
Projet QC-2019-05

Norme CIP-008-6 – Cybersécurité – Sécurité physique des systèmes électroniques BES

1. PRÉSENTATION DE LA NORME

1.1. Applicabilité de la norme

La norme CIP-008-6 s'applique aux fonctions visées suivantes :

- *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)*¹

Les installations visées sont :

- Les installations du RTP qui répondent aux critères définis dans la section Applicabilité.
- Certaines installations spécifiques des distributeurs.

1.2. Objet de la norme

L'objectif de la norme CIP-008-6 est de réduire les risques posés au fonctionnement fiable du BES par un incident de cybersécurité en définissant des exigences d'intervention en cas d'incident.

1.3. Contexte réglementaire

La Régie de l'énergie (ci-après, la « Régie ») a adopté la norme CIP-008-5 dans la décision D-2016-119² et la norme est en vigueur depuis le 1^{er} janvier 2017.

La norme CIP-008-6 a été adoptée par le conseil d'administration de la NERC le 2 février 2019 et approuvée par la FERC le 20 juin 2019 dans le cadre du dossier RD19-3-000.³

¹ Voir la section Applicabilité des normes CIP pour les détails concernant l'application pour les distributeurs.

² Régie de l'énergie, Décision D-2016-119, consultée le 13 août 2019 au http://publicsde.regie-energie.qc.ca/projets/335/DocPri/R-3947-2015-A-0022-Dec-Dec-2016_07_29.pdf.

³ FERC, Docket No. RD19-3-000, consulté le 13 août 2019 au <https://www.nerc.com/FilingsOrders/us/FERCOrdersRules/Order%20Docket%20No.%20RD19-3-000.pdf> (en anglais seulement)

1.4. Dispositions particulières pour le Québec

Le *Coordonnateur de la fiabilité* (ci-après appelé le « *Coordonnateur* ») propose de reconduire les spécificités québécoises, notamment le champ d'application et les dispositions particulières, déjà adoptées par la Régie dans sa décision D-2016-119 qui exempte certaines centrales et leur poste élévateur. La norme s'applique aux installations du *réseau de transport principal (RTP)* et aux installations spécifiées pour les *distributeurs*. De plus, les dispositions particulières suivantes s'appliquent

- Est exemptée de cette 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.
- Sont exemptés de cette norme les postes élévateurs des *installations* de production exemptées selon le point précédent.

1.5. Dates d'entrée en vigueur proposées

La norme CIP-008-6 entrera en vigueur le 1^{er} janvier 2021. Le plan de mise en œuvre aux États-Unis⁴ précise que le délai entre l'approbation réglementaire et la mise en œuvre de la norme doit être de 18 mois.

Au Québec, le *Coordonnateur* propose le même délai de 18 mois entre l'adoption de la norme par la Régie et son entrée en vigueur.

1.6. Normes ou exigences à retirer

La norme CIP-008-5 doit être retirée dès l'entrée en vigueur de la norme CIP-008-6.

1.7. Modifications au Glossaire

Des modifications au Glossaire doivent prendre effet dès l'entrée en vigueur de la norme CIP-008-6. Les termes suivants sont modifiés :

- *incident de cybersécurité* ;
- *incident de cybersécurité à déclarer*.

Les définitions de ces termes sont présentées, en français et en anglais, dans le document *Modifications au Glossaire*.

La mise en vigueur des normes est conditionnelle aux changements des définitions des termes *automatisme de réseau* et *plan de défense* tel que demandés à la Régie au dossier R-4070-2018.

2. ÉVALUATION DE LA PERTINENCE

À la suite de l'ordonnance 848⁵ de la FERC, la NERC a modifié la norme CIP-008-5 afin d'augmenter la notification obligatoire des *incidents de cybersécurité*, notamment les tentatives susceptibles de nuire au bon fonctionnement du *système de production-transport de l'électricité*.

4. NERC Implementation Plan, consulté le 8 octobre 2019 au https://www.nerc.com/pa/Stand/Project%20201802%20Modifications%20to%20CIP008%20Cyber%20Secur/2018-02_CIP-008_Implementation%20Plan_Final%20Ballot_clean_01152019.pdf (en anglais seulement).

5. Ordonnance n° 848 de la FERC, consultée le 8 octobre 2019 au <https://www.ferc.gov/whats-new/comm-meet/2018/071918/E-1.pdf> (en anglais seulement).

La nouvelle norme CIP-008-6 ainsi que les modifications apportées aux définitions, aborde les quatre éléments décrits dans l'ordonnance 848 de la FERC⁶ :

- le signalement d'*incidents de cybersécurité* compromettant ou tentant de compromettre un *périmètre de sécurité électronique (ESP) (Electric Security Perimeter)* ou un *système de contrôle ou de surveillance des accès électronique (EACMS) (Electronic Access Control or Monitoring System)* associé ;
- l'amélioration de la qualité des rapports d'*incidents de cybersécurité* en veillant à ce que chaque rapport comprenne des champs d'information spécifiés afin de faciliter la comparaison ;
- l'établissement des délais pour le dépôt des rapports d'*incident de cybersécurité* selon la gravité de l'incident ;
- l'obligation de transmettre les rapports de cybersécurité à l'Electricity Information Sharing and Analysis Center (E-ISAC) ainsi qu'au Department of Homeland Security (DHS) et à l'Industrial Control System Cyber Emergency Response Team (ICS-CERT).

En effet, les modifications quant à l'augmentation des types d'*incidents de cybersécurité* faisant l'objet d'une notification obligatoire, notamment les tentatives de compromettre un *ESP* ou un *EACMS* d'une entité ainsi que les révisions apportées aux exigences R1 à R4 tenant compte de l'ajout des *EACMS* associés aux *systèmes électroniques BES* à impact moyen et à impact élevé sont aussi pertinentes au Québec qu'ailleurs en Amérique du Nord.

Conformément à l'entente conclue en 2009 entre la Régie, la NERC et le NPCC et avec l'autorisation du gouvernement du Québec⁷, cette norme a été élaborée et approuvée par des organismes externes pour l'Amérique du Nord, y compris le Québec. Le *coordonnateur de la fiabilité* est d'avis que cette norme est pertinente pour la fiabilité du réseau du Québec et qu'elle contribue à l'harmonisation avec les réseaux voisins.

3. ÉVALUATION PRÉLIMINAIRE DE L'IMPACT

Cette section présente l'évaluation préliminaire de l'impact selon le *coordonnateur de la fiabilité*.

| CIP-008-6 | Faible | Modéré | Important |
|--------------------------|--------|--------|-----------|
| Implantation de la norme | | X | |
| Maintien de la norme | | X | |
| Suivi de la conformité | | X | |

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.

6. Consideration of Issues and Directives (en anglais seulement), consulté en ligne le 8 octobre 2019 au https://www.nerc.com/pa/Stand/Project%20201802%20Modifications%20to%20CIP008%20Cyber%20Secur/CIP-008_Consideration_of_Issues_and_Directives_Feb_2019.pdf (en anglais seulement).

7. Entente conclue conformément au décret n° 443-2019 du 8 avril 2019.

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

4. ÉVALUATION FINALE DE L'IMPACT

Section à remplir dès réception des formulaires d'évaluation de l'impact et à la conclusion du processus de consultation préalable au dépôt des normes auprès de la Régie.