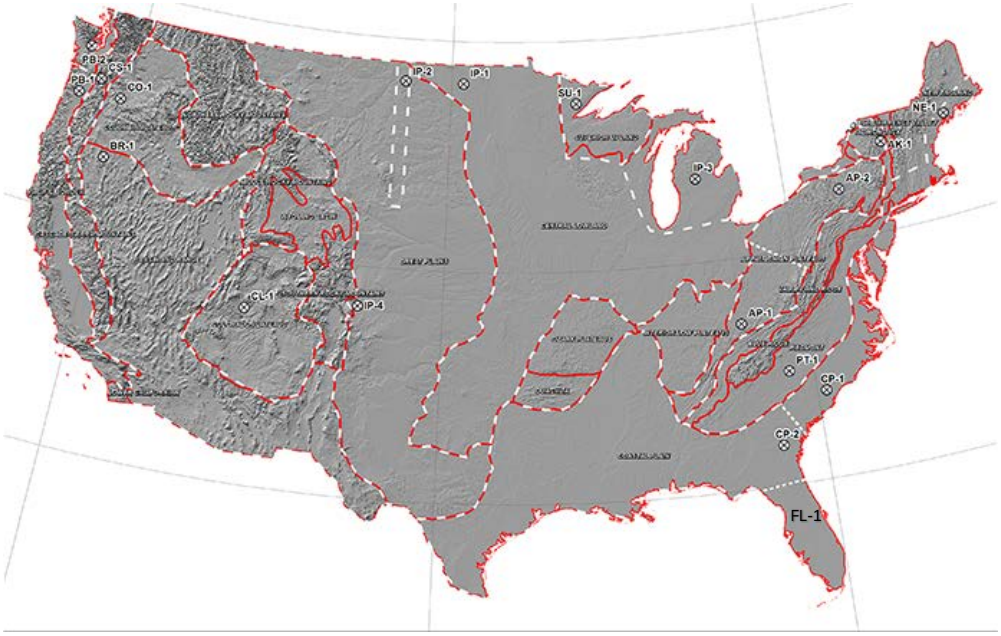


Figure 1: Physiographic Regions of the Continental United States[6]



Figure 2: Physiographic Regions of Canada

[6] Additional map detail is available at the U.S. Geological Survey: http://geomag.usgs.gov/.

Table 3: Geoelectric Field Scaling Factors		
Earth model	**Scaling Factor Benchmark Event (β_b)**	**Scaling Factor Supplemental Event (β_s)**
AK1A	0.56	0.51
AK1B	0.56	0.51
AP1	0.33	0.30
AP2	0.82	0.78
BR1	0.22	0.22
CL1	0.76	0.73
CO1	0.27	0.25
CP1	0.81	0.77
CP2	0.95	0.86
FL1	0.76	0.73
CS1	0.41	0.37
IP1	0.94	0.90
IP2	0.28	0.25
IP3	0.93	0.90
IP4	0.41	0.35
NE1	0.81	0.77
PB1	0.62	0.55
PB2	0.46	0.39
PT1	1.17	1.19
SL1	0.53	0.49
SU1	0.93	0.90
BOU	0.28	0.24
FBK	0.56	0.56
PRU	0.21	0.22
BC	0.67	0.62
PRAIRIES	0.96	0.88
SHIELD	1.0	1.0
ATLANTIC	0.79	0.76

Scaling factors in Table 3 are dependent upon the frequency content of the reference storm. Consequently, the benchmark GMD event and the supplemental GMD event may produce different scaling factors for a given earth model.

Table 4: Reference Earth Model (Quebec)	
Layer Thickness (km)	**Resistivity (Ω-m)**
15	20,000
10	200
125	1,000
200	100
∞	3

Reference Geomagnetic Field Time Series or Waveform for the Benchmark GMD Event[7]

The geomagnetic field measurement record of the March 13-14 1989 GMD event, measured at the NRCan Ottawa geomagnetic observatory, is the basis for the reference geomagnetic field waveform to be used to calculate the GIC time series, GIC(t), required for transformer thermal impact assessment.

The geomagnetic latitude of the Ottawa geomagnetic observatory is 55°; therefore, the amplitudes of the geomagnetic field measurement data were scaled up to the 60° reference geomagnetic latitude (see Figure 3) such that the resulting peak geoelectric field amplitude computed using the reference earth model was 8 V/km (see Figures 4 and 5). The sampling rate for the geomagnetic field waveform is 10 seconds.[8] To use this geoelectric field time series when a different earth model is applicable, it should be scaled with the appropriate benchmark conductivity scaling factor β_b.

[7] Refer to the Benchmark Geomagnetic Disturbance Event Description white paper for details on the determination of the reference geomagnetic field waveform: http://www.nerc.com/pa/stand/Pages/TPL0071RI.aspx.

[8] The data file of the benchmark geomagnetic field waveform is available on the Related Information webpage for TPL-007-1: http://www.nerc.com/pa/stand/Pages/TPL0071RI.aspx.

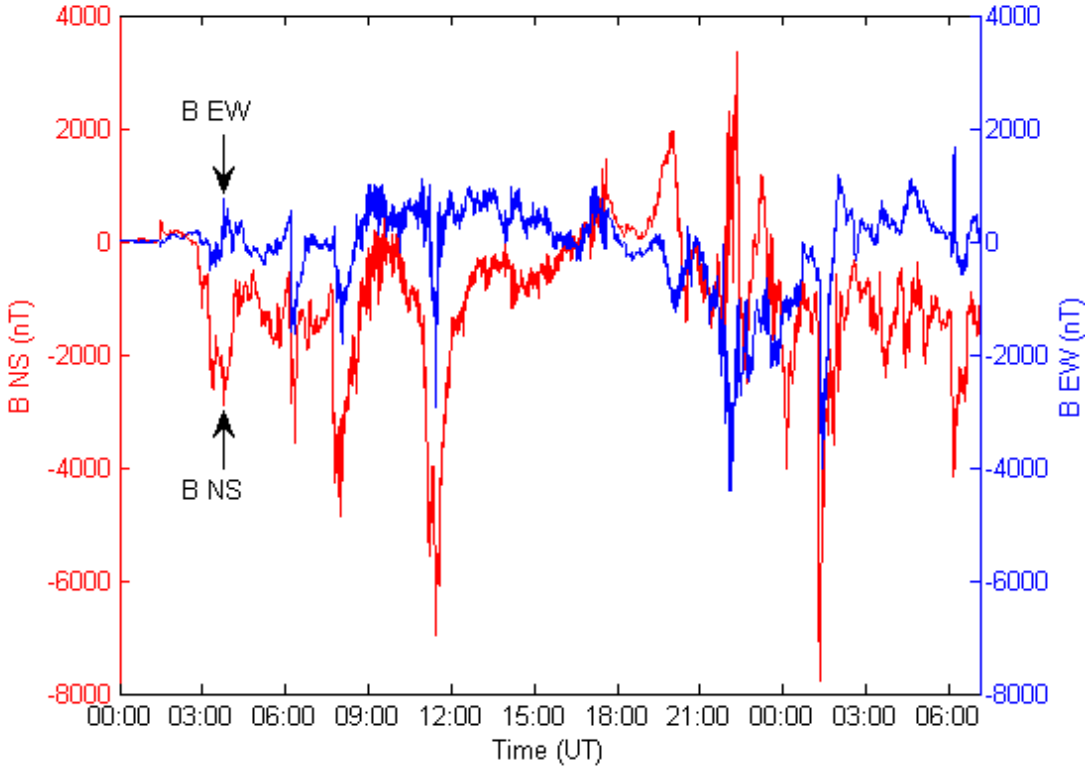


Figure 3: Benchmark Geomagnetic Field Waveform
Red B_n (Northward), Blue B_e (Eastward)

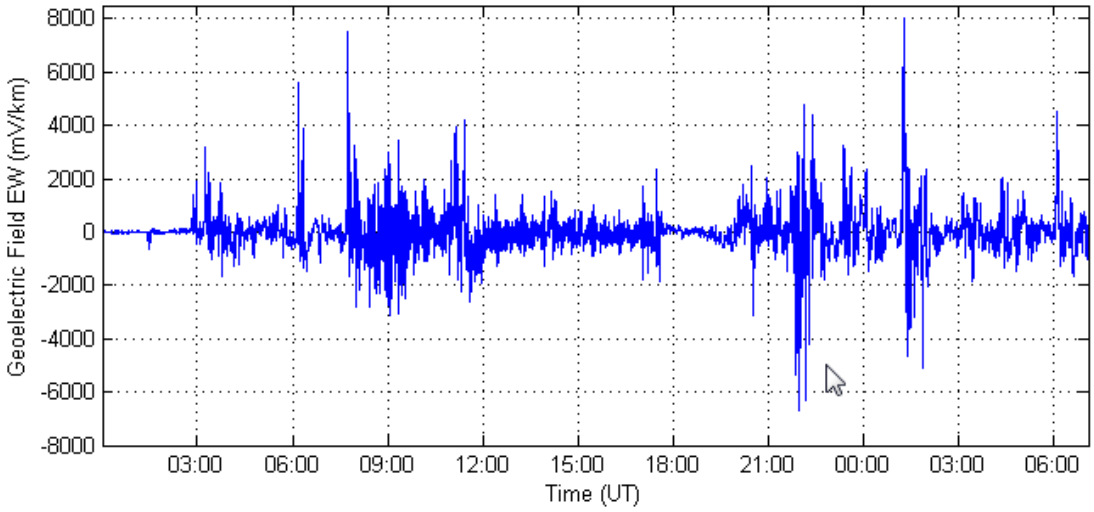


Figure 4: Benchmark Geoelectric Field Waveform
E_E (Eastward)

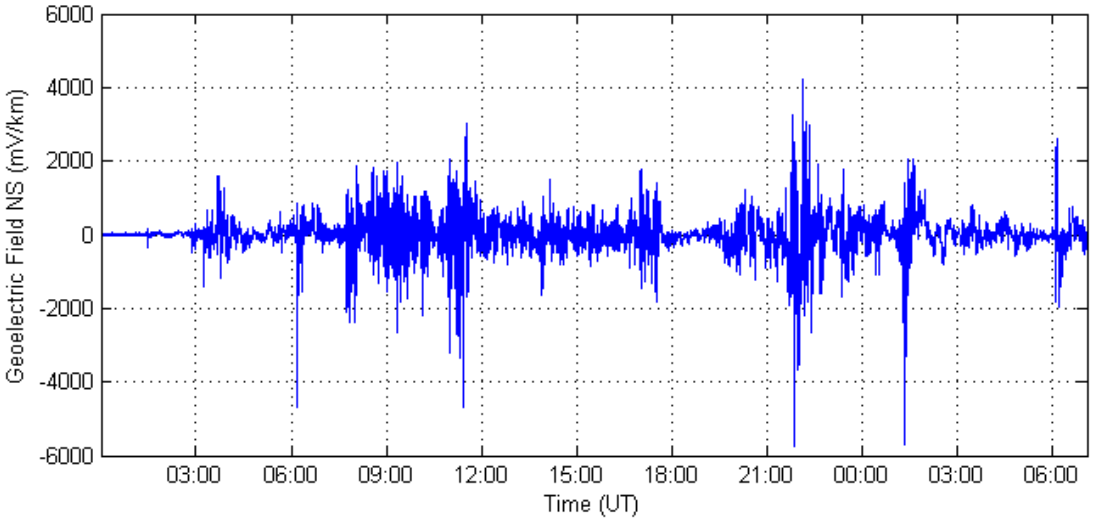


Figure 5: Benchmark Geoelectric Field Waveform
E_N (Northward)

Reference Geomagnetic Field Time Series or Waveform for the Supplemental GMD Event[9]

The geomagnetic field measurement record of the March 13-14, 1989 GMD event, measured at the NRCan Ottawa geomagnetic observatory, is the basis for the reference geomagnetic field waveform to be used to calculate the GIC time series, GIC(t), required for transformer thermal impact assessment for the supplemental GMD event. The supplemental GMD event waveform differs from the benchmark GMD event waveform in that the supplemental GMD event waveform has a local enhancement.

The geomagnetic latitude of the Ottawa geomagnetic observatory is 55°; therefore, the amplitudes of the geomagnetic field measurement data were scaled up to the 60° reference geomagnetic latitude (see Figure 6) such that the resulting peak geoelectric field amplitude computed using the reference earth model was 12 V/km (see Figure7). The sampling rate for the geomagnetic field waveform is 10 seconds.[10] To use this geoelectric field time series when a different earth model is applicable, it should be scaled with the appropriate supplemental conductivity scaling factor β_s.

[9] Refer to the Supplemental Geomagnetic Disturbance Event Description white paper for details on the determination of the reference geomagnetic field waveform: http://www.nerc.com/pa/Stand/Pages/Project-2013-03-Geomagnetic-Disturbance-Mitigation.aspx.

[10] The data file of the benchmark geomagnetic field waveform is available on the NERC GMD Task Force project webpage: http://www.nerc.com/comm/PC/Pages/Geomagnetic-Disturbance-Task-Force-(GMDTF)-2013.aspx.

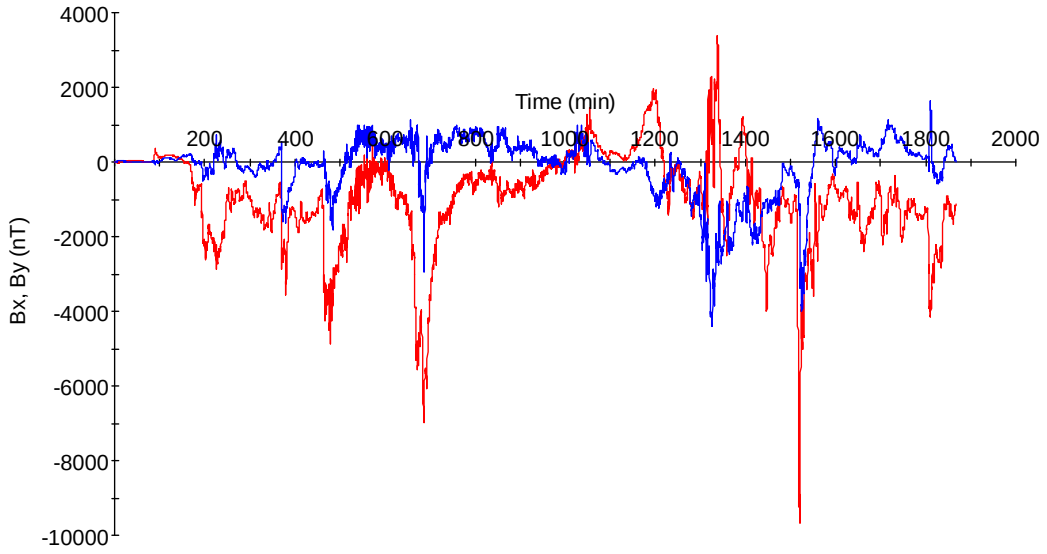


Figure 6: Supplemental Geomagnetic Field Waveform
Red B_N (Northward), Blue B_E (Eastward)

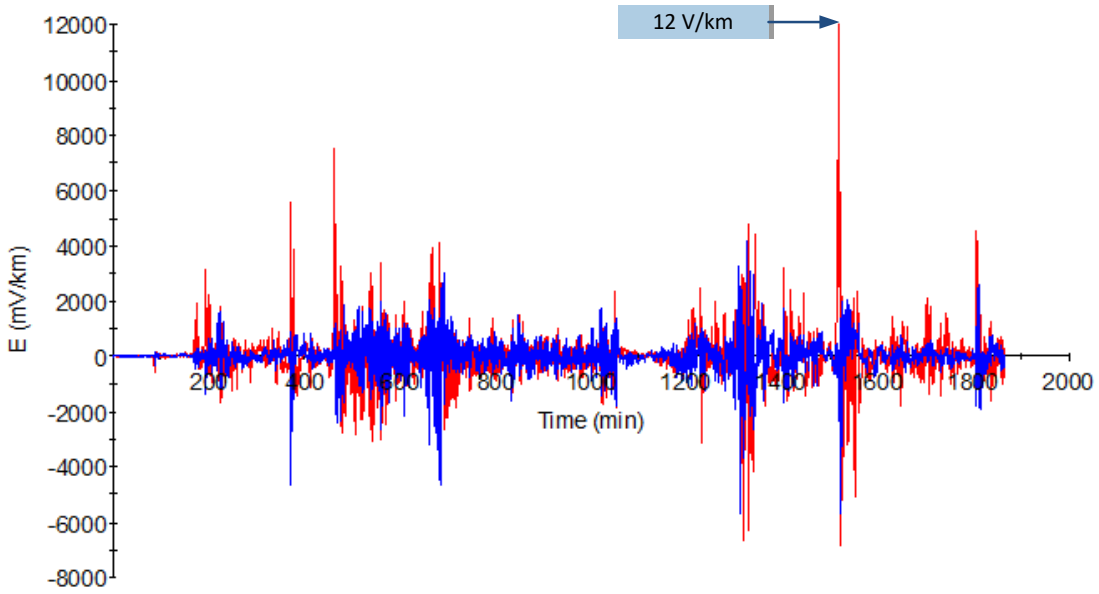


Figure 7: Supplemental Geoelectric Field Waveform
Blue E_N (Northward), Red E_E (Eastward)

Attachment 1-CAN

Attachment 1-CAN provides an alternative that a Canadian entity may use in lieu of the benchmark or supplemental GMD event(s) defined in Attachment 1 for performing GMD Vulnerability Assessment(s).

A Canadian entity may use the provisions of Attachment 1-CAN if it has regionally specific information that provides a technically justified means to re-define a 1-in-100 year GMD planning event(s) within its planning area.

Information for the Alternative Methodology

GMD Vulnerability Assessment(s) require the use of geophysical and engineering models. Canadian-specific data is available and growing. Ongoing research allows for more accurate characterization of regional parameters used in these models. Such Canadian-specific data includes geomagnetic field, earth conductivity, and geomagnetically induced current measurements that can be used for modeling and simulation validation.

Information used to calculate geoelectric fields for the benchmark and supplemental GMD events shall be clearly documented and technically justified. For example, the factors involved in the calculation of geoelectric fields are geomagnetic field variations and an earth transfer function(s).[1] Technically justified information used in modelling geomagnetic field variations may include: technical documents produced by governmental entities such as Natural Resources Canada; technical papers published in peer-reviewed journals; and data sets gathered using sound scientific principles. An earth transfer function may rely on magnetotelluric measurements or earth conductivity models.

Modeling assumptions shall also be clearly documented and technically justified. An entity may use sensitivity analysis to identify how the assumptions affect the results.

A simplified model may be used to perform a GMD Vulnerability Assessment(s), as long as the model is more conservative than a more detailed model.

When interpreting assessment results, the entity shall consider the maturity of the modeling, toolset, and techniques applied.

Geomagnetic Disturbance Planning Events

The 1-in-100 year planning event shall be based on regionally specific data and technically justifiable statistical analyses (e.g., extreme value theory) and applied to the benchmark and supplemental GMD Vulnerability Assessment(s).

For the benchmark GMD Vulnerability Assessment(s), an entity shall consider the large-scale spatial structure of the GMD event. For the supplemental GMD Vulnerability Assessment(s), an

[1] The “earth transfer function” is the relationship between the electric fields and magnetic field variations at the surface of the earth.

entity shall consider the small-scale spatial structure of the GMD event (e.g., using magnetometer measurements or realistic electrojet calculations).

Appendix TPL-007-4-QC-1

Specific provisions applicable in Québec for standard TPL-007-4 – Transmission System Planned Performance for Geomagnetic Disturbance Events

This appendix establishes specific provisions for the application of the standard in Québec. Provisions of the standard and of this appendix must be read jointly for comprehension and interpretation purposes. Where the standard and appendix differ, the appendix shall prevail.

A. Introduction

1. Title: No specific provisions.

2. Number: No specific provisions.

3. Purpose: No specific provisions.

4. Applicability:

4.1. Functional Entities

No specific provisions.

4.2. Facilities

4.2.1 No specific provisions**.**

5. Effective date:

5.1. Adoption of the standard by the Régie de l'énergie: September 14, 2022

5.2. Adoption of this appendix by the Régie de l'énergie: September 14, 2022

5.3. Effective date of the standard and of this appendix in Québec: April 1st, 2023

The requirements will be implemented on the following dates:

Requirement	Implementation date
R1	April 1st, 2023
R2	April 1st, 2023
R5 and R9	April 1st, 2023
R12 and R13	October 1st, 2023
R6 and R10	April 1st, 2025
R3, R4, R7, R8 and R11	April 1st, 2026

6. Background: No specific provisions.

Appendix TPL-007-4-QC-1

Specific provisions applicable in Québec for standard TPL-007-4 – Transmission System Planned Performance for Geomagnetic Disturbance Events

B. Requirements and Measures

Specific provision applicable to Requirement R5, R6, R9 and R10, and Measures M5, M6, M9 and M10 replace “BES” by “RTP”.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

In Québec, “Compliance Enforcement Authority” means the Régie de l’énergie in its roles of monitoring and enforcing compliance with respect to the Reliability Standard and to this appendix.

1.2. Evidence Retention

No specific provisions.

1.3. Compliance Monitoring and Enforcement Program

The Régie de l’énergie establishes the monitoring processes used to evaluate data or information for the purpose of determining compliance or non-compliance with the Reliability Standard and with this appendix.

Table 1: Steady State Planning GMD Event

Replace “BES” by “RTP”.

Violation Severity Levels

Replace “BES” by “RTP” for requirement R5, R6, R9 and R10 of the VSL.

D. Regional Variances

No specific provisions.

E. Associated Documents

No specific provisions.

Attachment 1

No specific provisions.

Attachment 1-CAN

No specific provisions.

Appendix TPL-007-4-QC-1

Specific provisions applicable in Québec for standard TPL-007-4 – Transmission System Planned Performance for Geomagnetic Disturbance Events

Version history

Version	Date	Action	Change tracking
1	September 14, 2022	New appendix as per decision D-2022-110.	New

A. Introduction

1. Title: Voltage and Reactive Control

2. Number: VAR-001-4.2

3. Purpose: To ensure that voltage levels, reactive flows, and reactive resources are monitored, controlled, and maintained within limits in Real-time to protect equipment and the reliable operation of the Interconnection.

4. Applicability:

4.1. Transmission Operators

4.2. Generator Operators within the Western Interconnection (for the WECC Variance)

5. Effective Date:

5.1. The standard shall become effective on the first day of the first calendar quarter after the date that the standard is approved by an applicable governmental authority or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective on the first day of the first calendar quarter after the date the standard is adopted by the NERC Board of Trustees or as otherwise provided for in that jurisdiction.

B. Requirements and Measures

R1. Each Transmission Operator shall specify a system voltage schedule (which is either a range or a target value with an associated tolerance band) as part of its plan to operate within System Operating Limits and Interconnection Reliability Operating Limits. *[Violation Risk Factor: High] [Time Horizon: Operations Planning]*

1.1. Each Transmission Operator shall provide a copy of the voltage schedules (which is either a range or a target value with an associated tolerance band) to its Reliability Coordinator and adjacent Transmission Operators within 30 calendar days of a request.

M1. The Transmission Operator shall have evidence that it specified system voltage schedules using either a range or a target value with an associated tolerance band.

For part 1.1, the Transmission Operator shall have evidence that the voltage schedules (which is either a range or a target value with an associated tolerance band) were provided to its Reliability Coordinator and adjacent Transmission Operators within 30 calendar days of a request. Evidence may include, but is not limited to, emails, website postings, and meeting minutes.

R2. Each Transmission Operator shall schedule sufficient reactive resources to regulate voltage levels under normal and Contingency conditions. Transmission Operators can provide sufficient reactive resources through various means including, but not limited to, reactive generation scheduling, transmission line and reactive resource switching, and using controllable load. *[Violation Risk Factor: High] [Time Horizon: Real-time Operations, Same-day Operations, and Operations Planning]*

M2. Each Transmission Operator shall have evidence of scheduling sufficient reactive resources based on their assessments of the system. For the operations planning time horizon, Transmission Operators shall have evidence of assessments used as the basis for how resources were scheduled.

R3. Each Transmission Operator shall operate or direct the Real-time operation of devices to regulate transmission voltage and reactive flow as necessary. *[Violation Risk Factor: High] [Time Horizon: Real-time Operations, Same-day Operations, and Operations Planning]*

M3. Each Transmission Operator shall have evidence that actions were taken to operate capacitive and inductive resources as necessary in Real-time. This may include, but is not limited to, instructions to Generator Operators to: 1) provide additional voltage support; 2) bring resources on-line; or 3) make manual adjustments.

R4. Each Transmission Operator shall specify the criteria that will exempt generators: 1) from following a voltage or Reactive Power schedule, 2) from having its automatic voltage regulator (AVR) in service or from being in voltage control mode, or 3) from having to make any associated notifications. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

4.1 If a Transmission Operator determines that a generator has satisfied the exemption criteria, it shall notify the associated Generator Operator.

M4. Each Transmission Operator shall have evidence of the documented criteria for generator exemptions.

For part 4.1, the Transmission Operator shall also have evidence to show that, for each generator in its area that is exempt: 1) from following a voltage or Reactive Power schedule, 2) from having its

automatic voltage regulator (AVR) in service or from being in voltage control mode, or 3) from having to make any notifications, the associated Generator Operator was notified of this exemption.

R5. Each Transmission Operator shall specify a voltage or Reactive Power schedule (which is either a range or a target value with an associated tolerance band) at either the high voltage side or low voltage side of the generator step-up transformer at the Transmission Operator's discretion. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

5.1. The Transmission Operator shall provide the voltage or Reactive Power schedule (which is either a range or a target value with an associated tolerance band) to the associated Generator Operator and direct the Generator Operator to comply with the schedule in automatic voltage control mode (the AVR is in service and controlling voltage).

5.2. The Transmission Operator shall provide the Generator Operator with the notification requirements for deviations from the voltage or Reactive Power schedule (which is either a range or a target value with an associated tolerance band).

5.3. The Transmission Operator shall provide the criteria used to develop voltage schedules or Reactive Power schedule (which is either a range or a target value with an associated tolerance band) to the Generator Operator within 30 days of receiving a request.

M5. The Transmission Operator shall have evidence of a documented voltage or Reactive Power schedule (which is either a range or a target value with an associated tolerance band).

For part 5.1, the Transmission Operator shall have evidence it provided a voltage or Reactive Power schedule (which is either a range or a target value with an associated tolerance band) to the applicable Generator Operators, and that the Generator Operator was directed to comply with the schedule in automatic voltage control mode, unless exempted.

For part 5.2, the Transmission Operator shall have evidence it provided notification requirements for deviations from the voltage or Reactive Power schedule (which is either a range or a target value with an associated tolerance band). For part 5.3, the Transmission Operator shall have evidence it provided the criteria used to develop voltage schedules or Reactive Power schedule (which is either a range or a target value with an associated tolerance band) within 30 days of receiving a request by a Generator Operator.

R6. After consultation with the Generator Owner regarding necessary step-up transformer tap changes and the implementation schedule, the Transmission Operator shall provide documentation to the Generator Owner specifying the required tap changes, a timeframe for making the changes, and technical justification for these changes. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M6. The Transmission Operator shall have evidence that it provided documentation to the Generator Owner when a change was needed to a generating unit's step-up transformer tap in accordance with the requirement and that it consulted with the Generator Owner.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

As defined in the NERC Rules of Procedure, “Compliance Enforcement Authority” refers to NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time a registered entity is required to retain specific evidence to demonstrate compliance. For instances in which the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask the registered entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Transmission Operator shall retain evidence for Measures M1 through M6 for 12 months. The Compliance Monitor shall retain any audit data for three years.

1.3. Compliance Monitoring and Assessment Processes:

“Compliance Monitoring and Assessment Processes” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated reliability standard.

1.4. Additional Compliance Information:

None

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**High**	N/A	N/A	N/A	The Transmission Operator does not specify a system voltage schedule (which is either a range or a target value with an associated tolerance band).
R2	**Real-time Operations, Same-day Operations, and Operations Planning**	**High**	N/A	N/A	The Transmission Operator does not schedule sufficient reactive resources as necessary to avoid violating an SOL.	The Transmission Operator does not schedule sufficient reactive resources as necessary to avoid violating an IROL.
R3	**Real-time Operations, Same-day Operations, and Operations Planning**	**High**	N/A	N/A	The Transmission Operator does not operate or direct any real-time operation of devices as necessary to avoid violating an SOL.	The Transmission Operator does not operate or direct any real-time operation of devices as necessary to avoid violating an IROL.

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R4	**Operations Planning**	**Lower**	N/A	N/A	The Transmission Operator has exemption criteria and notified the Generator Operator, but the Transmission Operator does not have evidence of the notification to the Generator Operator.	The Transmission Operator does not have exemption criteria.

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R5	**Operations Planning**	**Medium**	N/A	The Transmission Operator does not provide the criteria for voltage or Reactive Power schedules (which is either a range or a target value with an associated tolerance band) after 30 days of a request.	The Transmission Operator does not provide voltage or Reactive Power schedules (which is either a range or a target value with an associated tolerance band) to all Generator Operators.	The Transmission Operator does not provide voltage or Reactive Power schedules (which is either a range or a target value with an associated tolerance band) to any Generator Operators. Or The Transmission Operator does not provide the Generator Operator with the notification requirements for deviations from the voltage or Reactive Power schedule (which is either a range or a target value with an associated tolerance band).

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R6	**Operations Planning**	**Lower**	The Transmission Operator does not provide either the technical justification or timeframe for changing generator step-up tap settings.	N/A	N/A	The Transmission Operator does not provide the technical justification and the timeframe for changing generator step-up tap settings.

D. Regional Variances

The following Interconnection-wide variance shall be applicable in the Western Electricity Coordinating Council (WECC) and replaces, in their entirety, Requirements R4 and R5. Please note that Requirement R4 is deleted and R5 is replaced with the following requirements.

Requirements

E.A.13 Each Transmission Operator shall issue any one of the following types of voltage schedules to the Generator Operators for each of their generation resources that are on-line and part of the Bulk Electric System within the Transmission Operator Area: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same-day Operations]*

- A voltage set point with a voltage tolerance band and a specified period.
- An initial volt-ampere reactive output or initial power factor output with a voltage tolerance band for a specified period that the Generator Operator uses to establish a generator bus voltage set point.
- A voltage band for a specified period.

E.A.14 Each Transmission Operator shall provide one of the following voltage schedule reference points for each generation resource in its Area to the Generator Operator. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same-day Operations]*

- The generator terminals.
- The high side of the generator step-up transformer.
- The point of interconnection.
- A location designated by mutual agreement between the Transmission Operator and Generator Operator.

E.A.15 Each Generator Operator shall convert each voltage schedule specified in Requirement E.A.13 into the voltage set point for the generator excitation system. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same-day Operations]*

E.A.16 Each Generator Operator shall provide its voltage set point conversion methodology from the point in Requirement E.A.14 to the generator terminals within 30 calendar days of request by its Transmission Operator. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

E.A.17 Each Transmission Operator shall provide to the Generator Operator, within 30 calendar days of a request for data by the Generator Operator, its transmission equipment data and operating data that supports development of the voltage set point conversion methodology. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

E.A.18 Each Generator Operator shall meet the following control loop specifications if the Generator Operator uses control loops external to the automatic voltage regulators (AVR) to manage Mvar loading: *[Violation Risk Factor: Medium] [Time Horizon: Real-time Operations]*

E.A.18.1. Each control loop's design incorporates the AVR's automatic voltage controlled response to voltage deviations during System Disturbances.

E.A.18.2. Each control loop is only used by mutual agreement between the Generator Operator and the Transmission Operator affected by the control loop.

Measures[1]

M.E.A.13 Each Transmission Operator shall have and provide upon request, evidence that it provided the voltage schedules to the Generator Operator. Dated spreadsheets, reports, voice recordings, or other documentation containing the voltage schedule including set points, tolerance bands, and specified periods as required in Requirement E.A.13 are acceptable as evidence.

M.E.A.14 The Transmission Operator shall have and provide upon request, evidence that it provided one of the voltage schedule reference points in Requirement E.A.14 for each generation resource in its Area to the Generator Operator. Dated letters, e-mail, or other documentation that contains notification to the Generator Operator of the voltage schedule reference point for each generation resource are acceptable as evidence.

M.E.A.15 Each Generator Operator shall have and provide upon request, evidence that it converted a voltage schedule as described in Requirement E.A.13 into a voltage set point for the AVR. Dated spreadsheets, logs, reports, or other documentation are acceptable as evidence.

M.E.A.16 The Generator Operator shall have and provide upon request, evidence that within 30 calendar days of request by its Transmission Operator it provided its voltage set point conversion methodology from the point in Requirement E.A.14 to the generator terminals. Dated reports, spreadsheets, or other documentation are acceptable as evidence.

M.E.A.17 The Transmission Operator shall have and provide upon request, evidence that within 30 calendar days of request by its Generator Operator it provided data to support development of the voltage set point conversion methodology. Dated reports, spreadsheets, or other documentation are acceptable as evidence.

M.E.A.18 If the Generator Operator uses outside control loops to manage Mvar loading, the Generator Operator shall have and provide upon request, evidence that it met the control loop specifications in sub-parts E.A.18.1 through E.A.18.2. Design specifications with identified agreed-upon control loops, system reports, or other dated documentation are acceptable as evidence.

[1] The number for each measure corresponds with the number for each requirement, i.e. M.E.A.13 means the measure for Requirement E.A.13.

Violation Severity Levels

E #	Lower VSL	Moderate VSL	High VSL	Severe VSL
E.A.13	For the specified period, the Transmission Operator did not issue one of the voltage schedules listed in E.A.13 to at least one generation resource but less than or equal to 5% of the generation resources that are on-line and part of the BES in the Transmission Operator Area.	For the specified period, the Transmission Operator did not issue one of the voltage schedules listed in E.A.13 to more than 5% but less than or equal to 10% of the generation resources that are on-line and part of the BES in the Transmission Operator Area.	For the specified period, the Transmission Operator did not issue one of the voltage schedules listed in E.A.13 to more than 10% but less than or equal to 15% of the generation resources that are on-line and part of the BES in the Transmission Operator Area.	For the specified period, the Transmission Operator did not issue one of the voltage schedules listed in E.A.13 to more than 15% of the generation resources that are on-line and part of the BES in the Transmission Operator Area.
E.A.14	The Transmission Operator did not provide a voltage schedule reference point for at least one but less than or equal to 5% of the generation resources in the Transmission Operator area.	The Transmission Operator did not provide a voltage schedule reference point for more than 5% but less than or equal to 10% of the generation resources in the Transmission Operator Area.	The Transmission Operator did not a voltage schedule reference point for more than 10% but less than or equal to 15% of the generation resources in the Transmission Operator Area.	The Transmission Operator did not provide a voltage schedule reference point for more than 15% of the generation resources in the Transmission Operator Area.
E.A.15	The Generator Operator failed to convert at least one voltage schedule in Requirement E.A.13 into the voltage set point for the AVR for less than 25% of the voltage schedules.	The Generator Operator failed to convert the voltage schedules in Requirement E.A.13 into the voltage set point for the AVR for 25% or more but less than 50% of the voltage schedules.	The Generator Operator failed to convert the voltage schedules in Requirement E.A.13 into the voltage set point for the AVR for 50% or more but less than 75% of the voltage schedules.	The Generator Operator failed to convert the voltage schedules in Requirement E.A.13 into the voltage set point for the AVR for 75% or more of the voltage schedules.

E #	Lower VSL	Moderate VSL	High VSL	Severe VSL
E.A.16	The Generator Operator provided its voltage set point conversion methodology greater than 30 days but less than or equal to 60 days of a request by the Transmission Operator.	The Generator Operator provided its voltage set point conversion methodology greater than 60 days but less than or equal to 90 days of a request by the Transmission Operator.	The Generator Operator provided its voltage set point conversion methodology greater than 90 days but less than or equal to 120 days of a request by the Transmission Operator.	The Generator Operator did not provide its voltage set point conversion methodology within 120 days of a request by the Transmission Operator.
E.A.17	The Transmission Operator provided its data to support development of the voltage set point conversion methodology than 30 days but less than or equal to 60 days of a request by the Generator Operator.	The Transmission Operator provided its data to support development of the voltage set point conversion methodology greater than 60 days but less than or equal to 90 days of a request by the Generator. Operator.	The Transmission Operator provided its data to support development of the voltage set point conversion methodology greater than 90 days but less than or equal to 120 days of a request by the Generator. Operator.	The Transmission Operator did not provide its data to support development of the voltage set point conversion methodology within 120 days of a request by the Generator Operator.
E.A.18	N/A	The Generator Operator did not meet the control loop specifications in EA18.2 when the Generator Operator uses control loop external to the AVR to manage Mvar loading.	The Generator Operator did not meet the control loop specifications in EA18.1 when the Generator Operator uses control loop external to the AVR to manage Mvar loading.	The Generator Operator did not meet the control loop specifications in EA18.1 through EA18.2 when the Generator Operator uses control loop external to the AVR to manage Mvar loading.

E. Interpretations

None

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
0	April 1, 2005	Effective Date	New
1	August 2, 2006	BOT Adoption	Revised
1	June 18, 2007	FERC approved Version 1 of the standard.	Revised
1	July 3, 2007	Added “Generator Owners” and “Generator Operators” to Applicability section.	Errata
1	August 23, 2007	Removed “Generator Owners” and “Generator Operators” to Applicability section.	Errata
2	August 5, 2010	Adopted by NERC Board of Trustees; Modified to address Order No. 693 Directives contained in paragraphs 1858 and 1879.	Revised
2	January, 10 2011	FERC issued letter order approving the addition of LSEs and Controllable Load to the standard.	Revised
3	May 9, 2012	Adopted by NERC Board of Trustees; Modified to add a WECC region variance	Revised
3	June 20, 2013	FERC issued order approving VAR-001-3	Revised
3	November 21, 2013	R5 and associated elements approved by FERC for retirement as part of the Paragraph 81 project (Project 2013-02)	Revised
4	February 6, 2014	Adopted by NERC Board of Trustees	Revised
4	August 1, 2014	FERC issued letter order issued approving VAR-001-4	
4.1	August 25, 2015	Added “or” to Requirement R5, 5.3 to read: schedules or Reactive Power	Errata
4.1	November 13, 2015	FERC Letter Order approved errata to VAR-001-4.1. Docket RD15-6-000	Errata
4.2	June 14, 2017	Project 2016-EPR-02 errata recommendations	Errata
4.2	August 10, 2017	Adopted by NERC Board of Trustees	Errata
4.2	September 26, 2017	FERC Letter Order issued approving VAR-001-4.2 Docket No. RD17-7-000.	

Guidelines and Technical Basis

For technical basis for each requirement, please review the rationale provided for each requirement.

Rationale:

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for R1:

Paragraph 1868 of Order No. 693 requires NERC to add more "detailed and definitive requirements on “established limits” and “sufficient reactive resources”, and identify acceptable margins (i.e. voltage and/or reactive power margins)." Since Order No. 693 was issued, however, several FAC and TOP standards have become enforceable to add more requirements around voltage limits. More specifically, FAC-011 and FAC-014 require that System Operating Limits (SOLs) and reliability margins are established. The NERC Glossary definition of SOLs includes both: 1) voltage stability ratings (Applicable pre- and post-Contingency Voltage Stability) and 2*)* System Voltage Limits (Applicable pre- and post-Contingency voltage limits). Therefore, for reliability reasons Requirement R1 now requires a Transmission Operator (TOP) to set voltage or Reactive Power schedules with associated tolerance bands. Further, since neighboring areas can affect each other greatly, each TOP must also provide a copy of these schedules to its Reliability Coordinator (RC) and adjacent TOP upon request.

Rationale for R2:

Paragraph 1875 from Order No. 693 directed NERC to include requirements to run voltage stability analysis periodically, using online techniques where commercially available and offline tools when online tools are not available. This standard does not explicitly require the periodic voltage stability analysis because such analysis would be performed pursuant to the SOL methodology developed under the FAC standards. TOP standards also require the TOP to operate within SOLs and Interconnection Reliability Operating Limits (IROL). The VAR standard drafting team (SDT) and industry participants also concluded that the best models and tools are the ones that have been proven and the standard should not add a requirement for a responsible entity to purchase new online simulations tools. Thus, the VAR SDT simplified the requirements to ensuring sufficient reactive resources are online or scheduled. Controllable load is specifically included to answer FERC's directive in Order No. 693 at Paragraph 1879.

Rationale for R3:

Similar to Requirement R2, the VAR SDT determined that for reliability purposes, the TOP must ensure sufficient voltage support is provided in Real-time in order to operate within an SOL.

Rationale for R4:

The VAR SDT received significant feedback on instances when a TOP would need the flexibility for defining exemptions for generators. These exemptions can be tailored as the TOP deems necessary for the specific

area's needs. The goal of this requirement is to provide a TOP the ability to exempt a Generator Operator (GOP) from: 1) a voltage or Reactive Power schedule, 2) a setting on the AVR, or 3) any VAR-002 notifications based on the TOP's criteria. Feedback from the industry detailed many system events that would require these types of exemptions which included, but are not limited to: 1) maintenance during shoulder months, 2) scenarios where two units are located within close proximity and both cannot be in voltage control mode, and 3) large system voltage swings where it would harm reliability if all GOP were to notify their respective TOP of deviations at one time. Also, in an effort to improve the requirement, the sub-requirements containing an exemption list were removed from the currently enforceable standard because this created more compliance issues with regard to how often the list would be updated and maintained.

Rationale for R5:

The new requirement provides transparency regarding the criteria used by the TOP to establish the voltage schedule. This requirement also provides a vehicle for the TOP to use appropriate granularity when setting notification requirements for deviation from the voltage or Reactive Power schedule. Additionally, this requirement provides clarity regarding a "tolerance band" as specified in the voltage schedule and the control dead-band in the generator's excitation system.

Voltage schedule tolerances are the bandwidth that accompanies the voltage target in a voltage schedule, should reflect the anticipated fluctuation in voltage at the Generation Operator's facility during normal operations, and be based on the TOP's assessment of N-1 and credible N-2 system contingencies. The voltage schedule's bandwidth should not be confused with the control dead-band that is programmed into a Generation Operator's automatic voltage regulator's control system, which should be adjusting the AVR prior to reaching either end of the voltage schedule's bandwidth.

Rationale for R6:

Although tap settings are first established prior to interconnection, this requirement could not be deleted because no other standard addresses when a tap setting must be adjusted. If the tap setting is not properly set, then the amount of VARs produced by a unit can be affected.

Appendix QC-VAR-001-4.2
Provisions specific to the standard VAR-001-4.2 applicable in Québec

This appendix establishes specific provisions for the application of the standard in Québec. Provisions of the standard and of its appendix must be read together for the purposes of understanding and interpretation. Where the standard and appendix differ, the appendix shall prevail.

A. Introduction

1. **Title:** Voltage Reactive Control
2. **Number:** VAR-001-4.2
3. **Purpose:** No specific provision
4. **Applicability:**

Functions

No specific provision.

Facilities

This standard only applies to the facilities of the Main Transmission System (RTP).

5. **Effective Date:**

5.1. Adoption of the standard by the Régie de l'énergie: February 22nd, 2018

5.2. Adoption of the appendix by the Régie de l'énergie: February 22nd, 2018

5.3. Effective date of the standard and its appendix in Québec: April 1st, 2018

B. Requirements and Measures

Specific provision applicable to requirement R6:

The Transmission Operators is not required to provide documentation to the Generator Owner specifying necessary tap changes, a timeframe for making the changes and technical justification for these changes considering that the Transmission Operator will give instructions based on the voltage to be maintained on the transmission system.

C. Compliance

1. **Compliance Monitoring Process**

1.1. Compliance Enforcement Authority

The Régie de l'énergie is responsible, in Québec, for compliance enforcement with respect to the reliability standard and its appendix that it adopts.

1.2. Evidence Retention

No specific provision

1.3. Compliance Monitoring and Assessment Processes

No specific provision

1.4. Additional Compliance Information

No specific provision

Table of Compliance Elements

No specific provision

D. Regional Variances

No specific provision

E. Interpretations

No specific provision

F. Associated Documents

No specific provision

Guidelines and Technical Basis

No specific provision

Revision History

Revision	Date	Action	Change Tracking
0	February 22nd, 2018	New appendix	New

A. Introduction

1. Title: **Generator Operation for Maintaining Network Voltage Schedules**

2. Number: **VAR-002-4.1**

3. Purpose: To ensure generators provide reactive support and voltage control, within generating Facility capabilities, in order to protect equipment and maintain reliable operation of the Interconnection.

4. Applicability:

4.1. Generator Operator

4.2. Generator Owner

5. Effective Dates

See Implementation Plan.

B. Requirements and Measures

R1. The Generator Operator shall operate each generator connected to the interconnected transmission system in the automatic voltage control mode (with its automatic voltage regulator (AVR) in service and controlling voltage) or in a different control mode as instructed by the Transmission Operator unless: 1) the generator is exempted by the Transmission Operator, or 2) the Generator Operator has notified the Transmission Operator of one of the following: *[Violation Risk Factor: Medium] [Time Horizon: Real-time Operations]*

- That the generator is being operated in start-up,[1] shutdown,[2] or testing mode pursuant to a Real-time communication or a procedure that was previously provided to the Transmission Operator; or
- That the generator is not being operated in automatic voltage control mode or in the control mode that was instructed by the Transmission Operator for a reason other than start-up, shutdown, or testing.

M1. The Generator Operator shall have evidence to show that it notified its associated Transmission Operator any time it failed to operate a generator in the automatic voltage control mode or in a different control mode as specified in Requirement R1. If a generator is being started up or shut down with the automatic voltage control off, or is being tested, and no notification of the AVR status is made to the Transmission Operator, the Generator Operator will have evidence that it notified the Transmission Operator of its procedure for placing the unit into automatic voltage control mode as required in Requirement R1. Such evidence may include, but is not limited to, dated evidence of transmittal of the procedure such as an electronic message or a transmittal letter with the procedure included or attached. If a generator is exempted, the Generator Operator shall also have evidence that the generator is exempted from being in automatic voltage control mode (with its AVR in service and controlling voltage).

[1] Start-up is deemed to have ended when the generator is ramped up to its minimum continuously sustainable load and the generator is prepared for continuous operation.

[2] Shutdown is deemed to begin when the generator is ramped down to its minimum continuously sustainable load and the generator is prepared to go offline.

R2. Unless exempted by the Transmission Operator, each Generator Operator shall maintain the generator voltage or Reactive Power schedule[3] (within each generating Facility's capabilities[4]) provided by the Transmission Operator, or otherwise shall meet the conditions of notification for deviations from the voltage or Reactive Power schedule provided by the Transmission Operator. *[Violation Risk Factor: Medium] [Time Horizon: Real-time Operations]*

2.1. When a generator's AVR is out of service or the generator does not have an AVR, the Generator Operator shall use an alternative method to control the generator reactive output to meet the voltage or Reactive Power schedule provided by the Transmission Operator.

2.2. When instructed to modify voltage, the Generator Operator shall comply or provide an explanation of why the schedule cannot be met.

2.3. Generator Operators that do not monitor the voltage at the location specified in their voltage schedule shall have a methodology for converting the scheduled voltage specified by the Transmission Operator to the voltage point being monitored by the Generator Operator.

M2. In order to identify when a generator is deviating from its schedule, the Generator Operator will monitor voltage based on existing equipment at its Facility. The Generator Operator shall have evidence to show that the generator maintained the voltage or Reactive Power schedule provided by the Transmission Operator, or shall have evidence of meeting the conditions of notification for deviations from the voltage or Reactive Power schedule provided by the Transmission Operator.

Evidence may include, but is not limited to, operator logs, SCADA data, phone logs, and any other notifications that would alert the Transmission Operator or otherwise demonstrate that the Generator Operator complied with the Transmission Operator's instructions for addressing deviations from the voltage or Reactive Power schedule.

For Part 2.1, when a generator's AVR is out of service or the generator does not have an AVR, a Generator Operator shall have evidence to show an alternative method was used to control the generator reactive output to meet the voltage or Reactive Power schedule provided by the Transmission Operator.

For Part 2.2, the Generator Operator shall have evidence that it complied with the Transmission Operator's instructions to modify its voltage or provided an explanation to the Transmission Operator of why the Generator Operator was unable to comply with the instruction. Evidence may include, but is not limited to, operator logs, SCADA data, and phone logs.

For Part 2.3, for Generator Operators that do not monitor the voltage at the location specified on the voltage schedule, the Generator Operator shall demonstrate the methodology for converting the scheduled voltage specified by the Transmission Operator to the voltage point being monitored by the Generator Operator.

[3] The voltage or Reactive Power schedule is a target value with a tolerance band or a voltage or Reactive Power range communicated by the Transmission Operator to the Generator Operator.

[4] Generating Facility capability may be established by test or other means, and may not be sufficient at times to pull the system voltage within the schedule tolerance band. Also, when a generator is operating in manual control, Reactive Power capability may change based on stability considerations.

R3. Each Generator Operator shall notify its associated Transmission Operator of a status change on the AVR, power system stabilizer, or alternative voltage controlling device within 30 minutes of the change. If the status has been restored within 30 minutes of such change, then the Generator Operator is not required to notify the Transmission Operator of the status change. *[Violation Risk Factor: Medium] [Time Horizon: Real-time Operations]*

M3. The Generator Operator shall have evidence it notified its associated Transmission Operator within 30 minutes of any status change identified in Requirement R3. If the status has been restored within the first 30 minutes, no notification is necessary.

R4. Each Generator Operator shall notify its associated Transmission Operator within 30 minutes of becoming aware of a change in reactive capability due to factors other than a status change described in Requirement R3. If the capability has been restored within 30 minutes of the Generator Operator becoming aware of such change, then the Generator Operator is not required to notify the Transmission Operator of the change in reactive capability. *[Violation Risk Factor: Medium] [Time Horizon: Real-time Operations]*

- Reporting of status or capability changes as stated in Requirement R4 is not applicable to the individual generating units of dispersed power producing resources identified through Inclusion I4 of the Bulk Electric System definition.

M4. The Generator Operator shall have evidence it notified its associated Transmission Operator within 30 minutes of becoming aware of a change in reactive capability in accordance with Requirement R4. If the capability has been restored within the first 30 minutes, no notification is necessary.

R5. The Generator Owner shall provide the following to its associated Transmission Operator and Transmission Planner within 30 calendar days of a request. *[Violation Risk Factor: Lower] [Time Horizon: Real-time Operations]*

5.1. For generator step-up and auxiliary transformers[5] with primary voltages equal to or greater than the generator terminal voltage:

5.1.1. Tap settings.

5.1.2. Available fixed tap ranges.

5.1.3. Impedance data.

M5. The Generator Owner shall have evidence it provided its associated Transmission Operator and Transmission Planner with information on its step-up and auxiliary transformers as required in Requirement R5, Part 5.1.1 through Part 5.1.3 within 30 calendar days.

[5] For dispersed power producing resources identified through Inclusion I4 of the Bulk Electric System definition, this requirement applies only to those transformers that have at least one winding at a voltage of 100 kV or above.

R6. After consultation with the Transmission Operator regarding necessary step-up transformer tap changes, the Generator Owner shall ensure that transformer tap positions are changed according to the specifications provided by the Transmission Operator, unless such action would violate safety, an equipment rating, a regulatory requirement, or a statutory requirement. *[Violation Risk Factor: Lower] [Time Horizon: Real-time Operations]*

6.1. If the Generator Owner cannot comply with the Transmission Operator's specifications, the Generator Owner shall notify the Transmission Operator and shall provide the technical justification.

M6. The Generator Owner shall have evidence that its step-up transformer taps were modified per the Transmission Operator's documentation in accordance with Requirement R6. The Generator Owner shall have evidence that it notified its associated Transmission Operator when it could not comply with the Transmission Operator's step-up transformer tap specifications in accordance with Requirement R6, Part 6.1.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

As defined in the NERC Rules of Procedure, “Compliance Enforcement Authority” refers to NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Generator Owner shall keep its latest version of documentation on its step-up and auxiliary transformers. The Generator Operator shall maintain all other evidence for the current and previous calendar year.

The Compliance Monitor shall retain any audit data for three years.

1.3. Compliance Monitoring and Assessment Processes:

“Compliance Monitoring and Assessment Processes” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated reliability standard.

1.4. Additional Compliance Information:

None.

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Real-time Operations**	**Medium**	N/A	N/A	N/A	Unless exempted, the Generator Operator did not operate each generator connected to the interconnected transmission system in the automatic voltage control mode or in a different control mode as instructed by the Transmission Operator, and failed to provide the required notifications to Transmission Operator as identified in Requirement R1.

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R2	**Real-time Operations**	**Medium**	N/A	N/A	The Generator Operator did not have a conversion methodology when it monitors voltage at a location different from the schedule provided by the Transmission Operator.	The Generator Operator did not maintain the voltage or Reactive Power schedule as instructed by the Transmission Operator and did not make the necessary notifications required by the Transmission Operator. OR The Generator Operator did not have an operating AVR, and the responsible entity did not use an alternative method for controlling voltage. OR The Generator Operator did not modify voltage when directed, and the responsible entity did not provide any explanation.
R3	**Real-time Operations**	**Medium**	N/A	N/A	N/A	The Generator Operator did not make the required notification within 30 minutes of the status change.

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R4	**Real-time Operations**	**Medium**	N/A	N/A	N/A	The Generator Operator did not make the required notification within 30 minutes of becoming aware of the capability change.
R5	**Real-time Operations**	**Lower**	N/A	N/A	The Generator Owner failed to provide its associated Transmission Operator and Transmission Planner one of the types of data specified in Requirement R5 Parts 5.1.1, 5.1.2, and 5.1.3.	The Generator Owner failed to provide to its associated Transmission Operator and Transmission Planner two or more of the types of data specified in Requirement R5 Parts 5.1.1, 5.1.2, and 5.1.3.

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R6	**Real-time Operations**	**Lower**	N/A	N/A	N/A	The Generator Owner did not ensure the tap changes were made according the Transmission Operator's specifications. OR The Generator Owner failed to perform the tap changes, and the Generator Owner did not provide technical justification for why it could not comply with the Transmission Operator specifications.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	5/1/2006	Added "(R2)" to the end of levels on non-compliance 2.1.2, 2.2.2, 2.3.2, and2.4.3.	July 5, 2006
1a	12/19/2007	Added Appendix 1 – Interpretation of R1 and R2 approved by BOT on August 1, 2007	Revised
1a	1/16/2007	In Section A.2., Added "a" to end of standard number. Section F: added "1."; and added date.	Errata
1.1a	10/29/2008	BOT adopted errata changes; updated version number to "1.1a"	Errata
1.1b	3/3/2009	Added Appendix 2 – Interpretation of VAR-002-1.1a approved by BOT on February 10, 2009	Revised
2b	4/16/2013	Revised R1 to address an Interpretation Request. Also added previously approved VRFs, Time Horizons and VSLs. Revised R2 to address consistency issue with VAR-001-2, R4. FERC Order issued approving VAR-002-2b.	Revised
3	5/5/2014	Revised under Project 2013-04 to address outstanding Order 693 directives.	Revised
3	5/7/2014	Adopted by NERC Board of Trustees	
3	8/1/2014	Approved by FERC in docket RD14-11-000	
4	8/27/2014	Revised under Project 2014-01 to clarify applicability of Requirements to	Revised

		BES dispersed power producing resources.	
4	11/13/2014	Adopted by NERC Board of Trustees	
4	5/29/2015	FERC Letter Order in Docket No. RD15-3-000 approving VAR-002-4	
4.1	June 14, 2017	Project 2016-EPR-02 errata recommendations	Errata
4.1	August 10, 2017	Adopted by the NERC Board of Trustees	Errata
4.1	September 26, 2017	FERC Letter Order issued approving VAR-002-4.1 RD17-7-000	

Guidelines and Technical Basis

Rationale:

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for R1:

This requirement has been maintained due to the importance of running a unit with its automatic voltage regulator (AVR) in service and in either voltage controlling mode or the mode instructed by the TOP. However, the requirement has been modified to allow for testing, and the measure has been updated to include some of the evidence that can be used for compliance purposes.

Rationale for R2:

Requirement R2 details how a Generator Operator (GOP) operates its generator(s) to provide voltage support and when the GOP is expected to notify the Transmission Operator (TOP). In an effort to remove prescriptive notification requirements for the entire continent, the VAR-002-3 standard drafting team (SDT) opted to allow each TOP to determine the notification requirements for each of its respective GOPs based on system requirements. Additionally, a new Part 2.3 has been added to detail that each GOP may monitor voltage by using its existing facility equipment.

Conversion Methodology: There are many ways to convert the voltage schedule from one voltage level to another. Some entities may choose to develop voltage regulation curves for their transformers; others may choose to do a straight ratio conversion; others may choose an entirely different methodology. All of these methods have technical challenges, but the studies performed by the TOP, which consider N-1 and credible N-2 contingencies, should compensate for the error introduced by these methodologies, and the TOP possesses the authority to direct the GOP to modify its output if its performance is not satisfactory. During a significant system event, such as a voltage collapse, even a generation unit in automatic voltage control that controls based on the low-side of the generator step-up transformer should see the event on the low-side of the generator step-up transformer and respond accordingly.

Voltage Schedule Tolerances: The bandwidth that accompanies the voltage target in a voltage schedule should reflect the anticipated fluctuation in voltage at the GOP's Facility during normal operations and be based on the TOP's assessment of N-1 and credible N-2 system contingencies. The voltage schedule's bandwidth should not be confused with the control dead-band that is programmed into a GOP's AVR control system, which should be adjusting the AVR prior to reaching either end of the voltage schedule's bandwidth.

Rationale for R3:

This requirement has been modified to limit the notifications required when an AVR goes out of service and quickly comes back in service. Notifications of this type of status change provide little to no benefit to reliability. Thirty (30) minutes have been built into the requirement to allow a GOP time to resolve an issue before having to notify the TOP of a status change. The requirement has

also been amended to remove the sub-requirement to provide an estimate for the expected duration of the status change.

Rationale for R4:

This requirement has been bifurcated from the prior version VAR-002-2b Requirement R3. This requirement allows GOPs to report reactive capability changes after they are made aware of the change. The current standard requires notification as soon as the change occurs, but many GOPs are not aware of a reactive capability change until it has taken place.

Rationale for Exclusion in R4:

VAR-002 addresses control and management of reactive resources and provides voltage control where it has an impact on the BES. For dispersed power producing resources as identified in Inclusion I4, Requirement R4 should not apply at the individual generator level due to the unique characteristics and small scale of individual dispersed power producing resources. In addition, other standards such as proposed TOP-003 require the Generator Operator to provide Real-time data as directed by the TOP.

Rationale for R5:

This requirement and corresponding measure have been maintained due to the importance of having accurate tap settings. If the tap setting is not properly set, then the VARs available from that unit can be affected. The prior version of VAR-002-2b, Requirement R4.1.4 (the +/- voltage range with step-change in % for load-tap changing transformers) has been removed. The percentage information was not needed because the tap settings, ranges and impedance are required. Those inputs can be used to calculate the step-change percentage if needed.

Rationale for Exclusion in R5:

The Transmission Operator and Transmission Planner only need to review tap settings, available fixed tap ranges, impedance data and the +/- voltage range with step-change in % for load-tap changing transformers on main generator step-up unit transformers which connect dispersed power producing resources identified through Inclusion I4 of the Bulk Electric System definition to their transmission system. The dispersed power producing resources individual generator transformers are not intended, designed or installed to improve voltage performance at the point of interconnection. In addition, the dispersed power producing resources individual generator transformers have traditionally been excluded from Requirement R4 and R5 of VAR-002-2b (similar requirements are R5 and R6 for VAR-002-3), as they are not used to improve voltage performance at the point of interconnection.

Rationale for R6:

This requirement and corresponding measure have been maintained due to the importance of having accurate tap settings. If the tap setting is not properly set, then the VARs available from that unit can be affected.

Appendix VAR-002-4.1-QC-1

Specific provisions applicable in Québec for standard VAR-002-4.1 – Generator Operation for Maintaining Network Voltage Schedules

This appendix establishes specific provisions for the application of the standard in Québec. Provisions of the standard and of this appendix must be read jointly for comprehension and interpretation purposes. Where the standard and appendix differ, the appendix shall prevail.

A. Introduction

1. Title: No specific provisions.

2. Number: No specific provisions.

3. Purpose: No specific provisions.

4. Applicability:

No specific provisions in regard to the applicable entities.

The Facilities subject to this Standard are the Facilities of the Main Transmission System (RTP).

5. Effective date:

5.1.	Adoption of the standard by the Régie de l'énergie:	October 8, 2020
5.2.	Adoption of this appendix by the Régie de l'énergie:	October 8, 2020
	Effective date of the standard and of this appendix in Québec:	January 1, 2021

B. Requirements and Measures

Specific provision applicable to Requirement R2:

If the Generator Operator is also a Transmission Owner, replace only the text of Requirement R2, without changing parts 2.1 to 2.3, with the following:

R2. Unless exempted by the Transmission Operator, each Generator Operator shall maintain the generator voltage or Reactive Power schedule[3] (within each generating Facility's capabilities[4]) provided by the Transmission Operator at the points of interconnection of its system to the Main Transmission System, or otherwise shall meet the conditions of notification for deviations from the voltage or Reactive Power schedule provided by the Transmission Operator.

Specific provision applicable to requirements R5 and R6:

Generator Owners are not required to comply with Requirement R5, and parts 5.1, 5.1.1, 5.1.2 and 5.1.3, or Requirement R6 and Part 6.1 given that the Transmission Operator will provide directives based on the voltage to be maintained on the transmission system.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

In Québec, "Compliance Enforcement Authority" means the Régie de l'énergie in its roles of monitoring and enforcing compliance with respect to the Reliability Standard and to this appendix.

1.2. Evidence Retention

No specific provisions.

1.3. Compliance Monitoring and Assessment Processes

The Régie de l'énergie establishes the monitoring processes used to evaluate data or information for the purpose of determining compliance or non-compliance with the Reliability Standard and with this appendix.

1.4. Additional Compliance Information

No specific provisions.

Table of Compliance Elements

No specific provisions.

D. Regional Variances

No specific provisions.

E. Interpretations

No specific provisions.

F. Associated Documents

No specific provisions.

Guidelines and Technical Basis

No specific provisions.

Version history

Version	Date	Action	Change tracking
1	October 8, 2020	New appendix	New