Informations relatives aux normes

Projet QC-2021-08

Normes *CIP-005-7 – Cybersécurité – Périmètres de sécurité électronique, CIP-010-4 – Cybersécurité – Gestion des changements de configuration et analyses de vulnérabilité et CIP-013-2 – Cybersécurité – Gestion des risques dans la chaîne d'approvisionnement*

1.1. Applicabilité des normes

Les fonctions visées par les normes proposées pour adoption, soit les normes de fiabilité CIP-005-7, CIP-010-4 et CIP-013-2, sont indiquées dans le tableau ci-dessous.

Norme	Fonctions visées
CIP-005-7	• *Exploitant d'installation de production (GOP)* • *Propriétaire d'installation de production (GO)* • *Responsable de l'équilibrage (BA)* • *Coordonnateur de la fiabilité (RC)* • *Exploitant de réseau de transport (TOP)* • *Propriétaire d'installation de transport (TO)* • *Certains distributeurs (DP)*
CIP-010-4	
CIP-013-2	

L'équipe de rédaction de la *North American Electric Reliability Corporation* (ci-après, la « NERC ») a supprimé la fonction de « *coordonnateur des échanges ou responsable des échanges* » pour les normes CIP-005-7 et CIP-010-4[1], c'est pourquoi les trois (3) normes ci-dessus ont désormais les mêmes fonctions visées.

1.2. Objet des normes

La présente section a pour objectif de présenter l'objet des normes visées par la présente demande. Plus spécifiquement, les prochains points présentent le titre puis l'objet de chacune des normes.

- **CIP-005-7 – Cybersécurité – Périmètres de sécurité électronique :** Gérer l'accès électronique aux *systèmes électroniques BES* en établissant un *périmètre de sécurité électronique (ESP)* contrôlé afin de protéger les *systèmes électroniques BES* contre les compromissions qui pourraient entraîner un fonctionnement incorrect ou une instabilité dans le *BES*.
- **CIP-010-4 – Cybersécurité - Gestions des changements de configurations et analyses de vulnérabilité :** Prévenir et détecter les changements non autorisés aux *systèmes électroniques BES* au moyen d'exigences relatives à la gestion des changements de configuration et aux analyses de vulnérabilité, afin de protéger les *systèmes électroniques BES* contre les compromissions qui

[1] Justification technique de la norme de fiabilité CIP-005-7 de la NERC (p.4/17), consultée le 29 juin 2021 au https://www.nerc.com/pa/Stand/Project201903_Cyber%20Security%20Supply%20Chain%20Risks/2019-03_CIP-005-7_Technical_Rationale_clean_10072020.pdf

pourraient entraîner un fonctionnement incorrect ou des instabilités dans le *système de production-transport d'électricité* (*BES*).

- **CIP-013-2 – Gestion des risques de la chaîne d'approvisionnement :** Atténuer les risques de cybersécurité susceptibles de menacer la fiabilité du *système de production-transport d'électricité* (*BES*) en établissant des contrôles de sécurité axés sur la gestion des risques dans la chaîne d'approvisionnement des *systèmes électroniques BES*.

1.3. Contexte réglementaire

Les trois (3) normes de fiabilité remplacent respectivement les normes CIP-005-6, CIP-010-3 et CIP-013-1 adoptées par la Régie de l'énergie (ci-après, la « Régie ») dans la décision D-2020-118[2]. Les normes CIP-005-6, CIP-010-3 et CIP-013-1 entreront en vigueur au Québec le 1er octobre 2022.

Adoptées par le conseil d'administration de la NERC le 5 novembre 2020 et approuvées par la *Federal Energy Regulatory Commission* (ci-après, la « FERC ») le 18 mars 2021 dans la lettre d'ordonnance RD21-2-000[3], les normes de fiabilité CIP-005-7, CIP-010-4 et CIP-013-2 entreront en vigueur aux États-Unis le 1er octobre 2022[4].

Le Coordonnateur de la fiabilité (ci-après appelé le « Coordonnateur ») dépose au présent dossier les normes CIP-005-7, CIP-010-4 et CIP-013-2 du projet 2019-03[5] (*Supply Chain Risk management*) de la NERC. Il s'agit du seul dépôt prévu dans le cadre de ce projet. Les trois (3) normes de fiabilité ont pour objectif de répondre aux directives émises dans l'Ordonnance 850[6] de la FERC afin de modifier les normes de fiabilité entourant la gestion des risques de cybersécurité liés aux chaînes d'approvisionnement des *systèmes électroniques BES*. La FERC a demandé à la NERC de soumettre des modifications pour traiter des *systèmes de contrôle ou de surveillance des accès électroniques (EACMS)*, plus spécifiquement ceux qui assurent le contrôle ou la surveillance des accès électroniques à des *systèmes électroniques BES* à impact élevé ou moyen. La NERC recommandait dans son rapport du 17 mai 2019[7] de modifier les normes de fiabilité entourant la gestion des risques de cybersécurité liés aux chaînes d'approvisionnement afin d'étendre leur portée aux *systèmes de contrôle des accès physiques (PACS)* qui assurent le contrôle des accès physiques à des *systèmes électroniques BES* à impact élevé ou moyen[8]. En d'autres termes, le projet 2019-03[9] a pour objectif de rehausser la portée des normes de fiabilité CIP-005-7, CIP-010-4 et CIP-013-2 en incluant les *EACMS* et les *PACS*.

---

[2] Décision D-2020-118 de la Régie, dossier R-4117-2020, consultée le 29 juin 2021 au http://publicsde.regie-energie.qc.ca/projets/536/DocPrj/R-4117-2020-A-0011-Dec-Dec-2020_09_10.pdf

[3] Lettre d'ordonnance RD21-2-000 de la FERC, consultée le 26 juillet 2021 au https://elibrary.ferc.gov/eLibrary/filelist?accession_num=20210318-3030 (en anglais seulement).

[4] Normes sujettes à une entrée en vigueur future sur le site de la NERC, consultée le 16 juin 2021 au https://www.nerc.net/standardsreports/standardssummary.aspx (en anglais seulement).

[5] Projet 2019-03 de la NERC, consulté le 29 juin 2021 au https://www.nerc.com/pa/Stand/Pages/Project2019-03CyberSecuritySupplyChainRisks.aspx (en anglais seulement)

[6] Ordonnance 850 de la FERC, consultée le 29 juin 2021 au https://www.nerc.com/FilingsOrders/us/FERCOrdersRules/Order%20No.%20850%20Supply%20Chain%20Risk%20Management%20Reliability%20Standards.pdf

[7] Rapport de la NERC, *Cyber Security Supply Chain Risks, Staff Report and Recommended Actions*, consulté le 29 juin 2021 au https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf (en anglais seulement)

[8] Demande d'autorisation des normes « Standard Authorization Request», consultée le 29 juin 2021 au https://www.nerc.com/pa/Stand/Project201903_Cyber%20Security%20Supply%20Chain%20Risks/SAR%20Supply%20Chain_July2019.pdf

[9] Projet 2019-03 de la NERC, consulté le 29 juin 2021 au https://www.nerc.com/pa/Stand/Pages/Project2019-03CyberSecuritySupplyChainRisks.aspx (en anglais seulement)

1.4. Disposition particulière pour le Québec

Le Coordonnateur propose de reconduire les spécificités québécoises, notamment le champ d'application et les dispositions particulières aux versions précédentes des normes de fiabilité, soit les normes CIP-005-6, CIP-010-3 et CIP-013-1 déjà adoptées par la Régie dans sa décision D-2020-118, qui exemptent certaines centrales et leur poste élévateur.

La première disposition particulière concerne le champ d'application de la norme :

> « La présente norme s'applique seulement aux installations du *réseau de transport principal* (RTP) et aux installations spécifiées pour le *distributeur*. Dans l'application de cette norme, toute référence aux termes « *système de production-transport d'électricité* » ou « BES » doit être remplacée par les termes « *réseau de transport principal* » ou « RTP » respectivement. »

Le Coordonnateur est d'avis que cette disposition particulière est toujours applicable, puisque le champ d'application établi par la Régie pour la majorité des normes de fiabilité au Québec est le RTP.

Le Coordonnateur propose de reconduire les exemptions additionnelles suivantes :

> « Sont exemptés de l'application de la présente norme :
>
> - Toute installation de production qui répond aux deux conditions suivantes : (1) la puissance nominale de l'installation est de 300 MVA ou moins et (2) aucun groupe de l'installation ne peut être synchronisé avec un réseau voisin.
> - Postes élévateurs des installations de production identifiées au point précédent. »

Le Coordonnateur est d'avis que la disposition particulière concernant les exemptions additionnelles est toujours applicable dans les nouvelles versions des normes CIP-005, CIP-010 et CIP-013, car les critères mentionnés ci-dessus font référence aux installations à impact faible.

1.5. Dates d'entrée en vigueur proposées

Le plan de mise en œuvre du projet 2019-03[10] de la NERC propose une entrée en vigueur des normes de fiabilité CIP-005-7, CIP-010-4 et CIP-013-2 le premier jour du premier trimestre civil à survenir dix-huit (18) mois[11] après l'approbation de l'organisme réglementaire. L'entrée en vigueur aux États-Unis a été fixée au 1er octobre 2022.

Le Coordonnateur considère que les critères établis par la Régie d'avoir une mise en vigueur le premier jour d'un trimestre civil[12] et un délai minimal de soixante (60) jours[13] entre la date d'adoption et l'entrée en vigueur d'une norme sont respectés dans le cadre du plan de mise en œuvre de la NERC.

Étant donné l'importance d'avoir des pratiques uniformes avec des normes obligatoires en vigueur harmonisées avec les États-Unis, le Coordonnateur propose une entrée en vigueur le premier jour du

[10] Plan d'implantation de la NERC du projet 2019-03, consulté le 16 juin 2021 au https://www.nerc.com/pa/Stand/Project201903_Cyber%20Security%20Supply%20Chain%20Risks/2019-03_Implementation_Plan_clean_10072020.pdf (en anglais seulement).

[11] Plan d'implantation de la NERC du projet 2019-03 (p.2/4), consulté le 16 juin 2021 au https://www.nerc.com/pa/Stand/Project201903_Cyber%20Security%20Supply%20Chain%20Risks/2019-03_Implementation_Plan_clean_10072020.pdf

[12] Par sa décision D-2015-168, la Régie fixe l'entrée en vigueur des normes au 1er jour des trimestres civils suivant la date d'adoption.

[13] Par sa décision D-2016-011, la Régie fixe à soixante (60) jours le délai minimal à prévoir entre la date d'adoption et celle d'entrée en vigueur des normes à venir.

premier trimestre civil à survenir dix-huit (18) mois après l'adoption des trois (3) normes de fiabilité par la Régie.

1.6. Normes à retirer

Les normes de fiabilité CIP-005-6, CIP-010-3 et CIP-013-1 doivent être retirées dès l'entrée en vigueur des normes de fiabilité CIP-005-7, CIP-010-4 et CIP-013-2 respectivement.

1.7. Modifications au Glossaire

Aucune modification au Glossaire.

1.8. Modifications au Registre

Aucune modification au Registre.

2. ÉVALUATION DE LA PERTINENCE

Aux États-Unis, la FERC a émis une directive dans son Ordonnance 850[14] que les *systèmes de contrôle ou de surveillance des accès électroniques (EACMS)*, plus spécifiquement ceux qui assurent le contrôle ou la surveillance des accès électroniques à des *systèmes électroniques BES* à impact élevé ou moyen, soient inclus à la portée des normes concernant la gestion des risques de cybersécurité liés aux chaînes d'approvisionnement. En effet, la FERC affirme qu'il demeure un risque de cybersécurité significatif associé à la chaîne d'approvisionnement pour les *systèmes électroniques BES*, car le contrôle et la surveillance de l'accès électronique ne sont pas traités dans les versions actuelles des normes[15]. Les normes proposées dans le présent document répondent à la directive de la FERC.

Les *EACMS* jouent un rôle important dans la protection des *systèmes électroniques BES* à impact élevé et moyen. En effet, lorsqu'un *EACMS* est compromis, une personne malveillante pourrait plus facilement entrer dans le périmètre de sécurité du *système électronique BES* ou de l'actif électronique et le contrôler[16].

En ajout à la directive de la FERC, la NERC a proposé d'inclure à la portée des normes concernant la gestion des risques de cybersécurité liés aux chaînes d'approvisionnement les *systèmes de contrôle des accès physiques (PACS),* qui assurent le contrôle des accès physiques à des *systèmes électroniques BES* à impact élevé ou moyen et ce, même si une présence physique est tout de même nécessaire pour exploiter la vulnérabilité de *systèmes électroniques BES* à la suite de leur compromission à distance. Le risque pour la fiabilité du *système électronique BES* que représente un *PACS* compromis, mal utilisé, endommagé ou indisponible justifie l'inclusion des *PACS* parmi les catégories d'*actifs électroniques* visées[17].

---

[14] Ordonnance 850 de la FERC, consultée le 29 juin 2021 au https://www.nerc.com/FilingsOrders/us/FERCOrdersRules/Order%20No.%20850%20Supply%20Chain%20Risk%20Management%20Reliability%20Standards.pdf (en anglais seulement)

[15] Ordonnance 850 de la FERC (p.3), consultée le 29 juin 2021 au https://www.nerc.com/FilingsOrders/us/FERCOrdersRules/Order%20No.%20850%20Supply%20Chain%20Risk%20Management%20Reliability%20Standards.pdf (en anglais seulement)

[16] Ordonnance 850 de la FERC (p.4), consultée le 29 juin 2021 au https://www.nerc.com/FilingsOrders/us/FERCOrdersRules/Order%20No.%20850%20Supply%20Chain%20Risk%20Management%20Reliability%20Standards.pdf

[17] Justification technique de la NERC, consultée le 29 juin 2021 au https://www.nerc.com/pa/Stand/Project201903_Cyber%20Security%20Supply%20Chain%20Risks/2019-03_CIP-005-7_Technical_Rationale_clean_10072020.pdf (en anglais seulement)

Concrètement, il s'agit de l'ajout de l'exigence E3 dans la norme de fiabilité CIP-005-7 et l'ajout des *EACMS* et des *PACS* aux exigences déjà présentes aux normes de fiabilité CIP-010-4 et CIP-013-2. L'exigence E3 a été ajoutée afin de disposer d'une ou de plusieurs méthodes pour déterminer, interrompre et contrôler la possibilité de reconnexion des connexions à distance authentifiées commandées par des fournisseurs[18].

Pour les normes de fiabilité CIP-010-4 et CIP-013-2, une référence aux *EACMS* et *PACS* a été ajoutée à chacune des exigences.

Conformément à sa lettre d'ordonnance RD21-2-000[19], la FERC est d'avis que l'inclusion des *EACMS* et des *PACS* aux normes de fiabilité CIP-005-7, CIP-010-4 et CIP-013-2 rehausse la fiabilité du réseau *BES* tout en maintenant les objectifs de sécurité mentionnés dans la version originale des normes entourant la gestion des risques de cybersécurité liés aux chaînes d'approvisionnement.

De plus, l'Instance n° 498[20] à la Commission de l'énergie et des services publics du Nouveau-Brunswick, traitant du projet 2019-03 de la NERC, a été approuvée le 26 juillet 2021 et la Commission de l'énergie de l'Ontario a débuté le traitement de ce projet.

Le Coordonnateur est d'avis que les normes CIP-005-7, CIP-010-4 et CIP-013-2 sont pertinentes pour le Québec, car il existe la même faiblesse au niveau de la gestion des risques de cybersécurité liés aux chaînes d'approvisionnement, soit qu'une attaque malveillante pourrait être faite via les *EACMS* et les *PACS* et par le fait même impacter directement *les systèmes électroniques BES*, notamment en perturbant les activités qui lui sont associées. Ces normes proposées viennent donc corriger cette faiblesse.

En considérant les éléments mentionnés ci-haut concernant les normes CIP-005-7, CIP-010-4 et CIP-013-2 et en considérant que ces normes ont été élaborées par des organismes reconnus en Amérique du Nord et ce, conformément à l'entente conclue en 2009 entre la Régie, la NERC et le NPCC avec l'autorisation du gouvernement du Québec[21], le Coordonnateur est d'avis que les normes CIP-005-7, CIP-010-4 et CIP-013-2 contribuent à la fiabilité du réseau du Québec.

3. ÉVALUATION PRÉLIMINAIRE DE L'IMPACT

Cette section présente l'évaluation préliminaire de l'impact sur l'ensemble des entités du Québec selon le *coordonnateur de la fiabilité*.

Pour les normes CIP-005 et CIP-013, les entités visées possèdent déjà des mécanismes en place pour rencontrer les exigences des nouvelles versions des normes, c'est pourquoi un impact faible est motivé par le Coordonnateur de la fiabilité. En ce qui concerne la norme CIP-010, l'impact sur les entités visées est modéré, car il y a une augmentation de la charge de travail au niveau de l'implantation, du maintien et du suivi des exigences de la nouvelle version de la norme et la gestion du mécanisme en place peut être améliorée.

[18] Sommaire des modifications de la NERC, consulté le 12 août 2021 au https://www.nerc.com/pa/Stand/Project201903_Cyber%20Security%20Supply%20Chain%20Risks/2019-03_CIP-005-7_Summary_of_Changes_10072020.pdf (en anglais seulement).

[19] Lettre d'ordonnance RD21-2-000 de la FERC, consultée le 16 juin 2021 au https://www.nerc.com/FilingsOrders/us/NERC%20Filings%20to%20FERC%20DL/Petition%20-%20Supply%20Chain%20Risk%20Management_final.pdf (en anglais seulement).

[20] Instance n° 498 au Nouveau-Brunswick, consultée le 29 juin 2021 au https://filemaker.nbeub.ca/fmi/webd/NBEUB%20ToolKit13

[21] Entente conclue conformément au décret n° 443-2009 publié le 8 avril 2009. http://www.regie-energie.qc.ca/audiences/normes_fiab_tranp_elec/Entente_Regie_NERC_NPCC_5mai09.pdf

	Impacts		
Norme	Implantation	Maintien	Suivi
CIP-005-7	Faible	Faible	Faible
CIP-010-4	Modéré	Modéré	Modéré
CIP-013-2	Faible	Faible	Faible

Légende :

Faible : Pratique normale de l'industrie ou norme n'entraînant que des ajustements mineurs aux processus ou aux pratiques en place.

Modéré : Changement qui nécessite de mobiliser certaines ressources matérielles, humaines ou financières pour implanter la norme proposée, la maintenir ou assurer le suivi de la conformité.

Important : Changement qui nécessite de prévoir et de mobiliser d'importantes ressources matérielles, humaines ou financières pour planifier et implanter la norme proposée, la maintenir ou assurer le suivi de la conformité.

4. Évaluation finale de l'impact

Au terme de la période de consultation, les entités HQP et RTA ont transmis des commentaires. De plus, HQP et RTA ont fait parvenir un tableau des impacts financiers pour la mise en application des normes. Le Coordonnateur retranscrit d'une manière littérale le tableau soumis par les entités HQP et RTA.

Entité	Norme	Coût de mise en œuvre ($)	Coût récurrents annuels ($/an)	Justification
HQP	CIP-005-7	0,00	0,00	Les nouvelles exigences E3.1 et E3.2 ne s'appliquent pas à HQP puisque nous n'avons pas de systèmes BES à impact élevé ni de systèmes BES moyen à connectivité externe routable.
HQP	CIP-010-4	0,00	0,00	Pas de changement dans le processus existant malgré l'ajout des EACMS associées en tant que nouveau système visé.
HQP	CIP-013-2	50 000,00	25 000,00	Ajustement de processus
RTA	CIP-005-7	10 000,00	5 000,00	mise à jour Doc, contrôles, diffusion, suivi
RTA	CIP-010-4	10 000,00	15 000,00	mise à jour Doc, contrôles, diffusion, suivi
RTA	CIP-013-2	5 000,00	5 000,00	mise à jour Doc, contrôles, diffusion, suivi
	Total	75 000,00	50 000,00	

En considérant les commentaires reçus, le Coordonnateur est d'avis que son évaluation de l'impact demeure inchangée pour les normes CIP-005-7 et CIP-010-4. Cependant, pour la norme CIP-013-2, l'impact

pour l'implantation, le maintien et le suivi de la norme passe de faible à modéré, car elle implique des changements au niveau de la chaîne d'approvisionnement, qui est le principal vecteur d'infection par virus informatique.