

A. Introduction

1. **Titre :** Cybersécurité — Gestion des changements de configuration et analyses de vulnérabilité
2. **Numéro :** CIP-010-1
3. **Objet :** 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 pourraient entraîner un fonctionnement incorrect ou des instabilités dans le BES.
4. **Applicabilité :**
 - 4.1. **Entités fonctionnelles :** Dans le contexte des exigences de la présente norme, les entités fonctionnelles indiquées ci-après seront appelées collectivement « les entités responsables ». Dans le cas des exigences de cette norme qui visent une entité fonctionnelle particulière ou un sous-ensemble particulier d'entités fonctionnelles, la ou les entités fonctionnelles sont précisées explicitement.
 - 4.1.1 **Responsable de l'équilibrage**
 - 4.1.2 **Distributeur** qui possède un ou plusieurs des *installations*, systèmes et équipements suivants pour la protection ou la remise en charge du BES :
 - 4.1.2.1 Chaque système de délestage de charge en sous-fréquence (DSF) ou de délestage de charge en sous-tension (DST) qui :
 - 4.1.2.1.1 fait partie d'un programme de délestage de *charge* qui est visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou régionale, et
 - 4.1.2.1.2 effectue du délestage automatique de *charge* de 300 MW ou plus par un système de commande commun détenu par l'entité responsable, sans déclenchement par un exploitant humain.
 - 4.1.2.2 Chaque *automatisme de réseau* ou *plan de défense* dans le cas où l'*automatisme de réseau* ou le *plan de défense* est visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou régionale.
 - 4.1.2.3 Chaque *système de protection* applicable au *transport* (excluant les systèmes DSF et DST) dans le cas où le *système de protection* est visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou régionale.
 - 4.1.2.4 Chaque *chemin de démarrage* et groupe d'*éléments* respectant les exigences relatives aux manœuvres initiales depuis une *ressource à démarrage autonome* jusqu'au premier point de raccordement, inclusivement, d'alimentation des services auxiliaires du ou des groupes de production suivants à démarrer.
 - 4.1.3 **Exploitant d'installation de production**

4.1.4 Propriétaire d'installation de production

4.1.5 Coordonnateur des échanges ou Responsable des échanges

4.1.6 Coordonnateur de la fiabilité

4.1.7 Exploitant de réseau de transport

4.1.8 Propriétaire d'installation de transport

4.2. Installations : Dans le contexte des exigences de la présente norme, les *installations*, systèmes et équipements suivants détenus par chaque entité responsable indiquée à la section 4.1 sont ceux auxquels ces exigences sont applicables. Dans le cas des exigences de cette norme qui visent un type particulier d'*installations*, de système ou d'équipements, ou un sous-ensemble d'*installations*, de systèmes ou d'équipements, ceux-ci sont précisés explicitement.

4.2.1 Distributeur : Un ou plusieurs des *installations*, systèmes et équipements suivants détenus par le distributeur pour la protection ou la remise en charge du BES :

4.2.1.1 Chaque système de DSF ou de DST qui :

4.2.1.1.1 fait partie d'un programme de délestage de *charge* qui est visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou régionale, et

4.2.1.1.2 effectue du délestage automatique de *charge* de 300 MW ou plus par un système de commande commun détenu par l'entité responsable, sans déclenchement par un exploitant humain.

4.2.1.2 Chaque *automatisme de réseau* ou *plan de défense* dans le cas où l'*automatisme de réseau* ou le *plan de défense* est visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou régionale.

4.2.1.3 Chaque *système de protection* applicable au *transport* (excluant les systèmes DSF et DST) dans le cas où le *système de protection* est visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou régionale.

4.2.1.4 Chaque *chemin de démarrage* et groupe d'*éléments* respectant les exigences relatives aux manœuvres initiales depuis une *ressource à démarrage autonome* jusqu'au premier point de raccordement, inclusivement, d'alimentation des services auxiliaires du ou des groupes de production suivants à démarrer.

4.2.2 Entités responsables indiquées en 4.1, sauf les distributeurs :

Toutes les *installations* du BES.

4.2.3 Exemptions : Sont exemptés de la norme CIP-010-1 :

4.2.3.1 Les *actifs électroniques* aux *installations* réglementées par la Commission canadienne de sûreté nucléaire ;

- 4.2.3.2** les *actifs électroniques* associés aux réseaux de communication et aux liaisons d'échange de données entre des *périmètres de sécurité électroniques* distincts ;
- 4.2.3.3** les systèmes, structures et composantes régis par la U.S. Nuclear Regulatory Commission en vertu d'un plan de cybersécurité conforme à la norme CFR 10, section 73.54 ;
- 4.2.3.4** dans le cas des distributeurs, les systèmes et les équipements non mentionnés à la section 4.2.1 ci-dessus ;
- 4.2.3.5** les entités responsables qui déterminent qu'elles n'ont pas de *systèmes électroniques BES* catégorisés comme impact élevé ou impact moyen en conformité avec le processus d'identification et de catégorisation de la CIP-002-5.

5. Dates de mise en vigueur

1. **24 mois minimum** – La norme CIP-010-1 entrera en vigueur soit le 1er juillet 2015, soit le premier jour civil du neuvième trimestre civil suivant l'entrée en vigueur de l'ordonnance d'approbation réglementaire appropriée, selon le délai le plus long.
2. Dans les juridictions où aucune approbation réglementaire n'est requise, la norme CIP-010-1 entrera en vigueur le premier jour du neuvième trimestre civil suivant l'approbation par le Conseil d'administration, ou selon les modalités d'approbation prévues par la loi pour les organismes gouvernementaux chargés de la fiabilité électrique (ERO).

6. Contexte :

La norme CIP-010-1 fait partie d'une série de normes CIP sur la cybersécurité. La norme CIP-002-5 exige l'identification et la catégorisation initiales des *systèmes électroniques BES*. Les normes CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1 et CIP-011-1 exigent un niveau minimal de mesures organisationnelles, opérationnelles et administratives pour réduire les risques aux *systèmes électroniques BES*. Cette série de normes CIP est appelée « version 5 des normes CIP sur la cybersécurité ».

La plupart des exigences commencent ainsi : « Chaque entité responsable doit mettre en œuvre un ou plusieurs [processus, plans, etc.] documentés qui correspondent à toutes les parties d'exigence applicables du tableau [référence au tableau]. » Le tableau en référence précise les éléments qui doivent être inclus dans les procédures pour le thème commun de l'exigence.

Le SDT a intégré à la présente norme une reconnaissance à l'effet que certaines exigences ne devraient pas mettre l'accent sur les cas individuels de défaillance comme seul motif d'infraction à la norme. En particulier, le SDT a intégré une approche visant à habilitier l'industrie à identifier, à évaluer et à corriger les lacunes

dans la mise en œuvre de certaines exigences. L'intention est de changer la manière de considérer les infractions dans ces exigences, de sorte qu'il ne s'agisse plus de savoir *si* une lacune existe, mais plutôt d'identifier, d'évaluer et de corriger les lacunes. Ceci est présenté dans ces exigences en modifiant la notion de « mise en œuvre » de la façon suivante :

Chaque entité responsable doit mettre en œuvre, **d'une manière permettant d'identifier, d'évaluer et de corriger les lacunes...**

L'expression « processus documenté » désigne un ensemble de consignes spécifiques à l'entité responsable et visant à produire un résultat particulier. Cette expression n'implique pas de structure de nommage ou d'approbation au-delà de la formulation des exigences. Une entité devrait inclure autant qu'elle le juge nécessaire à leurs processus documentés, pourvu que les exigences pertinentes soient couvertes. Les processus documentés eux-mêmes n'ont pas à intégrer la démarche « détecter, évaluer et corriger les lacunes » décrite au paragraphe précédent, car cette démarche est liée à la manière de mettre en œuvre les processus documentés et pourrait être réalisée par d'autres mesures de contrôle ou de gestion de la conformité.

Les mots « programme » et « plan » sont parfois utilisés au lieu de « processus documenté », lorsque cela a du sens et est communément compris. Par exemple, les processus documentés qui décrivent une réponse sont généralement appelés « plans » (plan d'action en cas d'incident, plan de rétablissement, etc.). De plus, un plan de sécurité peut décrire une approche comportant plusieurs procédures couvrant un thème étendu.

De même, le mot « programme » peut désigner la mise en œuvre générale par l'organisation de ses politiques, plans et procédures portant sur un thème donné. Le programme d'évaluation des risques liés au personnel et le programme de formation du personnel sont un exemple trouvé dans les normes. La mise en œuvre complète des normes CIP sur la cybersécurité pourrait aussi être appelée « programme ». Toutefois, les mots « programme » et « plan » n'impliquent pas d'exigences supplémentaires au-delà de ce qui est indiqué dans les normes.

Les entités responsables peuvent mettre en œuvre des moyens communs qui répondent aux besoins de plusieurs *systèmes électroniques BES* à impact élevé et moyen. Par exemple, un même programme de formation pourrait répondre aux exigences en formation du personnel de plusieurs *systèmes électroniques BES*.

Les mesures présentent des exemples de pièces justificatives pour montrer la documentation et la mise en œuvre de l'exigence. Ces mesures servent à fournir des conseils aux entités sur ce qui peut constituer des dossiers de conformité acceptables et ne devraient pas être considérées comme une liste exhaustive.

Dans l'ensemble des normes, sauf indication particulière, les éléments présentés à la section Exigences et mesures sous forme de liste à puces sont liés par l'opérateur « ou », et les éléments présentés sous forme de liste numérotée sont liés par l'opérateur « et ».

Plusieurs références de la section Applicabilité utilisent un seuil de 300 MW pour les systèmes DSF et DST. Ce seuil particulier de 300 MW pour les systèmes DSF et DST provient de la version 1 des normes CIP sur la cybersécurité. Le seuil demeure à 300 MW puisqu'il concerne spécifiquement les systèmes DST et DSF, qui constituent des efforts de dernier recours pour sauver le *système de production-transport d'électricité*. Un examen des tolérances de systèmes DSF définies dans les normes de fiabilité régionales pour les exigences des programmes de DSF à ce jour indique que la valeur historique de 300 MW représente une valeur de seuil adéquate et raisonnable pour les tolérances d'exploitation admissibles des systèmes DSF.

Colonnes « Systèmes visés » des tableaux

Chaque tableau comporte une colonne intitulée « Systèmes visés » qui définit plus précisément les systèmes auxquels s'applique l'exigence. Le SDT CSO706 a adapté ce concept à partir du cadre de gestion des risques du National Institute of Standards and Technology (NIST) en vue d'établir une méthode d'application des exigences qui tient compte plus adéquatement de l'impact et des caractéristiques de connectivité. La colonne « Systèmes visés » repose sur les conventions suivantes :

- **Systèmes électroniques BES à impact élevé** – Désigne les *systèmes électroniques BES* classés dans la catégorie « impact élevé », conformément aux processus d'identification et de catégorisation de la norme CIP-002-5.
- **Systèmes électroniques BES à impact moyen** – Désigne les *systèmes électroniques BES* classés dans la catégorie « impact moyen », conformément aux processus d'identification et de catégorisation de la norme CIP-002-5.
- **Systèmes de contrôle ou de surveillance des accès électroniques (EACMS)** – Désigne tout *système de contrôle ou de surveillance des accès électroniques* associé à un *système électronique BES* à impact élevé ou moyen visé. Exemples non limitatifs : pare-feu, serveurs d'authentification, et systèmes de surveillance de registre d'événement et d'alerte.
- **Systèmes de contrôle des accès physiques (PACS)** – Désigne tout *système de contrôle des accès physiques* associé à un *système électronique BES* à impact élevé ou moyen visé à *connectivité externe routable*.
- **Actifs électroniques protégés (PCA)** – Désigne tout *actif électronique protégé* associé à un *système électronique BES* à impact élevé ou moyen visé.

B. Exigences et mesures

- E1.** Chaque entité responsable doit mettre en œuvre, d’une manière permettant d’identifier, d’évaluer et de corriger les lacunes, un ou plusieurs processus documentés qui, collectivement, comprennent toutes les parties d’exigence applicables du tableau E1 (CIP-010-1) – Gestion des changements de configuration. [*Facteur de risque de la non-conformité : moyen*] [*Horizon : planification de l’exploitation*].
- M1.** Les pièces justificatives doivent comprendre chacun des processus documentés applicables qui, collectivement, comprennent toutes les parties d’exigence applicables du tableau E1 (CIP-010-1) – Gestion des changements de configuration, ainsi que des pièces justificatives additionnelles attestant la mise en œuvre, selon la colonne Mesures du tableau.

Tableau E1 (CIP-010-1) – Gestion des changements de configuration			
Partie	Systèmes visés	Exigences	Mesures
1.1	<p><i>Systèmes électroniques BES à impact élevé et leurs :</i></p> <ol style="list-style-type: none"> 1. EACMS associés ; 2. PACS associés ; et 3. PCA associés. <p><i>Systèmes électroniques BES à impact moyen et leurs :</i></p> <ol style="list-style-type: none"> 1. EACMS associés ; 2. PACS associés ; et 3. PCA associés. 	<p>Établir une configuration de référence, individuellement ou par groupe, qui doit comprendre les points suivants :</p> <ol style="list-style-type: none"> 1.1.1. système(s) d’exploitation (y compris la version), ou microprogramme en l’absence de système d’exploitation indépendant ; 1.1.2. tout logiciel d’application du commerce ou logiciel ouvert (y compris la version) installé intentionnellement ; 1.1.3. tout logiciel personnalisé installé ; 1.1.4. tout port logique accessible par le réseau ; et 1.1.5. toute rustine de sécurité appliquée. 	<p>Exemples non limitatifs de pièces justificatives :</p> <ul style="list-style-type: none"> • feuille de calcul indiquant les éléments de configuration de référence requis pour chaque <i>actif électronique</i>, individuellement ou par groupe ; ou • enregistrement dans un système de gestion d’actifs indiquant les éléments de configuration de référence requis pour chaque <i>actif électronique</i>, individuellement ou par groupe.

Tableau E1 (CIP-010-1) – Gestion des changements de configuration			
Partie	Systèmes visés	Exigences	Mesures
1.2	<p><i>Systèmes électroniques BES à impact élevé et leurs :</i></p> <ol style="list-style-type: none"> 1. EACMS associés ; 2. PACS associés ; et 3. PCA associés. <p><i>Systèmes électroniques BES à impact moyen et leurs :</i></p> <ol style="list-style-type: none"> 1. EACMS associés ; 2. PACS associés ; et 3. PCA associés. 	Autoriser et documenter tout changement par rapport à la configuration de référence existante.	<p>Exemples non limitatifs de pièces justificatives :</p> <ul style="list-style-type: none"> • fiche de demande de changement et autorisation électronique correspondante (accordée par une personne ou un groupe dûment habilité), pour chaque changement, dans un système de gestion des changements ; ou • documentation attestant que le changement a été effectué conformément à l'exigence.
1.3	<p><i>Systèmes électroniques BES à impact élevé et leurs :</i></p> <ol style="list-style-type: none"> 1. EACMS associés ; 2. PACS associés ; et 3. PCA associés. <p><i>Systèmes électroniques BES à impact moyen et leurs :</i></p> <ol style="list-style-type: none"> 1. EACMS associés ; 2. PACS associés ; et 3. PCA associés. 	Pour tout changement par rapport à la configuration de référence existante, mettre à jour la configuration de référence dans les 30 jours civils suivant l'exécution du changement.	Exemple non limitatif de pièce justificative : documentation de la configuration de référence avec mise à jour datée d'au plus 30 jours civils après la date d'exécution du changement.

Tableau E1 (CIP-010-1) – Gestion des changements de configuration			
Partie	Systèmes visés	Exigences	Mesures
1.4	<p><i>Systèmes électroniques BES à impact élevé et leurs :</i></p> <ol style="list-style-type: none"> 1. EACMS associés ; 2. PACS associés ; et 3. PCA associés. <p><i>Systèmes électroniques BES à impact moyen et leurs :</i></p> <ol style="list-style-type: none"> 1. EACMS associés ; 2. PACS associés ; et 3. PCA associés. 	<p>Pour tout changement par rapport à la configuration de référence existante :</p> <ol style="list-style-type: none"> 1.4.1. avant le changement, déterminer les mécanismes de cybersécurité de CIP-005 et CIP-007 qui pourraient être touchés par le changement ; 1.4.2. après le changement, vérifier que les mécanismes de cybersécurité déterminés en 1.4.1 ne sont pas altérés ; et 1.4.3. documenter les résultats de la vérification. 	<p>Exemple non limitatif de pièce justificative : liste de mécanismes de cybersécurité vérifiés ou mis à l'essai, avec résultats d'essai datés.</p>

Tableau E1 (CIP-010-1) – Gestion des changements de configuration			
Partie	Systèmes visés	Exigences	Mesures
1.5	<i>Systèmes électroniques BES à impact élevé.</i>	<p>Lorsque techniquement faisable, pour chaque changement par rapport à la configuration de référence existante :</p> <p>1.5.1. avant de mettre en œuvre un changement dans l'environnement de production, mettre à l'essai le changement dans un environnement d'essai ou mettre à l'essai le changement dans un environnement de production où l'essai est effectué d'une manière qui réduit au minimum les effets adverses, en simulant la configuration de référence de manière à s'assurer que les mécanismes de cybersécurité de CIP-005 et CIP-007 ne sont pas altérés ; et</p> <p>1.5.2. documenter les résultats des essais et, si un environnement d'essai est utilisé, les différences entre celui-ci et l'environnement de production, y compris la description des mesures visant à tenir compte des différences de fonctionnement entre les environnements d'essai et de production.</p>	Exemple non limitatif de pièce justificative : liste des mécanismes de cybersécurité mis à l'essai avec résultats d'essai concluants, liste de différences entre les environnements d'essai et de production et description des mesures visant à tenir compte des différences de fonctionnement, y compris la date de l'essai.

- E2.** Chaque entité responsable doit mettre en œuvre, d’une manière permettant d’identifier, d’évaluer et de corriger les lacunes, un ou plusieurs processus documentés qui, collectivement, comprennent toutes les parties d’exigence applicables du tableau E2 (CIP-010-1) – Surveillance de configuration. *[Facteur de risque de la non-conformité : moyen] [Horizon : planification de l'exploitation]*.
- M2.** Les pièces justificatives doivent comprendre chacun des processus documentés applicables qui, collectivement, comprennent toutes les parties d’exigence applicables du tableau E2 (CIP-010-1) – Surveillance de configuration, ainsi que des pièces justificatives additionnelles attestant la mise en œuvre, selon la colonne Mesures du tableau.

Tableau E2 (CIP-010-1) – Surveillance de la configuration			
Partie	Systèmes visés	Exigences	Mesures
2.1	<i>Systèmes électroniques BES à impact élevé et leurs :</i> <ol style="list-style-type: none"> 1. EACMS associés ; et 2. PCA associés. 	Surveiller au moins une fois tous les 35 jours civils les changements dans la configuration de référence (tel que décrit à l’exigence E1, partie 1.1). Documenter tout changement non autorisé détecté et faire enquête.	Exemples non limitatifs de pièces justificatives : registres d’un système de surveillance de configuration et dossiers d’enquête pour tout changement non autorisé détecté.

- E3.** Chaque entité responsable doit mettre en œuvre un ou plusieurs processus documentés qui, collectivement, comprennent toutes les parties d’exigence applicables du tableau E3 (CIP-010-1) – Analyses de vulnérabilité. *[Facteur de risque de la non-conformité : moyen] [Horizon : planification à long terme et planification de l'exploitation]*
- M3.** Les pièces justificatives doivent comprendre chacun des processus documentés applicables qui, collectivement, comprennent toutes les parties d’exigence applicables du tableau E3 (CIP-010-1) – Analyses de vulnérabilité, ainsi que des pièces justificatives additionnelles attestant la mise en œuvre, selon la colonne Mesures du tableau.

Tableau E3 (CIP-010-1) – Analyses de vulnérabilité			
Partie	Systèmes visés	Exigences	Mesures
3.1	<p><i>Systèmes électroniques BES à impact élevé et leurs :</i></p> <ol style="list-style-type: none"> 1. EACMS associés ; 2. PACS associés ; et 3. PCA associés. <p><i>Systèmes électroniques BES à impact moyen et leurs :</i></p> <ol style="list-style-type: none"> 1. EACMS associés ; 2. PACS associés ; et 3. PCA associés. 	Au moins tous les 15 mois civils, effectuer une analyse de vulnérabilité sur papier ou active.	<p>Exemples non limitatifs de pièces justificatives :</p> <ul style="list-style-type: none"> • document indiquant la date de l'analyse (effectuée au moins une fois tous les 15 mois civils), les mécanismes évalués pour chaque <i>système électronique BES</i> et la méthode d'analyse ; ou • document indiquant la date de l'analyse et le résultat produit par tout outil utilisé pour l'analyse.

Tableau E3 (CIP-010-1) – Analyses de vulnérabilité			
Partie	Systèmes visés	Exigences	Mesures
3.2	<i>Systèmes électroniques BES à impact élevé.</i>	<p>Lorsque techniquement faisable, au moins une fois tous les 36 mois civils :</p> <p>3.2.1 effectuer une analyse de vulnérabilité active dans un environnement d’essai, ou effectuer une analyse de vulnérabilité active dans un environnement de production où l’essai est réalisé d’une manière qui réduit au minimum les effets adverses, en simulant la configuration de référence du <i>système électronique BES</i> dans un environnement de production ; et</p> <p>3.2.2 documenter les résultats des essais et, si un environnement d’essai a été utilisé, les différences entre l’essai et l’environnement de production, y compris la description des mesures visant à tenir compte des différences de fonctionnement entre les environnements d’essai et de production.</p>	<p>Exemples non limitatifs de pièces justificatives : document indiquant la date de l’analyse (effectuée au moins une fois tous les 36 mois civils), résultat produit par les outils utilisés pour effectuer l’analyse et liste des différences entre les environnements de production et d’essai, avec explications sur la prise en compte des différences dans l’analyse.</p>

Tableau E3 (CIP-010-1) – Analyses de vulnérabilité			
Partie	Systèmes visés	Exigences	Mesures
3.3	<p><i>Systèmes électroniques BES à impact élevé et leurs :</i></p> <ol style="list-style-type: none"> 1. EACMS associés ; 2. PCA associés. 	<p>Avant d'ajouter un <i>actif électronique</i> visé à un environnement de production, effectuer une analyse de vulnérabilité active du nouvel <i>actif électronique</i>, sauf dans des <i>circonstances CIP exceptionnelles</i> ou pour un remplacement à l'identique d'un <i>actif électronique</i> existant par un autre dont la configuration de référence simule celle de l'<i>actif électronique</i> remplacé ou d'un autre <i>actif électronique</i> existant.</p>	<p>Exemples non limitatifs de pièces justificatives : document indiquant la date de l'analyse (effectuée avant la mise en service du nouvel <i>actif électronique</i>) et le résultat produit par les outils utilisés pour l'analyse.</p>
3.4	<p><i>Systèmes électroniques BES à impact élevé et leurs :</i></p> <ol style="list-style-type: none"> 1. EACMS associés ; 2. PACS associés ; et 3. PCA associés. <p><i>Systèmes électroniques BES à impact moyen et leurs :</i></p> <ol style="list-style-type: none"> 1. EACMS associés ; 2. PACS associés ; et 3. PCA associés. 	<p>Documenter les résultats des analyses effectuées conformément aux parties 3.1, 3.2 et 3.3 ainsi que le plan d'action visant à corriger ou à atténuer les vulnérabilités identifiées lors des analyses, en précisant la date prévue d'achèvement du plan d'action et l'état d'exécution de toute mesure de correction ou d'atténuation.</p>	<p>Exemples non limitatifs de pièces justificatives : document donnant les résultats de l'examen ou de l'analyse, liste des mesures prises, dates proposées d'achèvement du plan d'action et dossier de l'état d'exécution des mesures à prendre (procès-verbaux de réunion d'étape, mises à jour dans un système de bons de travail ou suivi des mesures au moyen d'une feuille de calcul).</p>

C. Conformité

1. Processus de surveillance de la conformité :

1.1. Responsable de la surveillance de l'application des normes :

L'entité régionale joue le rôle de responsable de la surveillance de l'application des normes (CEA), à moins que l'entité concernée soit détenue, exploitée ou contrôlée par l'entité régionale. Dans de tels cas, le rôle de CEA est confié à l'ERO, à une entité régionale approuvée par la FERC ou à un autre organisme gouvernemental pertinent.

1.2. Conservation des pièces justificatives :

Les périodes de conservation des pièces justificatives indiquées ci-après établissent la durée pendant laquelle une entité est tenue de conserver certaines pièces justificatives afin de démontrer sa conformité. Dans les cas où la période de conservation des pièces justificatives indiquée est plus courte que le temps écoulé depuis le dernier audit, le CEA peut demander à l'entité de fournir d'autres pièces justificatives pour montrer qu'elle était conforme pendant la période complète écoulée depuis le dernier audit.

L'entité responsable doit conserver les données ou pièces justificatives attestant de sa conformité de la façon indiquée ci-après, à moins que son CEA lui demande de conserver certains documents plus longtemps dans le cadre d'une enquête :

- Chaque entité responsable doit conserver des pièces justificatives pour chaque exigence de la présente norme pendant trois années civiles.
- Si une entité responsable est jugée non conforme, elle doit conserver l'information relative à cette non-conformité jusqu'à ce que les correctifs aient été appliqués et approuvés ou pendant la période indiquée ci-dessus, selon la durée la plus longue.
- Le CEA doit conserver les derniers dossiers d'audit ainsi que tous les dossiers d'audit demandés et soumis par la suite.

1.3. Processus de surveillance et d'évaluation de la conformité :

- Audits de conformité
- Déclarations sur la conformité
- Contrôles ponctuels
- Enquêtes sur les non-conformités
- Déclarations volontaires
- Plaintes

1.4. Autres informations sur la conformité :

- Aucun

2. Tableau des éléments de conformité

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-010-1)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
E1	Planification de l'exploitation	Moyen	<p>L'entité responsable a documenté et mis en œuvre un ou des processus de gestion des changements de configuration qui comprend seulement quatre des éléments de référence exigés en 1.1.1 à 1.1.5. (1.1)</p> <p>OU</p> <p>L'entité responsable a documenté et mis en œuvre un ou des processus de gestion des changements de configuration qui comprend tous les éléments de référence exigés en 1.1.1 à 1.1.5 et a identifié les lacunes, mais elle n'a pas évalué et corrigé les lacunes. (1.1)</p>	<p>L'entité responsable a documenté et mis en œuvre un ou des processus de gestion des changements de configuration qui comprend seulement trois des éléments de référence exigés en 1.1.1 à 1.1.5. (1.1)</p> <p>OU</p> <p>L'entité responsable a documenté et mis en œuvre un ou des processus de gestion des changements de configuration qui comprend quatre des éléments de référence exigés en 1.1.1 à 1.1.5 et a identifié les lacunes, mais elle n'a pas évalué et corrigé les lacunes. (1.1)</p>	<p>L'entité responsable a documenté et mis en œuvre un ou des processus de gestion des changements de configuration qui comprend seulement deux des éléments de référence exigés en 1.1.1 à 1.1.5. (1.1)</p> <p>OU</p> <p>L'entité responsable a documenté et mis en œuvre un ou des processus de gestion des changements de configuration qui comprend trois des éléments de référence exigés en 1.1.1 à 1.1.5 et a identifié les lacunes, mais elle n'a pas évalué et corrigé les lacunes. (1.1)</p>	<p>L'entité responsable n'a documenté ou mis en œuvre aucun processus de gestion des changements de configuration. (E1)</p> <p>OU</p> <p>L'entité responsable a documenté et mis en œuvre un ou des processus de gestion des changements de configuration qui comprend seulement un des éléments de référence exigés en 1.1.1 à 1.1.5. (1.1)</p> <p>OU</p> <p>L'entité responsable a documenté et mis en œuvre un ou des processus de gestion des changements de configuration qui</p>

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-010-1)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
			<p>OU</p> <p>L'entité responsable a documenté et mis en œuvre un ou des processus de gestion des changements de configuration qui comprend tous les éléments de référence exigés en 1.1.1 à 1.1.5, mais elle n'a pas identifié, évalué et corrigé les lacunes. (1.1)</p> <p>OU</p> <p>L'entité responsable a un ou des processus pour réaliser les étapes de 1.4.1 et 1.4.2 pour un ou des changements par rapport à la configuration de référence existante et a identifié les lacunes dans la documentation</p>	<p>OU</p> <p>L'entité responsable a documenté et mis en œuvre un ou des processus de gestion des changements de configuration qui comprend quatre des éléments de référence exigés en 1.1.1 à 1.1.5, mais elle n'a pas identifié, évalué et corrigé les lacunes. (1.1)</p> <p>OU</p> <p>L'entité responsable a un ou des processus pour déterminer les mécanismes de sécurité requis dans CIP-005 et CIP-007 qui pourraient être touchés par un ou des changements par rapport à la configuration de</p>	<p>OU</p> <p>L'entité responsable a documenté et mis en œuvre un ou des processus de gestion des changements de configuration qui comprend trois des éléments de référence exigés en 1.1.1 à 1.1.5, mais elle n'a pas identifié, évalué et corrigé les lacunes. (1.1)</p> <p>OU</p> <p>L'entité responsable a un ou des processus qui exigent l'autorisation et la documentation des changements par rapport à la configuration de référence existante et a identifié les lacunes, mais elle n'a pas évalué</p>	<p>comprend deux des éléments de référence exigés en 1.1.1 à 1.1.5 ou moins et a identifié les lacunes, mais elle n'a pas évalué et corrigé les lacunes. (1.1)</p> <p>OU</p> <p>L'entité responsable a documenté et mis en œuvre un ou des processus de gestion des changements de configuration qui comprend deux des éléments de référence exigés en 1.1.1 à 1.1.5 ou moins, mais elle n'a pas identifié, évalué et corrigé les lacunes. (1.1)</p> <p>OU</p> <p>L'entité responsable n'a pas un ou des processus qui exigent</p>

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-010-1)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
			<p>de vérification, mais elle n'a pas évalué ou corrigé les lacunes. (1.4.3).</p> <p>OU</p> <p>L'entité responsable a un ou des processus pour réaliser les étapes de 1.4.1 et 1.4.2 pour un ou des changements par rapport à la configuration de référence existante, mais elle n'a pas identifié, évalué ou corrigé les lacunes dans la documentation de vérification. (1.4.3).</p>	<p>référence existante et a identifié les lacunes dans la détermination des mécanismes de sécurité affectés, mais elle n'a pas évalué ou corrigé les lacunes. (1.4.1)</p> <p>OU</p> <p>L'entité responsable a un ou des processus pour déterminer les mécanismes de sécurité requis dans CIP-005 et CIP-007 qui pourraient être touchés par un ou des changements par rapport à la configuration de référence existante, mais elle n'a pas identifié, évalué ou corrigé les lacunes dans la détermination des mécanismes de sécurité affectés.</p>	<p>ou corrigé les lacunes. (1.2)</p> <p>OU</p> <p>L'entité responsable a un ou des processus qui exigent l'autorisation et la documentation des changements par rapport à la configuration de référence existante, mais elle n'a pas identifié, évalué ou corrigé les lacunes. (1.2)</p> <p>OU</p> <p>L'entité responsable a un ou des processus pour mettre à jour la configuration de référence dans les 30 jours civils suivant l'exécution de changements par rapport à la</p>	<p>l'autorisation et la documentation des changements par rapport à la configuration de référence existante. (1.2)</p> <p>OU</p> <p>L'entité responsable n'a pas un ou des processus pour mettre à jour la configuration de référence dans les 30 jours civils suivant l'exécution de changements par rapport à la configuration de référence existante. (1.3)</p> <p>OU</p> <p>L'entité responsable a un ou des processus pour déterminer les mécanismes de sécurité requis dans</p>

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-010-1)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
				(1.4.1)	<p>configuration de référence existante et a identifié les lacunes, mais elle n'a pas évalué ou corrigé les lacunes. (1.3)</p> <p>OU</p> <p>L'entité responsable a un ou des processus pour mettre à jour la configuration de référence dans les 30 jours civils suivant l'exécution de changements par rapport à la configuration de référence existante, mais elle n'a pas identifié, évalué ou corrigé les lacunes. (1.3)</p> <p>OU</p> <p>L'entité responsable a un ou des processus pour vérifier que les</p>	<p>CIP-005 et CIP-007 qui pourraient être touchés par un ou des changements par rapport à la configuration de référence existante, mais elle n'a pas vérifié et documenté que les mécanismes requis n'étaient pas affectés négativement suivant le changement. (1.4.2 et 1.4.3)</p> <p>OU</p> <p>L'entité responsable n'a pas de processus pour mettre à l'essai les changements dans un environnement qui simule la configuration de référence avant de mettre en œuvre un changement par rapport à la configuration de</p>

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-010-1)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
					<p>mécanismes de sécurité requis dans CIP-005 et CIP-007 ne sont pas affectés négativement par un ou des changements par rapport à la configuration de référence existante et a identifié les lacunes dans les mécanismes requis, mais elle n'a pas évalué ou corrigé les lacunes. (1.4.2)</p> <p>OU</p> <p>L'entité responsable a un ou des processus pour vérifier que les mécanismes de sécurité requis dans CIP-005 et CIP-007 ne sont pas affectés négativement par un ou des changements par rapport à la configuration de référence existante,</p>	<p>référence. (1.5.1)</p> <p>OU</p> <p>L'entité responsable n'a pas de processus pour documenter les résultats de l'essai et, si un environnement d'essai est utilisé, pour documenter les différences entre les environnements d'essai et de production. (1.5.2)</p>

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-010-1)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
					<p>mais elle n'a pas identifié, évalué ou corrigé les lacunes dans les mécanismes requis. (1.4.2)</p> <p>OU</p> <p>L'entité responsable a un processus pour mettre à l'essai les changements dans un environnement qui simule la configuration de référence avant de mettre en œuvre un changement par rapport à la configuration de référence, et a identifié les lacunes, mais elle n'a pas évalué ou corrigé les lacunes. (1.5.1)</p> <p>OU</p> <p>L'entité responsable a un processus pour mettre à l'essai les</p>	

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-010-1)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
					<p>changements dans un environnement qui simule la configuration de référence avant de mettre en œuvre un changement par rapport à la configuration de référence, mais elle n'a pas identifié, évalué ou corrigé les lacunes. (1.5.1)</p> <p>OU</p> <p>L'entité responsable a un processus pour documenter les résultats de l'essai et, si un environnement d'essai est utilisé, pour documenter les différences entre les environnements d'essai et de production, et a identifié les lacunes, mais elle n'a pas évalué ou corrigé les lacunes.</p>	

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-010-1)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
					(1.5.2) OU L'entité responsable a un processus pour documenter les résultats de l'essai et, si un environnement d'essai est utilisé, pour documenter les différences entre les environnements d'essai et de production, mais elle n'a pas identifié, évalué ou corrigé les lacunes. (1.5.2)	
E2	Planification de l'exploitation	Moyen	Sans objet	Sans objet	Sans objet	L'entité responsable n'a pas documenté ou mis en œuvre un ou des processus pour surveiller, enquêter et documenter les changements non autorisés détectés à la référence au moins une fois tous les 35

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-010-1)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
						<p>jours civils. (2.1)</p> <p>OU</p> <p>L'entité responsable a documenté et mis en œuvre un ou des processus pour surveiller, enquêter et documenter les changements non autorisés détectés à la référence au moins une fois tous les 35 jours civils et a identifié les lacunes, mais elle n'a pas évalué ou corrigé les lacunes. (2.1)</p> <p>OU</p> <p>L'entité responsable a documenté et mis en œuvre un ou des processus pour surveiller, enquêter et documenter les changements non autorisés détectés à la</p>

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-010-1)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
						référence au moins une fois tous les 35 jours civils, mais elle n'a pas identifié, évalué ou corrigé les lacunes. (2.1)
E3	Planification à long terme et planification de l'exploitation	Moyen	<p>L'entité responsable a mis en œuvre un ou plusieurs processus documentés d'analyse de vulnérabilité pour chacun de ses <i>systèmes électroniques BES</i> visés, mais elle a effectué une analyse de vulnérabilité plus de 15 mois, mais en moins de 18 mois suivant la dernière analyse de l'un de ses <i>systèmes électroniques BES</i> visés. (3.1)</p> <p>OU</p> <p>L'entité responsable a mis en œuvre un ou plusieurs processus</p>	<p>L'entité responsable a mis en œuvre un ou plusieurs processus documentés d'analyse de vulnérabilité pour chacun de ses <i>systèmes électroniques BES</i> visés, mais elle a effectué une analyse de vulnérabilité plus de 18 mois, mais en moins de 21 mois suivant la dernière analyse de l'un de ses <i>systèmes électroniques BES</i> visés. (3.1)</p> <p>OU</p> <p>L'entité responsable a mis en œuvre un ou plusieurs processus</p>	<p>L'entité responsable a mis en œuvre un ou plusieurs processus documentés d'analyse de vulnérabilité pour chacun de ses <i>systèmes électroniques BES</i> visés, mais elle a effectué une analyse de vulnérabilité plus de 21 mois, mais en moins de 24 mois suivant la dernière analyse de l'un de ses <i>systèmes électroniques BES</i> visés. (3.1)</p> <p>OU</p> <p>L'entité responsable a mis en œuvre un ou plusieurs processus</p>	<p>L'entité responsable n'a mis en œuvre aucun processus d'analyse de vulnérabilité pour un de ses <i>systèmes électroniques BES</i> visés. (E3)</p> <p>OU</p> <p>L'entité responsable a mis en œuvre un ou plusieurs processus documentés d'analyse de vulnérabilité pour chacun de ses <i>systèmes électroniques BES</i> visés, mais elle a effectué une analyse de vulnérabilité plus de 24 mois suivant la</p>

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-010-1)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
			documentés d'analyse de vulnérabilité active pour les systèmes visés, mais elle a effectué une analyse de vulnérabilité active plus de 36 mois, mais en moins de 39 mois suivant la dernière analyse active de l'un de ses <i>systèmes électroniques BES</i> visés. (3.2)	documentés d'analyse de vulnérabilité active pour les systèmes visés, mais elle a effectué une analyse de vulnérabilité active plus de 39 mois, mais en moins de 42 mois suivant la dernière analyse active de l'un de ses <i>systèmes électroniques BES</i> visés. (3.2)	documentés d'analyse de vulnérabilité active pour les systèmes visés, mais elle a effectué une analyse de vulnérabilité active plus de 42 mois, mais en moins de 45 mois suivant la dernière analyse active de l'un de ses <i>systèmes électroniques BES</i> visés. (3.2)	<p>dernière analyse de l'un de ses <i>systèmes électroniques BES</i> visés. (3.1)</p> <p>OU</p> <p>L'entité responsable a mis en œuvre un ou plusieurs processus documentés d'analyse de vulnérabilité active pour les systèmes visés, mais elle a effectué une analyse de vulnérabilité active plus de 45 mois suivant la dernière analyse active de l'un de ses <i>systèmes électroniques BES</i> visés. (3.2)</p> <p>OU</p> <p>L'entité responsable a mis en œuvre et documenté un ou plusieurs processus d'analyse de vulnérabilité pour</p>

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-010-1)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
						<p>chacun de ses <i>systèmes électroniques BES</i> visés, mais elle n'a pas effectué l'analyse de vulnérabilité active d'une manière qui simule une configuration de référence existante de ses <i>systèmes électroniques BES</i> visés. (3.3)</p> <p>OU</p> <p>L'entité responsable a mis en œuvre un ou plusieurs processus documentés d'analyse de vulnérabilité pour chacun de ses <i>systèmes électroniques BES</i> visés, mais elle n'a pas documenté les résultats des analyses de vulnérabilité, les plans d'action pour remédier ou mitiger les vulnérabilités relevées</p>

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-010-1)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
						dans les analyses, la date planifiée d'achèvement du plan d'action et l'état d'exécution des plans de mitigation. (3.4)

D. Différences régionales

Aucune.

E. Interprétations

Aucune.

F. Documents connexes

Aucun.

Principes directeurs et fondements techniques

Section 4 – Portée de l'applicabilité des normes CIP sur la cybersécurité

La section « 4 Applicabilité » des normes présente de l'information importante pour aider les entités responsables à déterminer la portée d'application des exigences CIP sur la cybersécurité.

La section « 4.1. Entités fonctionnelles » est la liste des entités fonctionnelles de la NERC auxquelles s'applique la norme. Si l'entité est enregistrée au titre d'une ou de plusieurs des entités fonctionnelles énumérées à la section 4.1, alors les normes CIP sur la cybersécurité de la NERC s'appliquent. Il est à noter qu'il y a une restriction à la section 4.1 qui limite l'applicabilité dans le cas des distributeurs à ceux qui détiennent certains types de systèmes et d'équipements énumérés à la section 4.2.

La section « 4.2. Installations » définit la portée des installations, systèmes et équipements détenus par l'entité responsable qualifiée à la section 4.1, qui est visée par les exigences de la norme. Tel qu'indiqué à la section exemption 4.2.3.5, cette norme ne s'applique pas aux entités responsables qui n'ont pas de systèmes électroniques BES à impact élevé ou à impact moyen selon la catégorisation de la CIP-002- 5. Outre l'ensemble des installations du BES, des centres de contrôle et des autres systèmes et équipements, la liste comprend l'ensemble des systèmes et équipements détenus par les distributeurs. Bien que le terme « installations » du glossaire de la NERC comprenne déjà la caractéristique BES, l'utilisation additionnelle du terme « BES » vise ici à renforcer la portée d'applicabilité pour ces installations, en particulier dans cette section sur l'applicabilité. Cela établit quels sont les installations, systèmes et équipements visés par les normes.

Exigence E1 :

Configuration de référence

L'idée d'établir une configuration de référence pour un *actif électronique* vise à clarifier la formulation des exigences énoncées dans les versions précédentes des normes CIP. Tout changement apporté à un élément de la configuration de référence d'un *actif électronique* visé constitue le déclencheur du processus de gestion des changements par l'entité concernée.

Les configurations de référence dans la norme CIP-010 comportent cinq éléments : le système d'exploitation ou le microprogramme ; les logiciels d'application du commerce ou les logiciels ouverts ; les logiciels personnalisés ; les ports logiques accessibles par le réseau ; et les rustines de sécurité. L'information sur le système d'exploitation précise le nom et la version du logiciel en cours d'utilisation dans l'*actif électronique*. En l'absence de système d'exploitation indépendant (par exemple pour un relais de protection), l'information sur le microprogramme devrait être précisé. Les logiciels d'application du commerce ou les logiciels ouverts sont ceux qui ont été installés intentionnellement dans l'*actif électronique*. L'utilisation du mot « intentionnellement » vise à préciser que seuls les logiciels jugés nécessaires pour les *actifs électroniques* doivent être inclus dans la configuration de référence. Le SDT ne souhaite pas que soient inclus dans cette configuration les calepins, calepines, les DLL, les pilotes de

périphérique ou d'autres applications compris dans un système d'exploitation du commerce ou distribués à titre de logiciel ouvert. Les logiciels personnalisés installés peuvent comprendre des scripts programmés pour des fonctions locales de l'entité ou d'autres programmes créés en vue d'une tâche ou fonction spécifique à l'entité. Dans le cas d'un logiciel supplémentaire qui a été installé intentionnellement et qui n'est ni un logiciel du commerce ni un logiciel libre, ce logiciel pourrait être considéré comme un logiciel personnalisé. Si un dispositif a besoin de communiquer avec un autre dispositif à l'extérieur du réseau, les communications doivent être limitées aux seuls dispositifs qui doivent communiquer, conformément à la norme CIP-007-5. Les ports accessibles doivent être indiqués dans la configuration de référence. Les rustines de sécurité appliquées doivent comprendre toutes les rustines antérieures et courantes appliquées sur l'actif électronique. Alors que l'exigence E2.1 de la norme CIP-007-5 stipule que les entités doivent se tenir informées des rustines de sécurité, les évaluer et les appliquer, l'exigence E1.1.5 de la norme CIP-010 stipule que les entités doivent consigner toutes les rustines appliquées, antérieures et courantes.

Afin d'aider la compréhension, voici un exemple qui décrit la configuration de référence d'un relais à microprocesseur série seulement :

Actif n° 051028 au poste électrique Alpha

- E1.1.1 – Microprogramme : [FABRICANT]-[MODÈLE]-XYZ-1234567890-ABC
- E1.1.2 – Sans objet
- E1.1.3 – Sans objet
- E1.1.4 – Sans objet
- E1.1.5 – Rustine 12345, Rustine 67890, Rustine 34567 et Rustine 437823

En outre, pour un système informatique type, la configuration de référence pourrait renvoyer à une norme informatique qui précise les détails de la configuration. L'entité devrait alors présenter cette norme informatique à titre de preuve de conformité.

Mécanismes de cybersécurité

Les mécanismes de cybersécurité dont il est question dans cette exigence renvoient spécifiquement aux mécanismes des normes CIP-005 et CIP-007. Les parties pertinentes de l'exigence E1 de la norme CIP-010 stipulent que l'entité doit déterminer et analyser les mécanismes des normes CIP-005 et CIP-007 qui pourraient être touchés par un changement par rapport à la configuration de référence existante. Le SDT ne souhaite pas obliger l'entité responsable à passer en revue tous les mécanismes de cybersécurité des normes CIP-005 et CIP-007 pour chaque changement, mais seulement le ou les mécanismes susceptibles d'être touchés par le changement en question. Par exemple, les changements relatifs aux ports logiques concernent seulement l'exigence E1 de la norme CIP-007 (ports et services), tandis que

les changements relatifs aux rustines de sécurité concernent seulement l'exigence E2 de la norme CIP-007 (gestion des rustines de sécurité). Le SDT a choisi de ne pas préciser les exigences des normes CIP-005 et CIP-007 dans le texte de la norme CIP-010, étant donné que n'importe quel des mécanismes de cybersécurité de ces normes peut être touché par suite d'un changement dans la configuration de référence. L'équipe de rédaction considère qu'il est possible que toutes les exigences des normes CIP-005 et CIP-007 soient touchées par un changement important dans la configuration de référence, et c'est pourquoi les normes CIP-005 et CIP-007 sont citées dans leur globalité plutôt qu'à l'échelon de leurs exigences individuelles.

Environnement d'essai

L'environnement d'essai du *centre de contrôle* (ou l'environnement de production dans lequel l'essai est effectué d'une manière qui réduit au minimum les effets dommageables) doit simuler la configuration de référence, mais peut le faire au moyen de composants différents. Par exemple, un *système électronique BES* peut comporter une base de données sur un composant et un serveur Web sur un autre ; cependant, dans l'environnement d'essai, la base de données et le serveur Web peuvent résider sur un même composant pourvu que le système d'exploitation, les rustines de sécurité, les ports accessibles par le réseau et les logiciels soient identiques.

En outre, l'entité responsable doit prendre note que, lorsqu'il est question d'un environnement d'essai (ou d'un environnement de production dans lequel l'essai est effectué d'une manière qui réduit au minimum les effets dommageables), il s'agit bien de « simuler » la configuration de référence, et non de la reproduire à l'identique. Cette formulation a été choisie expressément pour les cas où il serait impossible de dupliquer certains éléments de *système électronique BES* d'un *centre de contrôle* ; par exemple, un modèle ancien de pilote de tableau de visualisation, ou encore les nombreuses liaisons d'échange de données à partir des installations sur le terrain ou vers d'autres *centres de contrôle* (comme les liaisons ICCP).

Exigence E2 :

L'idée maîtresse de cette exigence est la surveillance automatisée du *système électronique BES*. Cependant, le SDT reconnaît que certains *actifs électroniques* se prêtent mal à une surveillance automatisée (par exemple une horloge GPS). C'est pourquoi une surveillance technique automatisée n'est pas exigée explicitement ; l'entité responsable peut choisir de satisfaire à cette exigence par des procédures manuelles.

Exigence E3 :

L'entité responsable doit prendre note que l'exigence d'analyse de vulnérabilité fait une distinction entre analyse sur papier et analyse active. Cette distinction s'appuie sur l'ordonnance 706 de la FERC et la proposition réglementaire (*Notice of Proposed Rulemaking*) connexe. Dans l'élaboration de son processus d'analyse de vulnérabilité, l'entité responsable

est fortement encouragée à inclure à tout le moins les éléments suivants, dont plusieurs sont mentionnés dans les normes CIP-005 et CIP-007 :

Analyse de vulnérabilité sur papier :

1. Recherche de réseau – Examen de la connectivité réseau visant à inventorier tous les *points d'accès électronique* au *périmètre de sécurité électronique*.
2. Inventaire des ports et des services réseau – Examen permettant de vérifier que tous les ports et services activés ont une justification fonctionnelle.
3. Examen des vulnérabilités – Examen des règles et des configurations de sécurité, y compris les mesures de sécurité pour les comptes par défaut, les mots de passe et les chaînes de communauté pour la gestion du réseau.
4. Examen des réseaux sans fil – Inventaire des types courants de réseaux sans fil (par exemple 802.11a, b, g et n) et examen de leurs mesures de sécurité si ces réseaux sont utilisés d'une manière quelconque pour les communications du *système électronique BES*.

Analyse de vulnérabilité active :

1. Recherche de réseau – Recours à des outils de détection active pour inventorier les dispositifs actifs et les trajets de communication afin de confirmer que l'architecture réseau constatée correspond bien à l'architecture documentée.
2. Inventaire des ports et des services réseau – Recours à des outils de détection active (par exemple Nmap) pour déterminer les ports ouverts et les services actifs.
3. Balayage des vulnérabilités – Recours à un outil de balayage des vulnérabilités pour inventorier les ports et les services accessibles par le réseau et pour repérer les vulnérabilités connues associées aux services qui exploitent ces ports.
4. Balayage des réseaux sans fil – Recours à un outil de balayage pour inventorier les signaux et les réseaux sans fil dans le périmètre physique d'un *système électronique BES*. Permet de repérer les appareils sans fil non autorisés situés dans la portée de l'outil de balayage.

En outre, les entités responsables sont fortement encouragées à consulter la publication SP800-115 du NIST pour de plus amples renseignements sur la manière d'effectuer une analyse de vulnérabilité.

Raisonnement :

Pendant l'élaboration de cette norme, les références aux versions antérieures des normes CIP et le raisonnement derrière les exigences et leurs parties étaient intégrés à même la norme. Sur approbation du BOT, cette information a été déplacée à la présente section.

Raisonnement pour E1 :

Les processus de gestion des changements de configuration visent à empêcher les modifications non autorisées aux *systèmes électroniques BES*.

Référence à une version précédente : (Partie 1.1) Nouvelle exigence

Justification des modifications : (Partie 1.1)

L'exigence de configuration de référence provient du Catalog of Control Systems Security du Department of Homeland Security. Cette exigence vise aussi à préciser dans quel contexte un processus de gestion des changements est exigé et quels éléments de configuration doivent être examinés.

Référence à une version précédente : (Partie 1.2) CIP-007-3, E9 ; CIP-003-3, E6

Justification des modifications : (Partie 1.2)

Le SDT a ajouté l'exigence d'une autorisation explicite des changements. Cette exigence était auparavant implicite dans l'exigence E6 de la norme CIP-003-3.

Référence à une version précédente : (Partie 1.3) CIP-007-3, E9 ; CIP-005-3, E5

Justification des modifications : (Partie 1.3)

L'exigence de tenue à jour de la documentation selon les changements apportés à un *système électronique BES* est équivalente aux exigences des versions précédentes des normes CIP.

Référence à une version précédente : (Partie 1.4) CIP-007-3, E1

Justification des modifications : (Partie 1.4)

Le SDT a voulu préciser à quel moment les essais doivent être effectués et a retiré la prescription de procédures d'essai particulières, celle-ci étant implicite dans la mise en œuvre de l'exigence.

Référence à une version précédente : (Partie 1.5) CIP-007-3, E1

Justification des modifications : (Partie 1.5)

Cette exigence précise quand des essais doivent avoir lieu et prescrit des essais supplémentaires pour gérer adéquatement les conséquences accidentelles des changements planifiés.

Ce changement tient compte de l'ordonnance 706 de la FERC, paragraphes 397, 609, 610 et 611.

Raisonnement pour E2 :

Le processus de surveillance de la configuration vise à détecter les modifications non autorisées aux *systèmes électroniques BES*.

Référence à une version précédente : (Partie 2.1) Nouvelle exigence

Justification des modifications : (Partie 2.1)

L'exigence de surveillance de la configuration des *systèmes électroniques BES* vient affirmer qu'il faut tenir compte des actions malveillantes autant que des changements intentionnels.

Cette exigence a été ajoutée après consultation du Catalog of Control Systems Security du Department of Homeland Security et pour tenir compte de l'ordonnance 706 de la FERC, paragraphe 397.

Le délai de 35 jours civils permet d'établir une fréquence mensuelle, avec une certaine souplesse pour tenir compte des mois de 31 jours ou des mois qui commencent ou se terminent pendant une fin de semaine.

Raisonnement pour E3 :

Les processus d'analyse de vulnérabilité doivent être intégrés à un programme général visant un contrôle périodique de la bonne mise en œuvre des mécanismes de cybersécurité et l'amélioration continue de la posture de sécurité des *systèmes électroniques BES*.

Les analyses de vulnérabilité effectuées dans le contexte de cette exigence peuvent faire partie d'un programme de détection, d'évaluation et de correction des déficiences.

Référence à une version précédente : (Partie 3.1) CIP-005-4, E4 ; CIP-007-4, E8

Justification des modifications : (Partie 3.1)

Comme le suggère l'ordonnance 706 de la FERC, paragraphe 644, les détails sur lesquels doit porter l'analyse sont laissés à discrétion.

Référence à une version précédente : (Partie 3.2) Nouvelle exigence

Justification des modifications : (Partie 3.2)

Ordonnance 706 de la FERC, paragraphes 541, 542, 543, 544, 545 et 547.

Comme le suggère l'ordonnance 706 de la FERC, paragraphe 644, les détails sur lesquels doit porter l'analyse sont laissés à discrétion.

Référence à une version précédente : (Partie 3.3) Nouvelle exigence

Justification des modifications : (Partie 3.3)

Ordonnance 706 de la FERC, paragraphes 541, 542, 543, 544, 545 et 547.

Référence à une version précédente : (Partie 3.4) CIP-005-3, E4.5 ; CIP-007-3, E8.4

Justification des modifications : (Partie 3.4)

Ajout d'une exigence quant à la date prévue d'achèvement par l'entité, conformément à l'ordonnance 706 de la FERC, paragraphe 643.

Historique des versions

Version	Date	Intervention	Suivi des modifications
1	26 novembre 2012	Adoption par le conseil d'administration de la NERC.	Cette norme encadre la gestion des changements de configuration et des analyses de vulnérabilité en coordination avec d'autres normes CIP et met en œuvre certaines dispositions de l'ordonnance 706 de la FERC.
1	22 novembre 2013	Émission d'une ordonnance de la FERC approuvant CIP-010-1 (L'ordonnance entre en vigueur le 3 février 2014)	

Annexe QC-CIP-010-1

Dispositions particulières de la norme CIP-010-1 applicables au Québec

Cette annexe établit les dispositions particulières d'application de la norme au Québec. Les dispositions de la norme et de son annexe doivent obligatoirement être lues conjointement pour fins de compréhension et d'interprétation. En cas de divergence entre la norme et l'annexe, l'annexe aura préséance.

A. Introduction

1. **Titre :** Cybersécurité — Gestion des changements de configuration et analyses de vulnérabilité
2. **Numéro :** CIP-010-1
3. **Objet :** Aucune disposition particulière
4. **Applicabilité :**

Entités fonctionnelles

Aucune disposition particulière

Installations

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.

5. **Date d'entrée en vigueur au Québec :**
 - 5.1. Adoption de la norme par la Régie de l'énergie : xx mois 201x
 - 5.2. Adoption de l'annexe par la Régie de l'énergie : xx mois 201x
 - 5.3. Date d'entrée en vigueur de la norme et de l'annexe au Québec : xx mois 201x
6. **Contexte :** Aucune disposition particulière

B. Exigences et mesures

Aucune disposition particulière

C. Conformité

1. **Processus de surveillance de la conformité**
 - 1.1. **Responsable de la surveillance de l'application des normes**

La Régie de l'énergie est responsable, au Québec, de la surveillance de l'application de la norme de fiabilité et de son annexe qu'elle adopte.
 - 1.2. **Conservation des pièces justificatives**

Aucune disposition particulière

Annexe QC-CIP-010-1

Dispositions particulières de la norme CIP-010-1 applicables au Québec

1.3. Processus de surveillance et d'évaluation de la conformité

Aucune disposition particulière

1.4. Autres informations sur la conformité

Aucune disposition particulière

2. Tableau des éléments de conformité

Aucune disposition particulière

D. Différences régionales

Aucune disposition particulière

E. Interprétations

Aucune disposition particulière

F. Documents connexes

Aucune disposition particulière

Principes directeurs et fondements techniques

Aucune disposition particulière

Raisonnement

Aucune disposition particulière

Historique des révisions

Révision	Date d'adoption	Intervention	Suivi des modifications
0	Xx mois 201x	Nouvelle annexe	Nouvelle