
Projet QC-2021-02

Norme CIP-012-1 – *Cybersécurité – Communications entre centres de contrôle*

1. PRÉSENTATION DE LA NORME

1.1. Applicabilité de la norme

La norme CIP-012-1 s'applique aux entités fonctionnelles suivantes qui détiennent ou exploitent un *centre de contrôle*, ci-après appelées « entités responsables ».

- *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)*

Exemptions : Sont exemptés de la norme de fiabilité CIP-012-1 :

- Tout *centre de contrôle* qui transmet à un autre *centre de contrôle* des données d'évaluation en temps réel ou de surveillance en temps réel concernant exclusivement la ressource de production ou le poste de transport situé au même endroit que le *centre de contrôle* transmetteur.

1.2. Objet de la norme

L'objectif de la norme CIP-012 est de protéger la confidentialité et l'intégrité des données d'évaluation en temps réel et de surveillance en temps réel transmises entre différents centres de contrôle.

1.3. Contexte réglementaire

La présente concerne le premier dépôt réglementaire auprès de la Régie de l'énergie (ci-après, la « Régie ») en vue de l'adoption de la norme CIP-012-1. Aux États-Unis, la norme CIP-012-1 a été adoptée par le conseil d'administration de la NERC le 16 août 2018 et approuvée par la FERC le 23 janvier 2020 dans l'ordonnance 866¹.

1.4. Dispositions particulières pour le Québec

Le Coordonnateur de la fiabilité (ci-après le « Coordonnateur ») propose que la norme CIP-012-1 s'applique aux centres de contrôle qui hébergent un personnel d'exploitation qui surveille et contrôle le réseau de transport principal (RTP).

¹ [https://www.nerc.com/FilingsOrders/us/FERCOrdersRules/Order%20Approving%20Reliability%20Standard%20CIP-012-1%20\(Cyber%20Security%20E2%80%93%20Communications%20between%20Control%20Centers\).pdf](https://www.nerc.com/FilingsOrders/us/FERCOrdersRules/Order%20Approving%20Reliability%20Standard%20CIP-012-1%20(Cyber%20Security%20E2%80%93%20Communications%20between%20Control%20Centers).pdf), consulté le 22 janvier 2021

1.5. Dates d'entrée en vigueur proposées

Le plan de mise en œuvre de la NERC² de la norme CIP-012-1 précise que le délai entre l'approbation gouvernementale et l'entrée en vigueur de cette norme est de 24 mois. La norme CIP-012-1 entrera en vigueur aux États-Unis le 1er juillet 2022³.

Au Québec, étant donné l'importance d'avoir des pratiques uniformes avec des normes obligatoires en vigueur harmonisées avec les États-Unis, le Coordonnateur propose une date d'entrée en vigueur le premier jour du premier trimestre civil⁴ à survenir 24 mois après l'adoption de la norme par la Régie. Il est cependant important de préciser qu'au vu du délai assez long, le Coordonnateur a considéré le délai de 60 jours⁵ dans ledit délai NERC de 24 mois.

1.6. Normes ou exigences à retirer.

Aucune norme à retirer.

1.7. Modifications au Glossaire

Aucune modification au Glossaire.

2. ÉVALUATION DE LA PERTINENCE

L'objectif de ce projet est de répondre à l'ordonnance n°822⁶ de la FERC visant à apporter des améliorations aux normes de fiabilité CIP afin d'atténuer les risques de cybersécurité en exigeant que les entités responsables protègent la confidentialité et l'intégrité des données d'évaluation en temps réel et de surveillance en temps réel transmises entre les centres de contrôle, garantissant ainsi l'échange de données opérationnelles et adressant le risque potentiel de perte de données. L'équipe de rédaction du projet à la NERC a déterminé que la directive de la FERC dans l'ordonnance 822 serait mieux respectée en élaborant une nouvelle norme de fiabilité au lieu de réviser la norme CIP-006-6. L'applicabilité des protections mentionnées dans la CIP-012-1 diffère de celles mentionnées dans la norme CIP-006-6⁷. La norme CIP-012-1 ne s'applique pas aux systèmes électroniques BES. Alors que l'exigence E1 partie 1.10 de la norme CIP-006-6 s'applique aux systèmes électroniques BES à impact moyen dans les centres de contrôle, la norme CIP-012-1 s'applique aux communications entre certains centres de contrôle. En outre, les modifications ont été apportées afin d'exiger des protections sur la disponibilité des liaisons de communication et des données communiquées entre les centres de contrôle du BES.

Par son ordonnance n°866⁸, la FERC a approuvé la norme CIP-012-1.

Alors que les normes CIP-003 à CIP-011 protègent les données emmagasinées, la norme CIP-012-1 exige que les entités responsables élaborent et mettent en œuvre un plan afin d'adresser les risques posés par

² <https://www.nerc.com/pa/Stand/Project%20201602%20Modifications%20to%20CIP%20Standards%20DL/CIP-012-1%20Implementation%20Plan%20Clean%2008032018.pdf>, consulté le 22 janvier 2021

³ <https://www.nerc.net/standardsreports/standardssummary.aspx>, consulté le 22 janvier 2021

⁴ <http://www.regie-energie.qc.ca/audiences/decisions/D-2015-168.pdf>

⁵ <http://www.regie-energie.qc.ca/audiences/decisions/D-2016-011.pdf>

⁶ <https://www.nerc.com/FilingsOrders/us/FERCOrdersRules/Order%20Approving%20Revised%20CIP%20Reliability%20Standards.pdf>

⁷ <https://www.nerc.com/pa/Stand/Project%20201602%20Modifications%20to%20CIP%20Standards%20RF/CIP%20Technical%20Rationale%20for%20CIP-012%20Clean%2008062018.pdf>

⁸ [https://www.nerc.com/FilingsOrders/us/FERCOrdersRules/Order%20Approving%20Reliability%20Standard%20CIP-012-1%20\(Cyber%20Security%20E2%80%93%20Communications%20between%20Control%20Centers\).pdf](https://www.nerc.com/FilingsOrders/us/FERCOrdersRules/Order%20Approving%20Reliability%20Standard%20CIP-012-1%20(Cyber%20Security%20E2%80%93%20Communications%20between%20Control%20Centers).pdf)

la divulgation non-autorisée (confidentialité) et la modification non-autorisée (intégrité) des données d'évaluation *en temps réel* et de surveillance *en temps réel* lors de leur transmission entre les *centres de contrôle*⁹. Le plan doit inclure les éléments suivants :

- 1- L'identification des protections en matière de sécurité
- 2- L'identification des endroits où les protections sont appliquées
- 3- L'identification des responsabilités de chaque entité dans le cas où les *centres de contrôle* sont détenus ou exploités par les différentes entités responsables.

Afin que certaines entités responsables puissent exécuter leurs fonctions de fiabilité *en temps réel*, leurs *centres de contrôle* associés doivent être capables de recevoir et stocker une variété de données sensibles provenant d'entités interconnectées. Les protections proposées dans la norme CIP-012-1 assurent la rapidité et l'exactitude de ces communications en prenant ainsi en charge les opérations fiables *du réseau de transport principal (RTP)* du Québec.

En outre, la NERC a pris la décision¹⁰ en juin 2017, de retirer la section dédiée aux Principes directeurs et fondements techniques dans les gabarits des normes de fiabilité. Les informations contenues sous cette section seront transférées vers les documents suivants : la Justification technique et/ou le Guide d'application¹¹. Ces documents associés aux normes seront affichés séparément sur le site internet de la NERC à la section « Related Information »¹² (Informations connexes du projet) associée à la norme de fiabilité CIP-012-1. Il est nécessaire de noter que le Guide d'application¹³ et la Justification technique¹⁴ de la norme CIP-012-1 ne sont pas encore disponibles en version finale à la NERC. Le Coordonnateur est en attente des versions finales qui seront déposées ultérieurement à la Régie.

Conformément à l'entente conclue en 2009 entre la Régie, la NERC et le NPCC avec l'autorisation du gouvernement du Québec¹⁵, cette norme a été élaborée et approuvée par des organismes externes pour l'Amérique du Nord, y compris le Québec. Le Coordonnateur est d'avis que cette norme contribue à la fiabilité du réseau du Québec et 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-012-1	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.

⁹ <https://www.nerc.com/FilingsOrders/us/NERC%20Filings%20to%20FERC%20DL/Final%20CIP-012-1%20Petition.pdf>

¹⁰ <https://www.nerc.com/pa/Stand/Technical%20Rationale%20for%20Reliability%20Standards/Technical%20Rationale%20Transition%20Plan.pdf>

¹¹ <https://www.nerc.com/pa/Stand/Pages/TechnicalRationaleforReliabilityStandards.aspx>

¹² <https://www.nerc.com/pa/Stand/Pages/StandardsSubjecttoFutureEnforcement.aspx?jurisdiction=United%20States>

¹³ [https://www.nerc.com/pa/comp/guidance/EROEndorsedImplementationGuidance/CIP-012-](https://www.nerc.com/pa/comp/guidance/EROEndorsedImplementationGuidance/CIP-012-1%20Communications%20Between%20Control%20Centers%20(2016-02%20SDT).pdf)

[1%20Communications%20Between%20Control%20Centers%20\(2016-02%20SDT\).pdf](https://www.nerc.com/pa/comp/guidance/EROEndorsedImplementationGuidance/CIP-012-1%20Communications%20Between%20Control%20Centers%20(2016-02%20SDT).pdf)

¹⁴ https://www.nerc.com/pa/Stand/Project%20201602%20Modifications%20to%20CIP%20Standards%20RF/CIP_Technical_Rationale_for_CIP-012_Clean_08062018.pdf

¹⁵ Entente conclue conformément au décret n° 443-2009 publié le 8 avril 2009.

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

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.