Justification technique et Guide d'application de la norme CIP-012-1 (version anglaise)

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Cyber Security – Communications between Control Centers

Technical Rationale and Justification for Reliability Standard CIP-012-1

August 2018

RELIABILITY | ACCOUNTABILITY



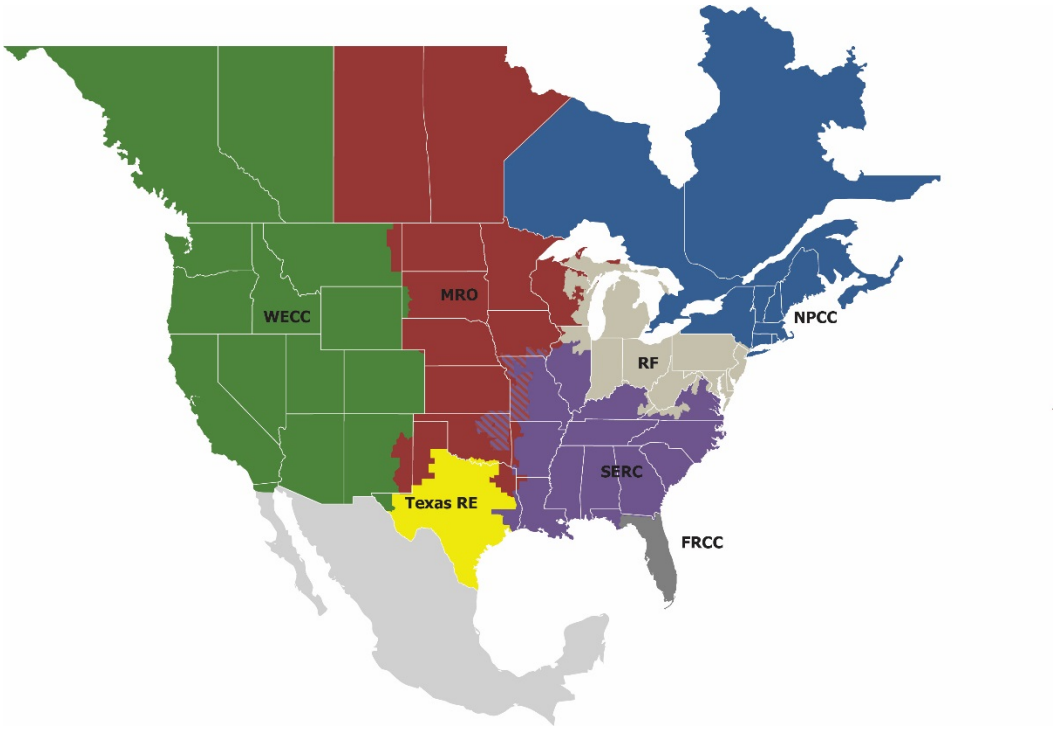

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Preface

The vision for the Electric Reliability Organization (ERO) Enterprise, which is comprised of the North American Electric Reliability Corporation (NERC) and the seven Regional Entities (REs), is a highly reliable and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

The North American BPS is divided into seven RE boundaries as shown in the map and corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one Region while associated Transmission Owners/Operators participate in another.



FRCC	Florida Reliability Coordinating Council
MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-012-1. It will provide stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. It also contains information on the SDT's intent in drafting the requirements. This Technical Rationale and Justification for CIP-012-1 is not a Reliability Standard and should not be considered mandatory and enforceable.

On January 21, 2016, the Federal Energy Regulatory Commission (FERC or Commission) issued Order No. 822, approving seven Critical Infrastructure Protection (CIP) Reliability Standards and new or modified terms in the Glossary of Terms Used in NERC Reliability Standards, and directing modifications to the CIP Reliability Standards. Among others, the Commission directed the North American Electric Reliability Corporation (NERC) to "develop modifications to the CIP Reliability Standards to require Responsible Entities[1] to implement controls to protect, at a minimum, communication links and sensitive bulk electric system data communicated between bulk electric system Control Centers in a manner that is appropriately tailored to address the risks posed to the bulk electric system by the assets being protected (i.e., high, medium, or low impact)." (Order 822, Paragraph 53)

In response to the directive in Order No. 822, the Project 2016-02 standard drafting team (SDT) drafted Reliability Standard CIP-012-1 to require Responsible Entities to implement controls to protect sensitive Bulk Electric System (BES) data and communications links between BES Control Centers. Due to the sensitivity of the data being communicated between Control Centers, as defined in the Glossary of Terms Used in NERC Reliability Standards, the standard applies to all impact levels (i.e., high, medium, or low impact).

Although the Commission directed NERC to develop modifications to CIP-006, the SDT determined that modifications to CIP-006 would not be appropriate. There are differences between the plan(s) required to be developed and implemented for CIP-012-1 and the protection required in CIP-006-6 Requirement R1 Part 1.10. CIP-012-1 Requirements R1 and R2 protect the applicable data during transmission between two separate Control Centers. CIP-006-6 Requirement R1 Part 1.10 protects nonprogrammable communication components within an Electronic Security Perimeter (ESP) but outside of a Physical Security Perimeter (PSP). The transmission of applicable data between Control Centers takes place outside of an ESP. Therefore, the protection contained in CIP-006-6 Requirement R1 Part 1.10 does not apply.

The SDT drafted requirements to provide Responsible Entities the latitude to protect the communication links, the data, or both to satisfy the security objective consistent with the capabilities of the Responsible Entity's operational environment.

CIP-012 Exemption (4.2.3) for certain Control Centers

In the process of drafting CIP-012, the SDT became aware of certain generating plant or Transmission substation situations where such field assets could be dual-classified as Control Centers based on the current Control Center definition. Their communications to their BA or TOP Control Centers, however, are not included in the intended scope of CIP-012. This is because the communications do not differ from those of any other generating plant or substation. The SDT wrote an exemption (Section 4.2.3 within CIP-012) for this particular scenario which is described in further detail below.

I

[1] As used in the CIP Standards, a Responsible Entity refers to the registered entities subject to the CIP Standards.

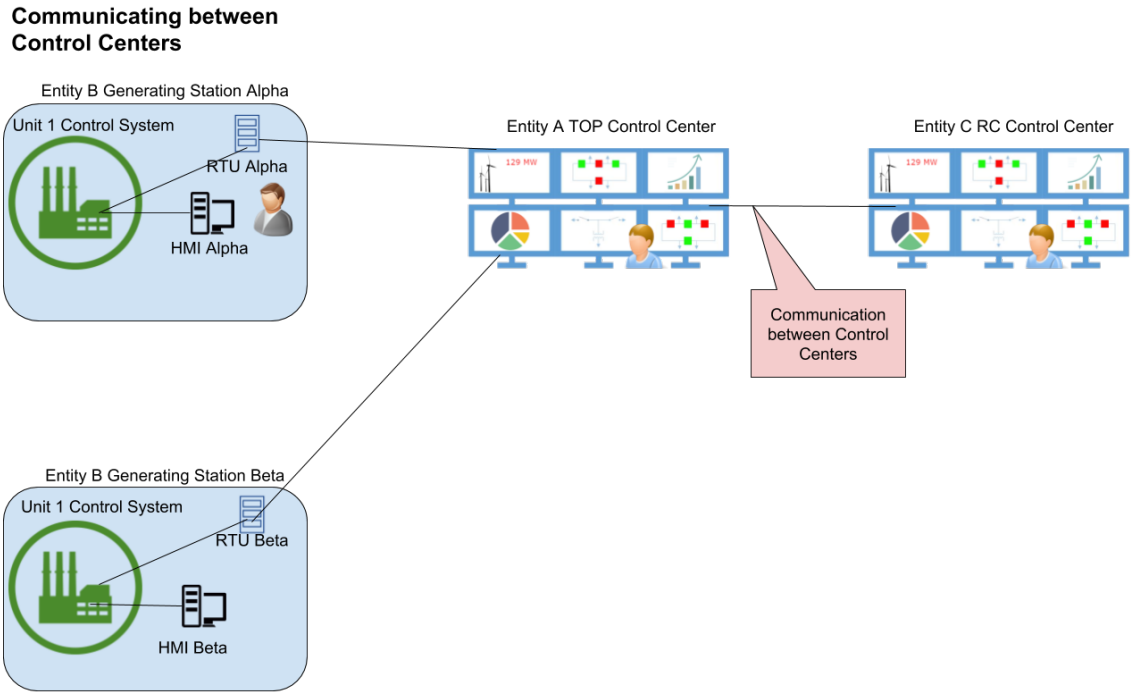


Figure 1

Figure 1 presents a typical scenario with two Control Centers communicating (in this instance Entity C's RC Control Center and Entity A's TOP Control Center). The communication between them is the intended scope of CIP-012's requirements if they meet the types of data inclusions and exclusions within the standard. The TOP Control Center is communicating with an RTU at two of Entity B's generating plants (Stations Alpha and Beta). Those RTU's are gathering information from each generating unit's control system. Each generating unit at each plant has an HMI (Human/Machine Interface; an operator workstation) that the local personnel use to operate their respective units.

Entity B decides that the generating unit at Station Beta, a small peaking facility, will only have an operator on site during the day. The operator at Station Alpha should be able to remotely start the unit at

Station Beta if necessary.

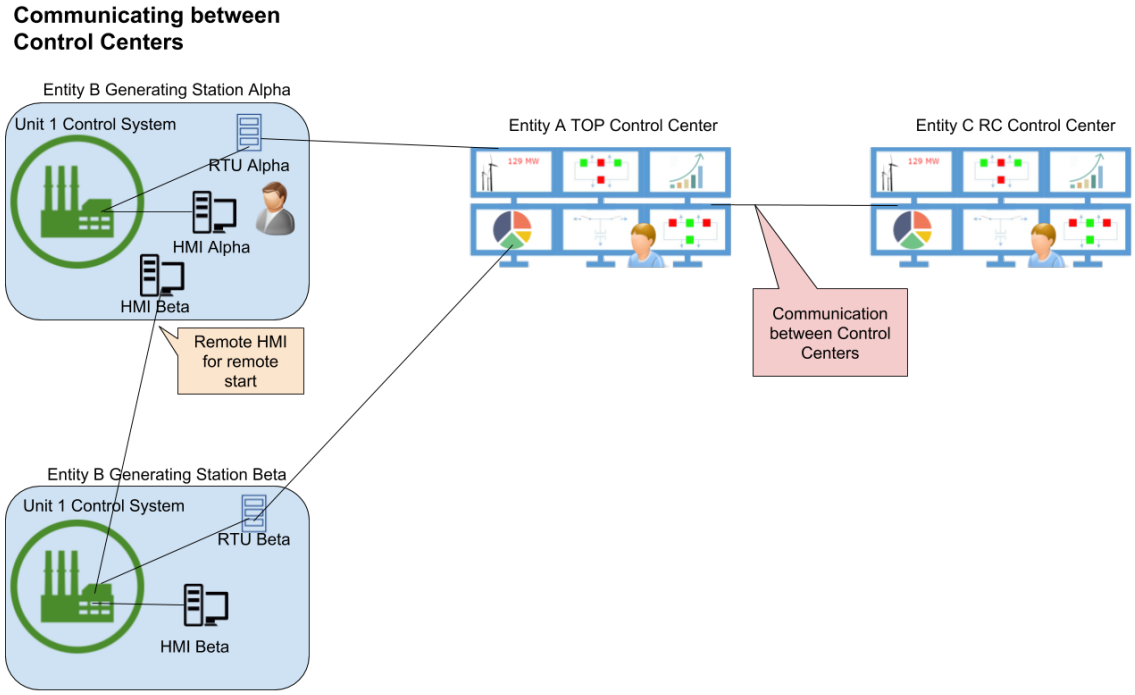


Figure 2

In Figure 2, Entity B installs a dedicated communications circuit from the control system on Station Beta's control system and puts a dedicated HMI at Station Alpha operator use. Station Alpha is now "one or more facilities hosting operating personnel that monitor and control the BES in real time to perform the reliability tasks of…a Generator Operator for generation Facilities at two or more locations" Because stations Alpha and Beta are two different plant locations. Station Alpha can now be dual-classified not only as a generation resource but also as a Control Center.

The communications to the TOP and RC Control Centers in Figure 1 have not changed. No new cyber systems are in place that can impact multiple units. In addition, no cyber systems have been added performing Control Center functions. The only change is that an HMI for Station Beta has been moved within close physical proximity to an HMI for Station Alpha.

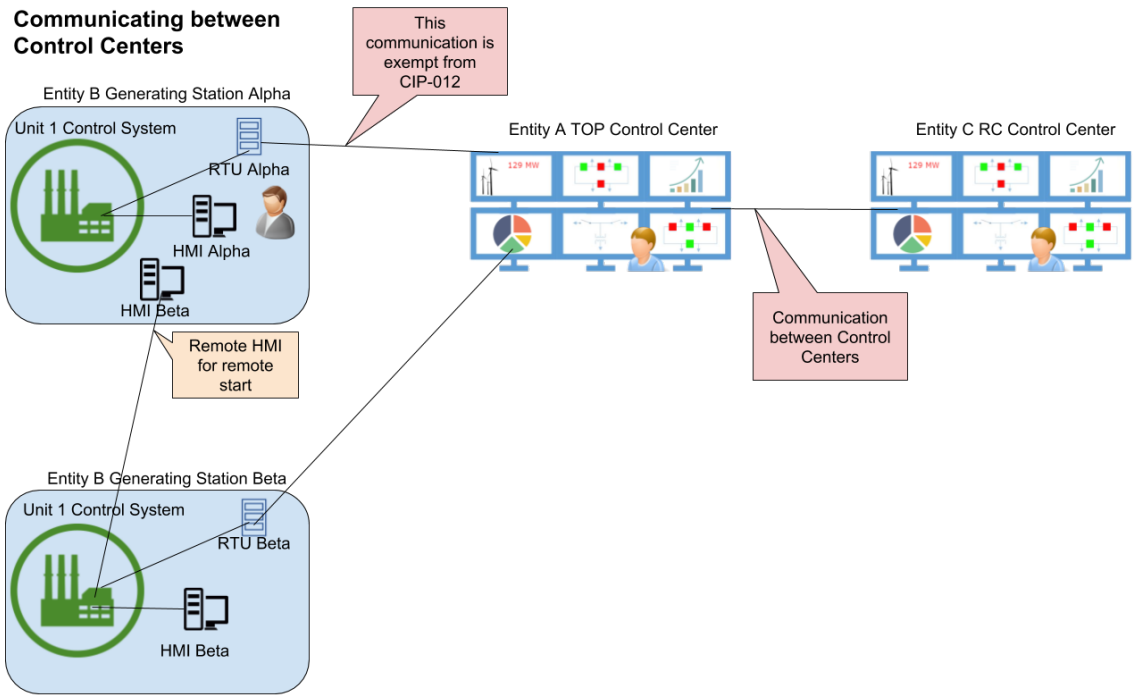


Figure 3

Although nothing has changed between them, this proximity makes the communication noted in Figure 3 between Station Alpha and Entity A's TOP Control Center subject to CIP-012 without the exemption. Two HMIs have been moved into the same room and a new NERC CIP standard applies to two entities.

This is an anomaly of the current Control Center definition of a facility, room, or building from which certain functions can be performed without regard to how they are done or what systems they are using. This is a generation specific example, but the potential situation exists where there are substations with an HMI or protective relay that "operating personnel" within the substation could use to impact an adjacent substation. It is also clear that in the criteria for TO's and GOP's the "two or more locations" is not a precise enough filter for defining what a Control Center truly is. The SDT's attempts to address this issue by clarifying the definition of Control Center pointed out larger issues that are not within the SDT's SAR to address at this time. Accordingly, the SDT is handling the issue through the 4.2.3 exemption within the CIP-012 standard which reads:

4.2.3. A Control Center g that transmits to another Control Center the transmitting Control Center.

The intent of this exemption is to exclude from CIP-012 the normal RTU-style communication from a field asset providing that field asset's status. Throughout this scenario or others like it, that communication has not changed and is still the same data pertaining only to the single location. The SDT recognizes that this communication is not the intent of the standard for protecting communications between Control Centers and this type of communications can be using older legacy communication technology and protocols.

The 4.2.3 exemption covers generation resources or Transmission station or substation locations that host operating personnel and can control BES Facilities at more than one location, possibly making them co-located Control Centers. The communication is exempt if each location is communicating the Real-time Assessment or Real-time monitoring data with another Control Center pertaining only to that location.

The above diagrams were generation specific. The following diagram is a more generic example:

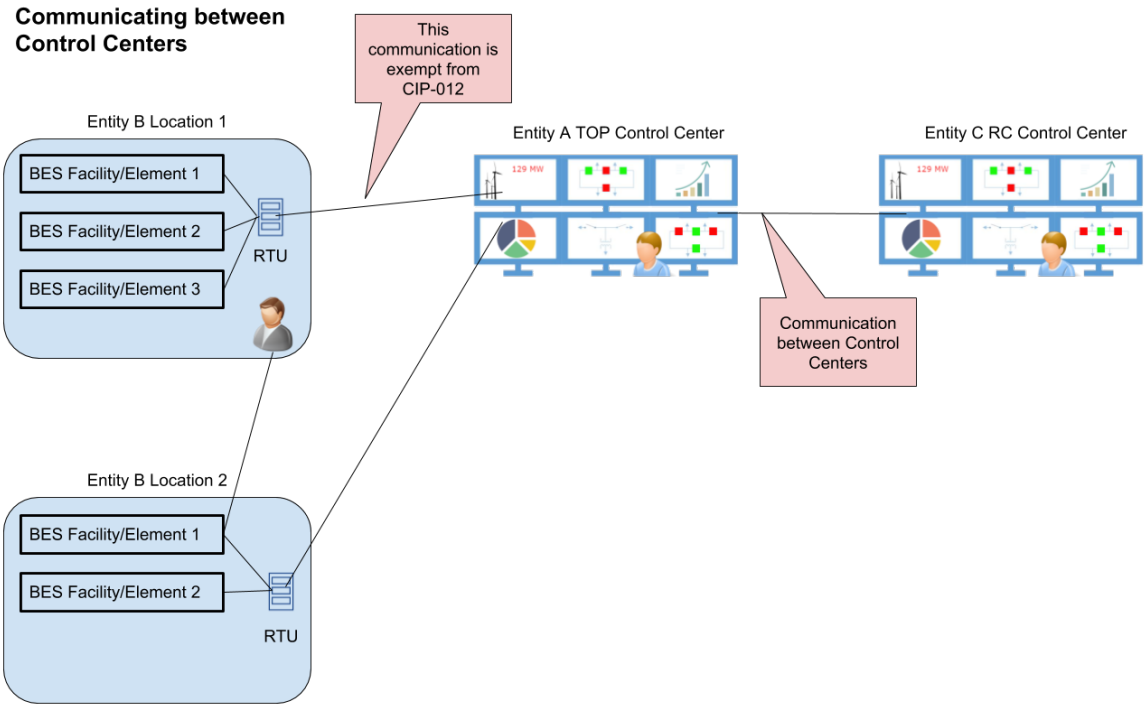


Figure 4

In Figure 4, each location is communicating only the Real-time Assessment or Real-time monitoring data pertaining to that single location. The communication from Entity B location one (1) to Entity A would be exempt from CIP-012-1.

If Location 2 communicates its data through Location 1,and Location 1 was both controlling and aggregating data from multiple locations to Entity A's TOP Control Center, the communication between Location 1 and Entity A's TOP Control Center would not be exempt from CIP-012.

Requirement R1

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 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.*

General Considerations for Requirement R1

Requirement R1 focuses on implementing a documented plan to protect information that is critical to the Real-time operations of the Bulk Electric System while in transit between applicable Control Centers. The SDT does not intend for the listed order of the three requirement parts to convey any sequence or significance.

Overview of confidentiality and integrity

The SDT drafted CIP-012-1 to address confidentiality and integrity of Real-time Assessment and Real-time monitoring data. This is accomplished by drafting the requirement to mitigate the risks posed by unauthorized disclosure (confidentiality) and unauthorized modification (integrity). For this Standard, the SDT relied on the definitions of confidentiality and integrity as defined by National Institute of Standards and Technology (NIST):

- Confidentiality is defined as, "Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information."[2]
- Integrity is defined as, "Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity."[3]

The SDT asserts that the availability of this data is already required by the performance obligation of the Operating and Planning Reliability Standards. The SDT drafted CIP-012-1 to address the data while being transmitted. The SDT maintains that this data resides within BES Cyber Systems, and while at rest is protected by CIP-003-6 through CIP-011-2.

Alignment with IRO and TOP standards

The SDT recognized the FERC reference to additional Reliability Standards and the responsibilities to protect the applicable data in accordance with NERC Reliability Standards TOP-003 and IRO-010. The SDT used these references to drive the identification of sensitive BES data and chose to base the CIP-012-1 requirements on the Real-time data

[2] NIST Special Publication 800-53A, Revision 4, page B-3
[3] NIST Special Publication 800-53A, Revision 4, page B-6

specification elements in these standards. This approach provides consistent scoping of identified data, and does not require each entity to devise its own list or inventory of this data. Many entities are required to provide this data under agreements executed with their RC, BA or TOP. Data requiring protection in CIP-012-1 consists of a subset of data that is identified by the RC, BA, and TOP in the TOP-003 and IRO-010 data specification standards, limited to Real-time Assessment data and Real-time monitoring data. CIP-012-1 excludes other data typically transferred between Control Centers such as Operational Planning Analysis data, weather data, market data, and other data that is not used by the RC, BA, and TOP to perform Real-time reliability assessments and analysis identified in TOP-003 and IRO-010. The SDT determined that Operational Planning Analysis data, if rendered unavailable, degraded, or misused, would not adversely impact the reliable operation of the BES within 15 minutes of the activation or exercise of the compromise as detailed in CIP-002- 5.1a. The SDT notes that there may be special instances during which Real-time Assessment or Real-time monitoring data is not identified by the RC, BA, or TOP. This would include data that may be exchanged between a Responsible Entity's primary and backup Control Center.

Identification of Where Security Protection is Applied by the Responsible Entity

The SDT noted the need for a Responsible Entity to identify where it will apply protection for applicable data. The SDT did not specify the location where CIP-012-1 security protection must be applied. This allows latitude for Responsible Entities to implement the security controls in a manner best fitting their individual circumstances. This latitude ensures entities can still take advantage of security measures, such as deep packet inspection implemented at or near the EAP when ESPs are present, while maintaining the capability to protect the applicable data being transmitted between Control Centers.

The SDT also recognizes that CIP-012 security protection may be applied to a Cyber Asset that is not an identified BES Cyber Asset, Protected Cyber Asset, or EACMS. The identification of the Cyber Asset as the location where security protection is applied does not expand the scope of Cyber Assets identified as applicable under Cyber Security Standards CIP-002 through CIP-011.

The SDT understands that in data exchanges between Control Centers, a single entity may not be responsible for both ends of the communication link. The SDT intends for a Responsible Entity to identify only where it applied security protection. The Responsible Entity should not be held accountable for identifying where a neighboring entity applied security protection at the neighboring entity's facility. A Responsible Entity, however, may decide to take responsibility for both ends of a communication link. For example, it may place a router in a neighboring entity's data center. In a scenario where a Responsible Entity has taken responsibility for applying security protection on both ends of the communication link, the Responsible Entity should identify where it applied security protection at both ends of the link. The SDT intends for there to be alignment between the identification of where security protection is applied in CIP-012-1 Requirement R1, Part 1.2 and the identification of Responsible Entity responsibilities in CIP-012-1 Requirement R1, Part 1.3.

Control Center Ownership

The standard requirements address protection for Real-time Assessment and Real-time monitoring data while being transmitted between Control Centers owned by a single Responsible Entity. They also cover the applicable data transmitted between Control Centers owned by two or more separate Responsible Entities. Unlike protection between a single Responsible Entity's Control Centers, applying protection between Control Centers owned by more than one Responsible Entity requires additional coordination. The requirements do not explicitly require formal agreements between Responsible Entities partnering for protection of applicable data. It is strongly recommended, however, that these partnering entities develop agreements, or use existing ones, to define responsibilities to ensure the security objective is met. An example noted in FERC Order No. 822 Paragraph 59 is, "if several registered entities have joint responsibility for a cryptographic key management system used between their respective Control Centers, they should have the prerogative to come to a consensus on which organization administers that particular key management system."

As an example, Figure 5 shows several data transmissions between Control Centers that a Responsible Entity should consider to be in-scope. The example does not include all possible scenarios. The solid green lines are in-scope communications and the dashed red lines are out-of-scope communications.

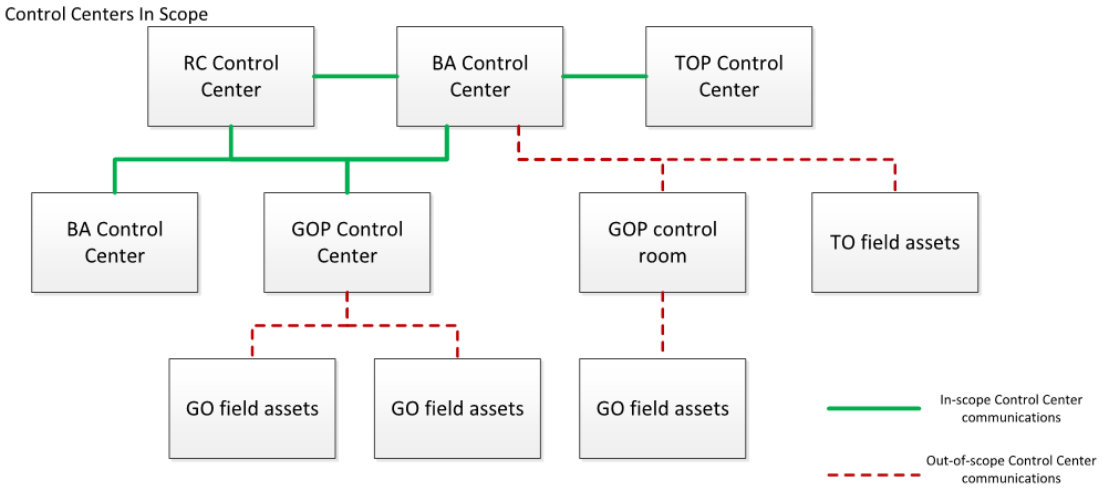


Figure 5: This reference model is an example and does not include all possible scenarios.

The SDT included Part 1.3 of the plan to address the situation when multiple registered entities are involved with protecting the data transmitted between Control Centers. Part 1.3 provides a mechanism to specify which entity is responsible for the application of security controls. The SDT included this requirement part to address security concerns as well as audit concerns. Where data is transmitted between different entities, the SDT asserts that it is necessary for both entities to understand the responsibilities of applying security controls to ensure the data is protected through its entire transmission and there is no security gap. The SDT also asserts this requirement part will provide evidence which may prevent the simultaneous auditing of multiple entities for each communication link between Control Centers when operated by different Responsible Entities. Security controls applied by the entity to achieve compliance with Parts 1.1 and 1.2 of the plan should correlate to the documented responsibilities in Part 1.3 of the entity's plan.

References

Here are several references to assist entities in developing plan(s) for protection of communication links:

- NIST Special Publication 800-53A, Revision 4: Security and Privacy Controls for Federal Information Systems and Organizations
- NIST Special Publication 800-82: Guide to Industrial Control Systems (ICS) Security
- NIST Special Publication 800-175B: Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms
- NIST Special Publication 800-47: Security Guide for Interconnecting Information Technology Systems

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

ERO Enterprise Endorsed

Cyber Security – Communications Between Control Centers

Implementation Guidance for CIP-012-1

RELIABILITY | RESILIENCE | SECURITY




3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Introduction

The Project 2016-02 SDT drafted this Implementation Guidance to provide example approaches for compliance with CIP-012-1. Implementation Guidance does not prescribe the only approach, but highlights one or more approaches that would be effective in achieving compliance with the standard. Because Implementation Guidance only provides examples, entities may choose alternative approaches that better fit their individual situations[1].

Responsible Entities may find it useful to consider this Implementation Guidance document along with the additional context and background provided in the SDT-developed Technical Rationale and Justification for CIP-012-1 document.

Background

The Commission issued Order No. 822 on January 21, 2016 approving seven CIP Reliability Standards and new or modified definitions, and directed modifications be made to the CIP Reliability Standards. Among other items, the Commission directed NERC to "develop modifications to the CIP Reliability Standards to require responsible entities to implement controls to protect, at a minimum, communication links and sensitive bulk electric system data communicated between bulk electric system Control Centers in a manner that is appropriately tailored to address the risks posed to the bulk electric system by the assets being protected (i.e., high, medium, or low impact)." (Order 822, Paragraph 53)

In response to the directive in Order No. 822, the Project 2016-02 standard drafting team (SDT) drafted Reliability Standard CIP-012-1 to require Responsible Entities to implement 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. Due to the sensitivity of the data being communicated between Control Centers, the standard applies to all impact levels (i.e., high, medium, or low impact).

The SDT drafted requirements to provide Responsible Entities the latitude to protect the Real-time Assessment and Real-time monitoring data itself, the communication links such data traverses, or a combination of both to satisfy the security objective consistent with the capabilities of the Responsible Entity's operational environment.

[1] NERC's Compliance Guidance Policy

Requirements

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.

General Considerations

Plan Development

As noted in the Technical Rationale and Justification for CIP-012-1, the focus of Requirement R1 is implementing a documented plan to protect information that is critical to the real-time operations of the Bulk Electric System while in transit between applicable Control Centers. The number of plan(s) and their content may vary depending on a Responsible Entity's management structure and operating conditions. The Responsible Entity may document as many plans as necessary to meet its needs. For instance, a Responsible Entity may choose to document one plan per Control Center or choose an all-inclusive, single plan for its Control Center communication environment. A Responsible Entity may choose to document one plan for communications between Control Centers it owns and a separate plan for communications between its Control Centers and the Control Centers of a neighboring Entity. The number and structure of the plans is at the discretion of the Responsible Entity as long as the plan(s) include the required elements described in Parts 1.1, 1.2, and 1.3 of Requirement R1.

Responsible Entities should note that "associated data centers" are included in the Control Center definition.

Identification of Real-time Assessment and Real-time monitoring data

Responsible Entities can expect to receive or have received requests for Operations Planning Analysis, Real-time Assessment and Real-time monitoring data from their RC(s), BA(s) and TOP(s). These data requests, pursuant to the data specification from TOP-003 and IRO-010 requirements, may also include other types of data under the same request. CIP-012 requires protection only for Real-time Assessment and Real-time monitoring data. If the provided data specification does not indicate which data is Real-time Assessment and Real-time monitoring data, Responsible Entities could choose to conduct an assessment to identify this data from among the other data requested or being communicated. Once a data assessment is completed, the Responsible Entity should confirm its findings with the other communicating entity before applying security controls. If the Real-time Assessment and Real-time monitoring data is not clearly identified in the provided data specification, the Responsible Entity should document the methodology used and all actions taken to identify the Real-time Assessment and Real-time monitoring data.

Identification of Security Protection (R1.1)

Entities have latitude to identify and choose which security protection is 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.

This security protection could consist of logical protection, physical protection, or some combination of both. To determine security protection, the requirement specifies that it must mitigate the risks posed by unauthorized disclosure and unauthorized modification of applicable data. Physical protection is usually appropriate if two Control Centers are in close physical proximity such that the cabling and connections over which the data travels between them is physically protected between the two. Physical protection may also be appropriate when the equipment that is performing encryption is close to but still outside a Control Center and physical protection is used to protect the cabling and connections between the encryption endpoint and the Control Center itself.

Security protection implementation can be demonstrated in many ways. If a Responsible Entity uses physical protection, it may demonstrate implementation through review of an applicable Control Center floor plan with details subsequently confirmed through visual inspection, which identifies the physical security measures in place protecting the communication link. If the Responsible Entity uses logical protection, it may demonstrate implementation through an export of the device configuration which applies the security protection. Some examples include:

- An export of the configuration of a firewall showing the configuration of a VPN tunnel and the routing that directs applicable data through the VPN

- An export of the configuration of a transport level device that demonstrates encryption is enabled for applicable (or all) data
- Configuration of an application that demonstrates that the applicable data is encrypted from the application to the remote client or application

Where the operational obligations of an entire communication link, including both endpoints, belong to the Control Center of another Responsible Entity, the Responsible Entity without operational obligations for the communication link may demonstrate compliance by ensuring the communications link endpoint is within its Control Center, which could be limited to including the communication link endpoint within a PSP or where other physical protection is applied.

Identification of Where Security Protection is Applied by the Responsible Entity (R1.2)

A Responsible Entity should consider its environment when identifying where security protections should be applied. One approach is to implement security within the Control Center itself to ensure that data confidentiality and integrity is protected throughout the transmission. The Responsible Entity can identify where security protection is applied using a logical or physical location. The application of security in accordance with CIP-012 requirements does not add additional assets to the scope of the CIP Reliability Standards. Locations of applied security protection may vary based on many factors such as impact levels of the Control Center, different technologies, or infrastructures. Where the operational obligations of an entire communication link, including both endpoints, belong to the Control Center of another Responsible Entity, the Responsible Entity without operational obligations for the communication link may demonstrate compliance by ensuring the communications link endpoint is within its Control Center, which could be limited to including the communication link endpoint within a PSP or where other physical protection is applied.

Identification of where a Responsible Entity applies security protection could be demonstrated with a list or a Control Center diagram showing either physical or logical security controls. Physical diagrams may require visual confirmation of these controls. These diagrams or a list could be included within the plan developed for R1. A Responsible Entity could also use labels to identify on-site devices where CIP-012 security protection is applied.

When exchanging data between two entities, if a Responsible Entity only manages one end of a communication link, the Responsible Entity is not responsible for identifying where the security protection is applied by the neighboring entity with which it is exchanging data. However, if a Responsible Entity has taken responsibility for both ends of the communication link (such as by placing a router within the neighboring entity's data center), then the Responsible Entity shall identify where the security protection is applied at both ends of the link.

Similarly, if a Responsible Entity owns and operates both Control Centers which are exchanging data (such as in the case of a primary and backup Control Center), then the Responsible Entity shall identify where security protection is applied at both ends of the link.

Identification of Responsibilities when the Control Centers are Owned or Operated by Different Responsible Entities (R1.3)

The Technical Rationale and Justification for CIP-012-1 identifies key considerations in the Control Center Ownership section when communications between Control Centers with different owners or operators. Many operational relationships between Responsible Entities are unique. Consequently, there is no single way to identify responsibilities for applying security protection to the transmission of Real-time Assessment and Real-time monitoring data between Control Centers.

Implementation of responsibilities could also be demonstrated in many ways. Some examples include a joint procedure, a memorandum of understanding, or meeting minutes, documenting the defined responsibilities between the two parties.

Where the operational obligations of an entire communication link, including both endpoints, belong to the Control Center of another Responsible Entity, the Responsible Entity without operational obligations for the communication link may demonstrate compliance by ensuring the communications link endpoint is within its Control Center, which could be limited to including the communication link endpoint within a PSP or where other physical protection is applied.

Reference Model

For this Implementation Guidance, the SDT uses a basic reference model of Primary and Backup Control Centers (Entity Alpha) to illustrate approaches to demonstrating compliance. These Control Centers communicate to each other and to a neighboring entity's Control Center (Entity Beta) in configurations outlined by the diagrams in this section. The SDT recognizes that the reference model does not contain many of the complexities of a real Control Center. For this Implementation Guidance, the registration or functions performed in the reference model Control Center are also not considered. A high-level block diagram of the basic reference model is shown below in Figure 1. This Implementation Guidance is developed from the perspective of Entity Alpha.

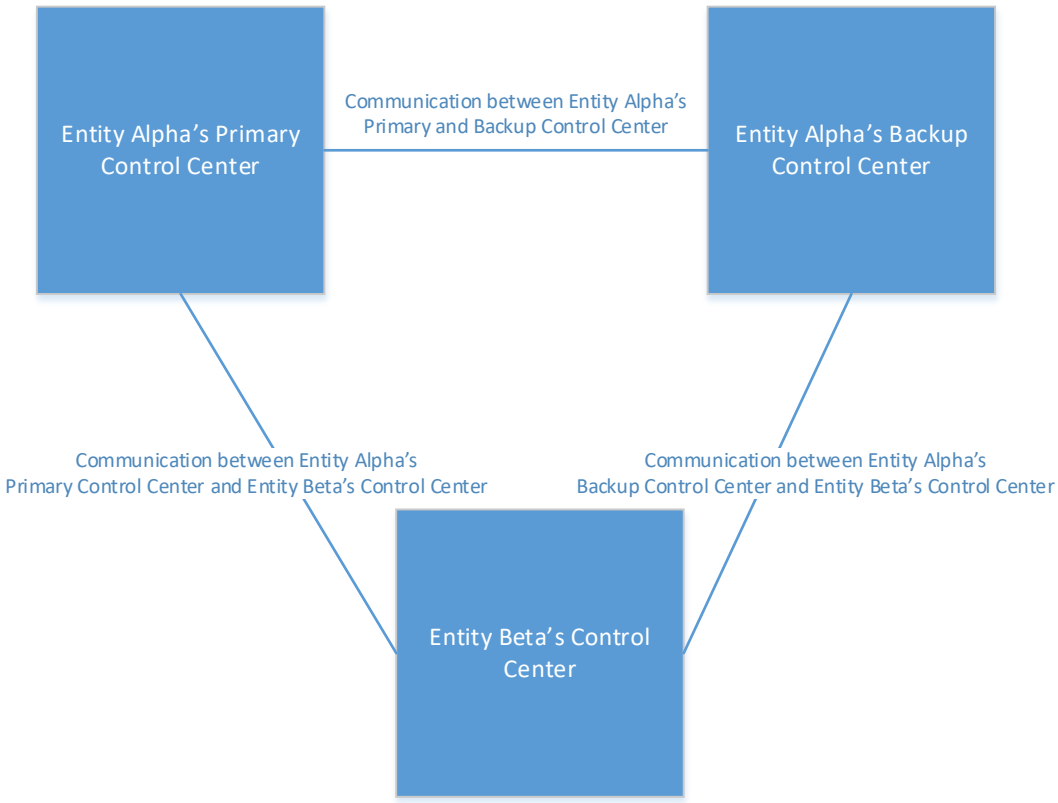


Figure 1: High Level Block Diagram of Reference Model Control Centers

Reference Model Discussion

Requirement R1 requires the implementation of a documented plan. To comply with requirement R1, one approach to a plan is to first determine which communications are in scope of CIP-012-1. There are multiple ways to identify an entity's scope in R1. For example, Entity Alpha in the reference model may first identify the Control Centers with which it communicates. Entity Alpha would determine that there are three: Entity Alpha's Primary Control Center, Entity Alpha's Backup Control Center, and Entity Beta's Control Center. Entity Alpha does not need to consider whether Entity Beta further shares its data with another Entity. That is the responsibility of Entity Beta and is outside of Entity Alpha's purview. Additionally, Entity Alpha does not need to consider any communications to other non-Control Center facilities such as generating plants or substations. These communications are out of scope for CIP-012-1.

Now that Entity Alpha has identified the Control Centers with which it communicates, Entity Alpha identifies either: (1) the Real-time Assessment and Real-time monitoring data; or (2) communication links which are used to transmit Real-time Assessment and Real-time monitoring data between Control Centers. In either case, Entity Alpha could

refer to the data specification for Real-time Assessment and Real-time monitoring data identified in TOP-003-3 and IRO-010-2. For this reference model scenario, identifying the communication links used to transmit Real-time Assessment and Real-time monitoring data may be the most straightforward approach. Through an evaluation of communication links between Control Centers and an evaluation of how it transmits and receives Real-time Assessment and Real-time monitoring data, Entity Alpha determined that it communicates applicable data between its primary and backup Control Centers across a single communication link. Entity Alpha also determined that it communicates applicable data to and from Entity Beta's Control Center across one of two links that originate from either Entity Alpha's primary or backup Control Center using the Inter-Control Center Communications Protocol (ICCP).

With an identified scope of communications links the applicable data traverses, Entity Alpha now considers the three required elements of its required communications between Control Centers for its plan.

Identification of Security Protection

Entity Alpha must ensure that protection is applied where identified in its CIP-012-1 plan. The protection must also meet the security objective of mitigating the risks posed by unauthorized disclosure and unauthorized modification of applicable data while in transit between Control Centers. The identification of security protection could be demonstrated by a network diagram similar to that shown in Figure 2 or Figure 3 that identifies one or more communication segments between Control Centers and the security protection implemented per segment.

In a simple case where the security protection is applied at a point within the Control Center, such as within the Physical Security Perimeter of the Control Center, Entity Alpha may use a single security protection method to meet the security objective. For this case, shown in Figure 2, Entity Alpha implements a Virtual Private Network (VPN) connection across a communication circuit for each of its three in-scope communication links. To meet the security objective, Entity Alpha documents that its VPN uses Internet Protocol security (IPsec) with encryption.

For more complex scenarios, Entity Alpha may need to use a combination of security controls. For instance, in Figure 3, Entity Alpha uses a combination of physical security controls (physical access control) and logical security controls (encrypted communications consistent with the first scenario above) to meet the security objective. In Figure 3, the encryption endpoint is located on transport equipment (WAN router) located outside the Control Center. Entity Alpha then physically protects the cabling and connections over which the data travels until it is within the Control Center. The SDT notes that the same technical architecture could exist where the responsibilities of the registered entities are different. Therefore as shown in Figure 2 & 3, in the scenario where entity Alpha owns and operationally manages the communication link and endpoint equipment, Entity Beta is responsible for ensuring the communication endpoint of the communication link is within a Control Center. Entity Beta ensures Entity Alpha's communication link endpoint equipment is within a Control Center by including the communication endpoint within a Control Center PSP. The physical controls for the PSP are described in CIP-006 documentation and do not need to be repeated for this requirement. This satisfies Entity Beta's obligation for Part 1.1 and 1.2.

While these scenarios are all specific to communication links, it is possible that Entity Alpha and Entity Beta achieve the security objective by applying protection to the data rather than the communication links. In this scenario, the application enabling the data exchange between Control Centers may be capable of applying security controls directly to the data. These security controls mitigate the risks posed by unauthorized disclosure and unauthorized modification of applicable data rather than relying on lower level network services to provide this security. For instance, Entity Alpha and Entity Beta may apply security protection at the application layer by using SSL/TLS or other application layer encryption methods to exchange applicable data.

Identification of Where Security Protection is Applied by the Responsible Entity

Similar to the identification of security protection above, the identification of where security protection is applied can also be demonstrated by a network diagram similar to those found in Figures 2 and 3.

- Figure 2 shows the identification where CIP-012-1 security protection is applied for the Entity Alpha reference model when a single encrypted tunnel is used to implement the required protection. Entity Alpha has identified that security protection is applied at each of its Control Centers on the external Ethernet interface on the WAN router. While the diagram depicts where Entity Beta has applied security protection for illustrative purposes, Entity Alpha is not responsible for identifying where Entity Beta has applied security protection.
- In order to understand the application of security protection in context of who controls the communication link, it may be helpful to identify both where CIP-012-1 security protection is applied and the location of the telecommunications carrier (telco) demarcation point. Figure 3 provides such an example where the telco demarcation point may not be within the Control Center and based the facts and circumstances surrounding this scenario, Entity Alpha has implemented a combination of security controls to comply with CIP-012-1. In this scenario, Entity Alpha identifies that it has applied physical security protection for its PSP and continuing for its WAN router and that it has applied logical security protection (encryption) at the WAN router. Entity Alpha has also identified the telco demarcation point at a point in the telecommunications cabling connecting to Entity Alpha's WAN router, perhaps at a punch down block for example. In Figure 3, the telco demarcation point is inside the same room as the WAN router. The telco demarcation points are referenced in the drawing for clarity, but are not part of the plan.
- Figures 2 & 3 provide an example of where the operational obligations of an entire communications link, including both endpoints, belong to Entity Alpha. In this case, Entity Beta may be responsible for ensuring the communications endpoint of the communications link is within their Control Center. Entity Beta ensures Entity Alpha's communication link endpoint equipment is within a Control Center by including the communication endpoint within a Control Center PSP. The documentation provided for Part 1.1 by Entity Beta fulfils this obligation.
- The data-centric scenario described above is less intuitive for identifying where security protection is applied by Entity Alpha. If security protection is applied at the application layer, Entity Alpha could reasonably identify the application or service applying the security as the location of where security protection is applied.

Identification of Responsibilities when the Control Centers are Owned or Operated by Different Responsible Entities

Entity Alpha and Entity Beta may determine they each are responsible for one end of the VPN configuration on their respective WAN routers. Entity Alpha and Entity Beta have agreed to a 30 character pre-shared key for IPSec authentication.

Rather than use a pre-shared key, Entity Alpha and Entity Beta may decide to use digital certificates for the IPSec authentication using a trusted certificate authority. In that scenario, Entity Alpha and Entity Beta would agree on who is the party responsible for managing the certificate authority.

In the example where the communication link and endpoint equipment are owned by Entity Alpha, both entities should include ownership responsibilities in their plans satisfying requirement 1.3. Examples include but are not limited to, a letter indicating ownership or responsibility, a copy of a contract indicating ownership or responsibilities, an excerpt from an operational agreement or manual indicating ownership or responsibility.

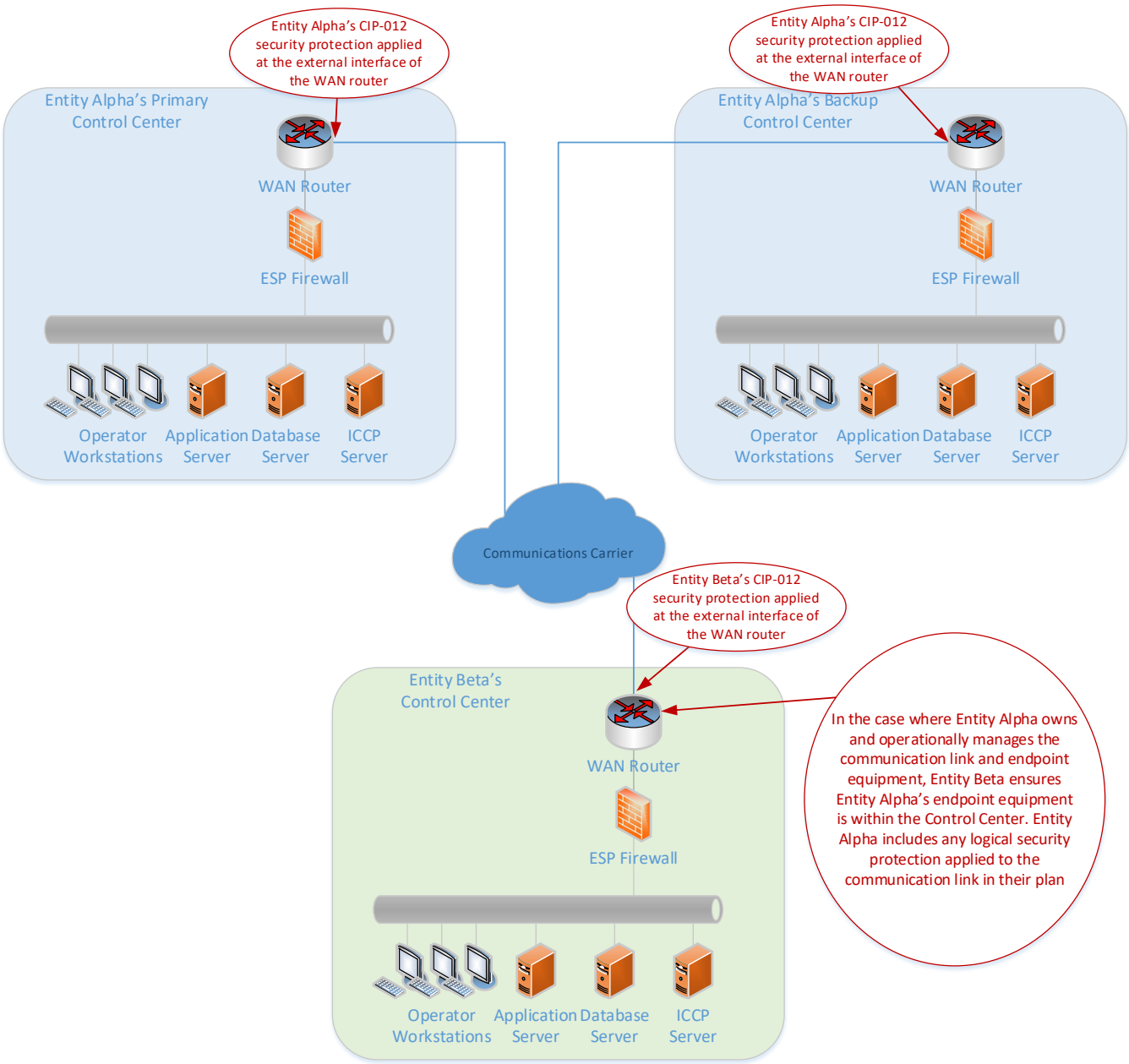


Figure 2: Network diagram and identification of where security protection is applied

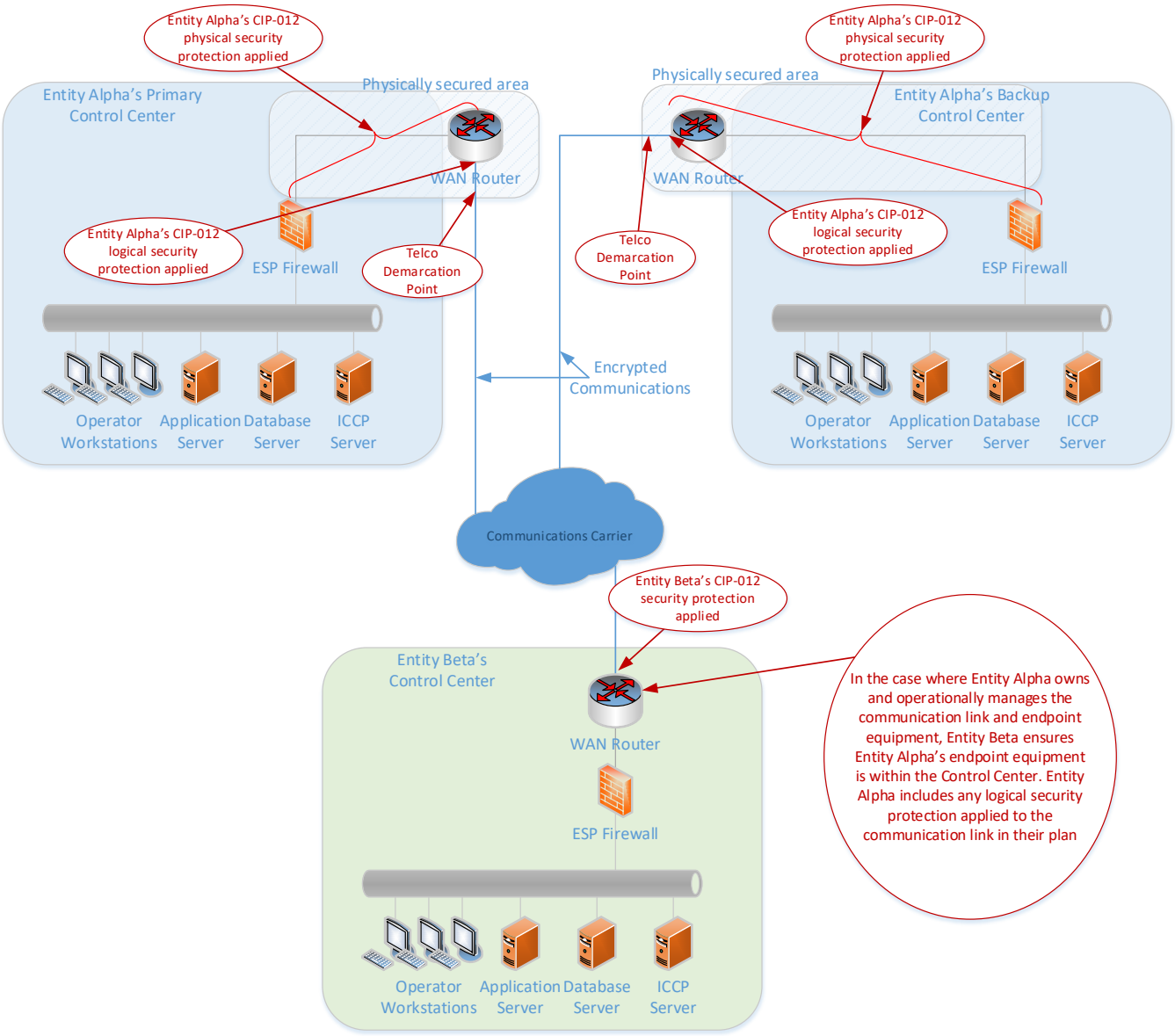


Figure 3: Network diagram using a combination of controls for CIP-012-1

References

Mitre Common Weakness Enumeration (CWE™) list of software weakness types
https://cwe.mitre.org/data/definitions/327.html

Cryptographic Standards and Guidelines
https://csrc.nist.gov/Projects/Cryptographic-Standards-and-Guidelines

NIST Special Publication 800-175B
Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-175B.pdf

Guide to Cryptography
https://www.owasp.org/index.php/Guide_to_Cryptography#Symmetric_Cryptography