
Projet QC-2014-02**Normes CIP-002-5 à CIP-009-5 et normes CIP-010-1 et CIP-011-1****Protection des infrastructures critiques**

1. ÉVALUATION DE LA PERTINENCE

Au cours des deux dernières décennies, les outils d'exploitation des réseaux électriques interconnectés ont considérablement évolués. Le déploiement de composants informatiques, d'appareils intelligents interconnectés et de réseaux de télécommunications de nouvelle génération a considérablement amélioré la fiabilité du service d'électricité. L'intégration de ces nouvelles technologies a également introduit de nouveaux risques liés aux menaces cybernétiques et les dommages potentiels qu'elles peuvent causer.

La protection du réseau électrique contre les attaques cybernétiques est d'une importance majeure pour la sécurité nationale. Des données récentes portent à croire que les cyber-attaques sur les infrastructures critiques et sur les réseaux électriques en particulier sont en augmentation, tant en fréquence qu'en sophistication. Ces tendances sont alarmantes, car les conséquences potentielles d'une attaque à grande échelle réussie sur le secteur de l'électricité ne peuvent être ignorées. Comme les pannes de réseau majeures passées l'ont montré, tout événement qui provoque des pannes de courant prolongées sur un grand territoire serait non seulement extrêmement coûteux, mais impacterait aussi sévèrement les habitudes de vie de millions de gens et pourrait profondément perturber la livraison des services essentiels, y compris les communications, la nourriture, l'eau, les soins de santé, et les interventions d'urgence. Par ailleurs, les menaces cybernétiques, contrairement aux menaces à la fiabilité du réseau électrique telles que les conditions météorologiques extrêmes, sont moins prévisibles et plus difficile à traiter. Le risque d'une attaque réussie est bien réel. En effet, l'équipe d'intervention d'urgence « Industrial Control Systems Cyber Emergency Response Team » (ICS-CERT), qui fait partie du ministère américain de la Sécurité intérieure (DHS), a rapporté répondre à 198 incidents de cybersécurité au cours de l'année 2012 dans tous les secteurs d'infrastructures critiques. Quarante et un pour cent de ces incidents impliquaient le secteur de l'énergie, et plus particulièrement l'électricité.

L'adoption en continu et l'évolution des normes en matière de cybersécurité est donc nécessaire pour protéger les réseaux électriques interconnectés contre les menaces mentionnées ci-dessus. La version 5 des normes CIP (CIP-002-5 à CIP-009-5 ainsi que les normes CIP-010-1 et CIP-011-1) représente une amélioration importante par rapport à la version 1 des normes CIP adoptées par la Régie de l'énergie dans le cadre du dossier R-3699-2009. Cette nouvelle version est forte des quatre années d'expérience acquises par l'industrie électrique nord-américaine dans l'application des versions 1 et 3 de ces normes¹. Malgré que le cadre d'application des nouvelles normes CIP dans son ensemble demeure semblable, la norme CIP-002-5 propose un nouveau processus pour identifier les actifs critiques du système de production-transport d'électricité en identifiant et catégorisant plutôt les systèmes électroniques associés à ces actifs. Les normes CIP-003-5 à CIP-011-1 s'appliqueront donc

¹ Les normes CIP en versions 2 et 4 ne sont jamais entrées en vigueur.

aux systèmes électroniques identifiés en vertu de la norme CIP-002. Parmi les améliorations notables, nous retrouvons :

- L'utilisation de critères de classification clairs et définis (« bright-line criteria ») pour identifier les éléments critiques à l'exploitation du réseau de transport rendant l'identification plus uniforme et objective.
- L'utilisation d'une approche basée sur l'Institut National des Normes et de la technologie (National Institute of Standards and Technology – NIST) pour catégoriser l'impact des systèmes sur le système de production-transport d'électricité (Impacts « Faible », « Moyen » ou « Élevé »). Cette approche permet de sécuriser adéquatement les systèmes selon leur impact réel.
- L'élimination des exigences de documentation superflues pour permettre aux entités de se concentrer sur la fiabilité et la sécurité du réseau de transport.
- Une mise en contexte et des principes directeurs compris dans chaque norme pour guider la mise en œuvre par les entités.
- Le traitement de toutes les directives de modifications émises par la FERC dans l'ordonnance 706.

Les normes CIP proposées satisfont l'objectif de fiabilité consistant à définir un cadre de cybersécurité complet et cohérent pour l'identification et la protection des systèmes électroniques qui sont nécessaires à l'exploitation fiable des réseaux de transport interconnectés. Les normes CIP peuvent être séparées en deux catégories :

- 1) Catégorisation du risque (Faible, Moyen ou Élevé)
 - CIP-002-5.1 – Catégorisation des systèmes électroniques BES
- 2) Cycle de vie de la mitigation du risque (mise en œuvre, évaluation, surveillance et mise-à-jour)
 - CIP-003-5 – Mécanismes de gestion de la sécurité
 - CIP-004-5.1 – Personnel et formation
 - CIP-005-5 – Périmètres de sécurité électroniques
 - CIP-006-5 – Sécurité physique des systèmes électroniques BES
 - CIP-007-5 – Gestion de la sécurité des systèmes
 - CIP-008-5 – Déclaration des incidents et planification des mesures d'intervention
 - CIP-009-5 – Plans de rétablissement des systèmes électroniques BES
 - CIP-010-1 – Gestion des changements de configuration et analyses de vulnérabilité
 - CIP-011-1 – Protection de l'information

La norme CIP-002-5, qui consiste en l'identification et la catégorisation des systèmes, constitue la première étape du cadre de cybersécurité. Une entité qui n'a identifié aucun système en conformité avec la CIP-002-5 n'aura pas à se conformer aux normes CIP-003-5 à CIP-011-1.

2. PRÉREQUIS À L'ADOPTION

Adoption des définitions proposées à la section suivante.

3. MODIFICATIONS À D'AUTRES NORMES OU AUX DÉFINITIONS DU GLOSSAIRE

Les ajouts, modifications ou retraits suivants entreront en vigueur en même temps que les normes proposées.

3.1. Normes ou exigences à retirer lors de l'entrée en vigueur :

Normes CIP-002-1 à CIP-009-1.

3.2. Nouvelles définitions à ajouter au glossaire :

Terme	Acronyme	Définition
Accès distant interactif		<p>Accès commandé par une personne utilisant un client d'accès distant ou une autre technologie d'accès distant avec un protocole routable. L'accès distant provient d'un <i>actif électronique</i> qui n'est pas un <i>système intermédiaire</i> et qui n'est situé ni à l'intérieur d'un des <i>périmètres de sécurité électronique</i> de l'entité responsable, ni à un <i>point d'accès électronique</i> (EAP) défini. L'accès distant peut être commandé à partir d'<i>actifs électroniques</i> utilisés ou détenus : 1) par l'entité responsable, 2) par des employés ou 3) par des fournisseurs, des entrepreneurs ou des consultants. L'<i>accès distant interactif</i> ne comprend pas les communications de processus de système à système.</p> <p>(Interactive Remote Access)</p> <p>Source : Glossaire des termes en usage dans les normes de fiabilité (NERC)</p>
Actif électronique BES		<p><i>Actif électronique</i> qui, s'il était endommagé, mal utilisé ou rendu indisponible, entraînerait, dans les 15 minutes suivant son fonctionnement requis, son fonctionnement incorrect, ou son non-fonctionnement, un impact négatif sur un ou plusieurs réseaux, <i>installations</i> ou équipements, lesquels, s'ils se trouvaient détruits, endommagés ou autrement rendus indisponibles en cas de besoin, affecteraient l'exploitation fiable du <i>système de production-transport d'électricité</i>. La redondance des réseaux, installations ou équipements en question ne doit pas être prise en compte dans l'évaluation de l'impact négatif. Chaque <i>actif électronique BES</i> est compris dans un ou plusieurs <i>systèmes électroniques BES</i>. (Un <i>actif électronique</i> n'est pas un <i>actif électronique BES</i> si, pendant 30 jours civils consécutifs ou moins, il est relié directement à un réseau situé dans un <i>périmètre de sécurité électronique</i> (ESP), à un <i>actif électronique</i> situé à l'intérieur d'un ESP ou à un <i>actif électronique BES</i> et qu'il est utilisé à des fins de transfert de données, d'analyse de vulnérabilité, de maintenance ou de diagnostic.)</p> <p>(BES Cyber Asset)</p> <p>Source : Glossaire des termes en usage dans les normes de fiabilité (NERC)</p>

Terme	Acronyme	Définition
Actifs électroniques protégés	PCA	<p>Un ou plusieurs <i>actifs électroniques</i> reliés au moyen d'un protocole routable, à l'intérieur ou autour d'un <i>périmètre de sécurité électronique</i> et qui ne font pas partie du <i>système électronique BES</i> dont le degré d'impact est le plus élevé à l'intérieur d'un même <i>périmètre de sécurité électronique</i>. Le degré d'impact des <i>actifs électroniques protégés</i> est égal à celui du <i>système électronique BES</i> dont le degré d'impact est le plus élevé dans le même ESP. Un <i>actif électronique</i> n'est pas un <i>actif électronique protégé</i> si, pendant 30 jours civils consécutifs ou moins, il est relié à un <i>actif électronique</i> situé à l'intérieur de l'ESP ou au réseau situé à l'intérieur de l'ESP, et qu'il est utilisé pour le transfert de données, l'analyse de vulnérabilité, la maintenance ou le diagnostic.</p> <p>(Protected Cyber Assets)</p> <p>Source : Glossaire des termes en usage dans les normes de fiabilité (NERC)</p>
Cadre supérieur CIP		<p>Un cadre supérieur unique qui dispose de l'autorité et de la responsabilité pour mener et gérer la mise en œuvre et le respect permanent des exigences des normes CIP-002 à CIP-011 de la NERC.</p> <p>(CIP Senior Manager)</p> <p>Source : Glossaire des termes en usage dans les normes de fiabilité (NERC)</p>
Centre de contrôle		<p>Une ou plusieurs installations (y compris les centres informatiques connexes) qui hébergent un personnel d'exploitation qui surveille et contrôle le <i>système de production-transport d'électricité</i> (BES) en temps réel afin d'effectuer les tâches de fiabilité de : 1) un <i>coordonnateur de la fiabilité</i> ; 2) un <i>responsable de l'équilibrage</i> ; 3) un <i>exploitant de réseau de transport</i> pour des <i>installations</i> de transport à deux endroits ou plus ; 4) un <i>exploitant d'installation de production</i> pour des <i>installations</i> de production à deux endroits ou plus.</p> <p>(Control Center)</p> <p>Source : Glossaire des termes en usage dans les normes de fiabilité (NERC)</p>
Circonstance CIP exceptionnelle		<p>Situation qui entraîne ou menace d'entraîner une ou plusieurs des conditions suivantes (ou des conditions semblables) mettant en cause la sécurité ou la fiabilité du BES : un risque de blessure ou de décès ; une catastrophe naturelle ; des troubles civils ; une panne imminente ou existante de matériel, de logiciel ou d'équipement ; un <i>incident de cybersécurité</i> nécessitant une aide d'urgence ; une intervention des services d'urgence ; l'adoption d'une entente d'assistance mutuelle ; une indisponibilité de main-d'œuvre à grande échelle.</p> <p>(CIP Exceptional Circumstance)</p> <p>Source : Glossaire des termes en usage dans les normes de fiabilité (NERC)</p>

Terme	Acronyme	Définition
Connectivité externe routable		<p>Capacité d'accéder à un <i>système électronique BES</i>, à partir d'un <i>actif électronique</i> situé à l'extérieur du <i>périmètre de sécurité électronique</i> qui y est associé, au moyen d'une liaison bidirectionnelle à protocole routable.</p> <p>(External Routable Connectivity)</p> <p>Source : Glossaire des termes en usage dans les normes de fiabilité (NERC)</p>
Connectivité par lien commuté		<p>Liaison d'échange de données qui est établie lorsqu'un équipement de télécommunications compose un numéro de téléphone et négocie une connexion avec un équipement situé à l'autre bout de la liaison.</p> <p>(Dial-up Connectivity)</p> <p>Source : Glossaire des termes en usage dans les normes de fiabilité (NERC)</p>
Incident de cybersécurité à déclarer		<p><i>Incident de cybersécurité</i> qui a compromis ou perturbé une ou plusieurs tâches de fiabilité d'une entité fonctionnelle.</p> <p>(Reportable Cyber Security Incident)</p> <p>Source : Glossaire des termes en usage dans les normes de fiabilité (NERC)</p>
Information de système électronique BES		<p>Information sur un <i>système électronique BES</i> qui pourrait être utilisée pour accéder sans autorisation au <i>système électronique BES</i> ou constituer une menace à sa sécurité. Une <i>information de système électronique BES</i> ne comprend pas les éléments d'information qui, pris séparément, ne constituent pas une menace ou ne pourraient pas être utilisés pour permettre l'accès non autorisé aux <i>systèmes électroniques BES</i>, tels que des noms de dispositif, des adresses IP individuelles sans contexte, des noms de <i>périmètre de sécurité électronique</i> et des énoncés de politique. Des exemples d'information de <i>système électronique BES</i> peuvent notamment comprendre des procédures de sécurité ou des informations de sécurité au sujet des <i>systèmes électroniques BES</i>, des <i>systèmes de contrôle des accès physiques</i>, des <i>systèmes de contrôle ou de surveillance des accès électroniques</i> qui ne sont pas accessibles au public et qui pourraient être utilisées pour permettre un accès ou une diffusion non autorisés ; des collections d'adresses réseau ; et la topologie réseau du <i>système électronique BES</i>.</p> <p>(BES Cyber System Information)</p> <p>Source : Glossaire des termes en usage dans les normes de fiabilité (NERC)</p>

Terme	Acronyme	Définition
Point d'accès électronique	EAP	<p>Interface d'<i>actif électronique</i>, sur un <i>périmètre de sécurité électronique</i> qui permet d'établir une communication routable entre des <i>actifs électroniques</i> à l'extérieur d'un <i>périmètre de sécurité électronique</i> et des <i>actifs électroniques</i> à l'intérieur du <i>périmètre de sécurité électronique</i>.</p> <p>(Electronic Access Point)</p> <p>Source : Glossaire des termes en usage dans les normes de fiabilité (NERC)</p>
Système électronique BES		<p>Un ou plusieurs <i>actifs électroniques BES</i> regroupés logiquement par une entité responsable afin d'effectuer une ou plusieurs tâches de fiabilité pour une entité fonctionnelle.</p> <p>(BES Cyber System)</p> <p>Source : Glossaire des termes en usage dans les normes de fiabilité (NERC)</p>
Système intermédiaire		<p><i>Actif électronique</i> ou groupe d'<i>actifs électroniques</i> effectuant un contrôle d'accès visant à restreindre l'<i>accès distant interactif</i> aux seuls utilisateurs autorisés. Le <i>système intermédiaire</i> ne doit pas être situé à l'intérieur du <i>périmètre de sécurité électronique</i>.</p> <p>(Intermediate System)</p> <p>Source : Glossaire des termes en usage dans les normes de fiabilité (NERC)</p>
Systèmes de contrôle des accès physiques	PACS	<p><i>Actifs électroniques</i> qui contrôlent, signalent ou consignent les accès à un ou plusieurs <i>périmètres de sécurité physique</i>, à l'exclusion du matériel et des dispositifs installés localement au <i>périmètre de sécurité physique</i>, tels que les détecteurs de mouvement, les mécanismes de verrouillage électroniques et les lecteurs de carte d'accès.</p> <p>(Physical Access Control Systems)</p> <p>Source : Glossaire des termes en usage dans les normes de fiabilité (NERC)</p>
Systèmes de contrôle ou de surveillance des accès électroniques	EACMS	<p><i>Actifs électroniques</i> qui effectuent le contrôle des accès électroniques ou la surveillance des accès électroniques du ou des <i>périmètres de sécurité électronique</i> ou des <i>systèmes électroniques BES</i>. Cette définition inclut les <i>systèmes intermédiaires</i>.</p> <p>(Electronic Access Control or Monitoring Systems)</p> <p>Source : Glossaire des termes en usage dans les normes de fiabilité (NERC)</p>

3.3. Définitions du glossaire à modifier :

Terme	Acronyme	Définition
Actifs électroniques		Dispositifs électroniques programmables et réseaux de communication , y compris le matériel, les logiciels et les données de ces dispositifs . (Cyber Assets) <small>Source : Glossaire des termes en usage dans les normes de fiabilité (NERC)</small>
Incident de cybersécurité		Tout Acte malveillant ou incident suspect qui : <ul style="list-style-type: none"> compromet ou avait pour but de compromettre le <i>périmètre de sécurité électronique</i> ou le <i>périmètre de sécurité physique</i> d'un actif électronique critique <i>système électronique BES</i>, ou perturbe ou avait pour but de perturber le fonctionnement d'un actif électronique critique <i>système électronique BES</i>. (Cyber Security Incident) <small>Source : Glossaire des termes en usage dans les normes de fiabilité (NERC)</small>
Périmètre de sécurité électronique	ESP	Frontière logique qui entoure le réseau sur lequel les actifs électroniques critiques <i>systèmes électroniques BES</i> sont connectés <u>au moyen d'un protocole routable et pour laquelle les accès sont contrôlés</u> . (Electronic Security Perimeter) <small>Source : Glossaire des termes en usage dans les normes de fiabilité (NERC)</small>
Périmètre de sécurité physique	PSP	Frontière physique qui entoure complètement (sur les six faces) les salles d'ordinateurs, les salles de télécommunications, les centres d'exploitation et les autres endroits hébergeant des actifs électroniques critiques, auxquels l'accès est contrôlé. Frontière physique qui entoure les lieux où se trouvent <u>des actifs électroniques BES, des systèmes électroniques BES ou des systèmes de contrôle ou de surveillance des accès électroniques</u> , et dont l'accès est contrôlé. (Physical Security Perimeter) <small>Source : Glossaire des termes en usage dans les normes de fiabilité (NERC)</small>

3.4. Définitions à retirer du glossaire :

Terme	Acronyme	Définition
Actifs critiques		Installations, systèmes et équipements dont la destruction, la dégradation ou toute autre forme d'indisponibilité affecterait la fiabilité ou l'exploitabilité du <i>système de production-transport d'électricité</i> . (Critical Assets) <small>Source : Glossaire des termes en usage dans les normes de fiabilité (NERC)</small>
Actifs électroniques critiques		<i>Actifs électroniques</i> essentiels à l'exploitation fiable des <i>actifs critiques</i> . (Critical Cyber Assets) <small>Source : Glossaire des termes en usage dans les normes de fiabilité (NERC)</small>

4. MODIFICATIONS AU REGISTRE DES ENTITÉS VISÉES

Dans le format actuellement à l'étude par la Régie de l'énergie, le registre identifie les actifs qui sont critiques au sens de la version 1 des normes CIP. L'évaluation exigée par la norme CIP-002-1 était effectuée par le Coordonnateur pour l'ensemble du Québec. Le nouveau cadre d'application des normes CIP exigeant une identification au niveau des systèmes électroniques, le Coordonnateur ne pourra plus effectuer cette analyse au compte des entités visées. Par ailleurs, la liste des éléments considérés comme critiques est spécifique aux activités de chaque entité et doit être revue et suivie en continu. Cette information ne peut donc pas être consignée dans le registre. Les entités visées par la norme devront donc, en application de la norme CIP-002-5, effectuer leur propre analyse de leurs actifs et leurs systèmes afin de déterminer si ceux-ci sont visés. Par conséquent, le registre devra être modifié pour retirer toute information à l'égard des actifs critiques. D'une part, le champ « Actifs classés critiques aux fins des normes CIP » des fiches des entités sera retiré. D'autre part, la colonne « Actif critique » des annexes pour les installations de transport, de production, de télécommunications et les centres d'exploitation sera également retirée.

À noter que puisque le registre est présentement à l'étude devant la Régie de l'énergie dans le cadre du dossier R-3699-2009, ces modifications seront apportées et déposées à la Régie une fois une décision finale rendue dans ce dossier.

5. NOTE CONCERNANT L'UTILISATION DU TERME « POSTE » DANS LA VERSION FRANÇAISE

La version anglaise des normes utilise les termes « stations » et « substations » pour désigner un ensemble d'équipements de transport situés dans un même emplacement. Le terme « substation » est souvent utilisé dans l'industrie pour désigner un poste qui contient au moins un autotransformateur, tandis que le terme « station » est utilisé pour désigner les postes qui sont exploités à un seul niveau de tension. Cette distinction n'existe pas en français, et le terme « poste » est utilisé pour désigner ces deux types d'installations. La version française des normes utilise donc uniquement le terme « poste » pour traduire les termes « station » et « substation ». Ainsi, la discussion terminologique portant sur l'utilisation de ces termes incluse à la section « Principes directeurs et fondements technique » de la norme CIP-002-5.1 (p. 29) n'a pu être traduite littéralement.

6. APPLICABILITÉ

L'ensemble des normes CIP version 5 (incluant CIP-010-1 et CIP-011-1) visent le même ensemble de fonctions et d'installations.

Fonctions visées :

- Responsable de l'équilibrage
- Distributeur²
- Exploitant d'installation de production
- Propriétaire d'installation de production
- Responsable des échanges
- Coordonnateur de la fiabilité
- Exploitant de réseau de transport
- Propriétaire d'installation de transport

Installations visées :

- Toutes les installations du système de production-transport d'électricité (BES)
- Installations spécifiques pour les *distributeurs*²

Exemptions :

Se référer à la section « Applicabilité » de chaque norme pour les exemptions spécifiques à celles-ci.

7. DISPOSITIONS PARTICULIÈRES POUR LE QUÉBEC (ANNEXES QC)

Les normes CIP visent uniquement les installations du *réseau de transport principal* (RTP) ainsi que les installations spécifiées dans les normes pour les *distributeurs*.

² Voir la section « Applicabilité » des normes CIP pour les détails concernant l'application pour les *distributeurs*.

8. DATES D'ENTRÉE EN VIGUEUR PROPOSÉES

Le délai accordé aux entités américaines lors de l'approbation de ces normes aux États-Unis était de 24 mois pour les *systèmes électroniques BES* catégorisés comme ayant un impact moyen et élevé et de 36 mois pour les systèmes à impact faible. L'entrée en vigueur a été fixée aux 1er avril 2016 et 2017.

Les dates d'entrée en vigueur proposées pour le Québec tiennent compte du fait qu'une entité possède déjà ou non des actifs critiques en vertu de la version 1 des normes CIP adoptées par la Régie :

Entité	Date d'entrée en vigueur proposée au Québec		Justification
	Impacts moyen et élevé	Impact faible	
Entités visées par la version 1 des normes CIP adoptées par la Régie.	2016-04-01	2017-04-01	Uniformisation des pratiques avec les autres juridictions.
Entités exemptées de l'application de la version 1 des normes CIP en vertu des dispositions particulières associées à ces normes.	2017-04-01	2018-04-01	Donner le temps nécessaire à la mise en œuvre de la version 5 des normes CIP aux entités qui étaient exemptées de l'application de la version 1.

9. ÉVALUATION PRÉLIMINAIRE DE L'IMPACT

Cette section présente l'évaluation préliminaire de l'impact monétaire des normes effectuée par le Coordonnateur. À noter que le cadre d'application des normes CIP implique, en premier lieu, l'identification et la catégorisation des systèmes électroniques selon la norme CIP-002. Une entité n'ayant identifié aucun système en vertu de cette norme n'aura pas à se conformer aux normes CIP-003 à CIP-011. L'impact pour ces entités serait donc nul pour ces normes.

Sommaire des impacts

Norme	Implantation			Maintien et suivi de la conformité		
	Faible	Modéré	Élevé	Faible	Modéré	Élevé
CIP-002-5.1		X			X	
CIP-003-5			X			X
CIP-004-5.1			X			X
CIP-005-5			X			X
CIP-006-5			X			X
CIP-007-5			X			X
CIP-008-5			X			X
CIP-009-5			X			X
CIP-010-1			X			X
CIP-011-1			X			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 d'allouer certaines ressources matérielles, humaines ou financières pour implanter, maintenir ou assurer le suivi de la conformité à la norme proposée.
Élevé :	Changement qui nécessite de prévoir et d'allouer des ressources matérielles, humaines ou financières importantes pour planifier et réaliser l'implantation, le maintien ou le suivi de la conformité à la norme proposée.

10. ÉVALUATION FINALE DE L'IMPACT

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