## A. Introduction

**1. Titre :** Cybersécurité – Sécurité physique des systèmes électroniques BES

**2. Numéro :** CIP-006-6

**3. Objet :** Gérer l'accès physique aux *systèmes électroniques BES* en établissant un plan de sécurité physique afin de protéger les *systèmes électroniques BES* contre les compromissions qui pourraient entraîner un fonctionnement incorrect ou une instabilité dans le *système de production-transport d'électricité* (*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* visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou de l'entité 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.

**4.1.2.2** Chaque *automatisme de réseau (SPS)* ou *plan de défense (RAS)* visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou de l'entité régionale.

**4.1.2.3** Chaque *système de protection* applicable au *transport* (à l'exclusion des systèmes DSF et DST) visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou de l'entité 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 prochains groupes de production 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* visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou de l'entité régionale ; et

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

**4.2.1.2** Chaque *automatisme de réseau* ou *plan de défense* visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou de l'entité régionale.

**4.2.1.3** Chaque *système de protection* applicable au *transport* (à l'exclusion des systèmes DSF et DST) dans le cas où le *système de protection* visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou de l'entité 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 prochains groupes de production 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-006-6 :

**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 composants régis par la U.S. Nuclear Regulatory Commission en vertu d'un plan de cybersécurité conforme au règlement 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* classés dans les catégories « impact élevé » ou « impact moyen » selon le processus de désignation et de catégorisation de la norme CIP-002-5.1.

## 5. Dates d'entrée en vigueur

Voir le plan de mise en œuvre de la norme CIP-006-6

## 6. Contexte

La norme CIP-006 fait partie d'une série de normes CIP sur la cybersécurité qui exigent la détermination et la catégorisation initiales des *systèmes électroniques BES*. Ces normes exigent aussi un niveau minimal de mesures organisationnelles, opérationnelles et administratives pour réduire les risques aux *systèmes électroniques BES*.

La plupart des exigences commencent ainsi : « Chaque entité responsable doit mettre en œuvre un ou plusieurs [processus, plans, etc.] documentés qui couvrent tous les alinéas 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.

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 doit inclure tout ce qu'elle juge nécessaire dans ses processus documentés, en s'assurant de bien couvrir les exigences pertinentes.

Les mots « programme » et « plan » sont parfois utilisés au lieu de « processus documenté », dans la mesure où la compréhension relève du bon sens. 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 des exemples qui figurent dans les normes. La mise en œuvre

complète des normes de fiabilité 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 concernant plusieurs *systèmes électroniques BES*.

Les mesures auxquelles renvoie l'énoncé initial de l'exigence correspondent simplement aux processus documentés eux-mêmes. La colonne « Mesures » présente des exemples de pièces justificatives attestant la documentation et la mise en œuvre des éléments pertinents dans les processus documentés ; ces exemples sont présentés à titre indicatif, et leur liste ne doit pas être considérée comme 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 *BES*. Un examen des tolérances des 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.

**Colonne « Systèmes visés » des tableaux**

Chaque tableau comporte une colonne intitulée « Systèmes visés » qui définit plus précisément les systèmes auxquels s'applique l'exigence. La SDT (équipe de rédaction) 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 », selon les processus de désignation et de catégorisation de la norme CIP-002-5.1.
- ***Systèmes électroniques BES* à impact moyen –** Désigne les *systèmes électroniques BES* classés dans la catégorie « impact moyen », selon les processus de désignation et de catégorisation de la norme CIP-002-5.1.

- ***Systèmes électroniques BES* à impact moyen sans connectivité externe routable** – Désigne uniquement les *systèmes électroniques BES* à impact moyen sans *connectivité externe routable*.
- ***Systèmes électroniques BES* à impact moyen à connectivité externe routable** – Désigne uniquement les *systèmes électroniques BES* à impact moyen à *connectivité externe routable*, à l'exclusion des *actifs électroniques* des *systèmes électroniques BES* auxquels on ne peut avoir accès directement par *connectivité externe routable*.
- ***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'événements et d'alerte.
- ***Systèmes de contrôle des accès physiques* (*PACS*)** – Désigne tout *système de contrôle des accès physique*s 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.
- **Matériel et dispositifs installés localement au *périmètre de sécurité physique*** – Désigne le matériel et les dispositifs (p. ex. détecteurs de mouvement, mécanismes de verrouillage électroniques ou lecteurs de carte d'accès) installés localement au *périmètre de sécurité physique* associé à un *système électronique BES* à impact élevé ou moyen à *connectivité externe routable* visé, mais qui ne contiennent pas et n'enregistrent pas d'information servant au contrôle des accès, et qui n'assurent pas de façon autonome l'authentification des accès. Ce matériel et ces dispositifs sont par définition exclus des *systèmes de contrôle des accès physiques*.

## B. Exigences et mesures

**E1.** Chaque entité responsable doit mettre en œuvre un ou plusieurs plans de sécurité physique documentés qui, collectivement, couvrent tous les alinéas applicables du tableau E1 (CIP-006-6) – Plan de sécurité physique. *[Facteur de risque de non-conformité : moyen] [Horizon : planification à long terme et exploitation le même jour]*

**M1.** Les pièces justificatives doivent comprendre chacun des plans de sécurité physique documentés qui, collectivement, couvrent tous les alinéas applicables du tableau E1 (CIP-006-6) – Plan de sécurité physique ; d'autres pièces justificatives doivent attester la mise en œuvre selon la colonne Mesures du tableau.

| Tableau E1 (CIP-006-6) – Plan de sécurité physique | | | |
|---|---|---|---|
| **Alinéa** | **Systèmes visés** | **Exigences** | **Mesures** |
| 1.1 | *Systèmes électroniques BES* à impact moyen sans *connectivité externe routable*.<br><br>*Systèmes de contrôle des accès physiques* (*PACS*) associés à :<br>• des *systèmes électroniques BES* à impact élevé ; ou<br>• des *systèmes électroniques BES* à impact moyen à *connectivité externe routable*. | Définir des mesures opérationnelles ou administratives permettant de restreindre l'accès physique. | Exemple non limitatif de pièces justificatives : documentation attestant que des mesures opérationnelles ou administratives sont en place. |

| Tableau E1 (CIP-006-6) – Plan de sécurité physique | | | |
|---|---|---|---|
| **Alinéa** | **Systèmes visés** | **Exigences** | **Mesures** |
| 1.2 | *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et :<br>1. les *EACMS* associés ; et<br>2. les *PCA* associés. | Utiliser au moins un mécanisme de contrôle des accès physiques permettant l'accès physique sans accompagnement à chaque *périmètre de sécurité physique* visé aux seules personnes ayant un accès physique autorisé sans accompagnement. | Exemple non limitatif de pièces justificatives : des énoncés dans le plan de sécurité physique qui décrivent chaque *périmètre de sécurité physique* et comment les accès physiques sans accompagnement y sont contrôlés par au moins un mécanisme, ainsi que des preuves qui attestent que seules les personnes autorisées y ont un accès physique sans accompagnement, comme des listes de personnes autorisées et les registres d'accès correspondants. |
| 1.3 | *Systèmes électroniques BES* à impact élevé et :<br>1. les *EACMS* associés ; et<br>2. les *PCA* associés. | Si c'est techniquement faisable, utiliser au moins deux mécanismes de contrôle des accès physiques différents (ce qui n'exige pas nécessairement deux systèmes de contrôle complètement indépendants) qui, ensemble, permettent l'accès physique sans accompagnement aux *périmètres de sécurité physique* aux seules personnes ayant un accès physique autorisé sans accompagnement. | Exemple non limitatif de pièces justificatives : des énoncés dans le plan de sécurité physique qui décrivent les *périmètres de sécurité physique* et comment les accès physiques sans accompagnement sont contrôlés par au moins deux mécanismes différents, ainsi que des preuves qui attestent que seules les personnes autorisées y ont un accès physique sans accompagnement, comme des listes de personnes autorisées et les registres d'accès correspondants. |

| Tableau E1 (CIP-006-6) – Plan de sécurité physique | | | |
|---|---|---|---|
| **Alinéa** | **Systèmes visés** | **Exigences** | **Mesures** |
| 1.4 | *Systèmes électroniques BES* à impact élevé et :<br>1. les *EACMS* associés ; et<br>2. les *PCA* associés.<br><br>*Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et :<br>1. les *EACMS* associés ; et<br>2. les *PCA* associés. | Surveiller les accès non autorisés à un point d'accès physique d'un *périmètre de sécurité physique*. | Exemple non limitatif de pièces justificatives : documentation des mécanismes de surveillance des accès non autorisés à un point d'accès physique d'un *périmètre de sécurité physique*. |

| Tableau E1 (CIP-006-6) – Plan de sécurité physique | | | |
|---|---|---|---|
| **Alinéa** | **Systèmes visés** | **Exigences** | **Mesures** |
| 1.5 | *Systèmes électroniques BES* à impact élevé et :<br>1. les *EACMS* associés ; et<br>2. les *PCA* associés.<br><br>*Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et :<br>1. les *EACMS* associés ; et<br>2. les *PCA* associés. | Déclencher une alarme ou une alerte en réponse à la détection d'un accès non autorisé à un point d'accès physique d'un *périmètre de sécurité physique*, à l'intention du personnel désigné dans le plan d'intervention en cas d'*incident de cybersécurité* lié au *BES*, dans les 15 minutes suivant la détection. | Exemple non limitatif de pièces justificatives : des énoncés dans le plan de sécurité physique décrivant le processus de déclenchement d'une alarme ou d'une alerte en réponse à un accès non autorisé à un point d'accès physique d'un *périmètre de sécurité physique,* et des pièces justificatives additionnelles qui attestent que l'alarme ou l'alerte a été déclenchée et communiquée conformément au plan d'intervention en cas d'*incident de cybersécurité* lié au *BES*, comme des journaux d'alarmes ou d'alertes électroniques ou manuelles ou des registres de communications par cellulaire ou téléavertisseur, ou d'autres pièces justificatives qui documentent que l'alarme ou l'alerte a été déclenchée et communiquée. |
| 1.6 | *Systèmes de contrôle des accès physiques* (PACS) associés à :<br>• des *systèmes électroniques BES* à impact élevé ; ou<br>• des *systèmes électroniques BES* à impact moyen à *connectivité externe routable*. | Surveiller chaque *système de contrôle des accès physiques* afin de détecter les accès physiques non autorisés à un *système de contrôle des accès physiques*. | Exemple non limitatif de pièces justificatives : documentation des mécanismes de détection des accès physiques non autorisés à un PACS. |

| Tableau E1 (CIP-006-6) – Plan de sécurité physique | | | |
|---|---|---|---|
| **Alinéa** | **Systèmes visés** | **Exigences** | **Mesures** |
| 1.7 | *Systèmes de contrôle des accès physiques* (PACS) associés à :<br>• des *systèmes électroniques BES* à impact élevé ; ou<br>• des *systèmes électroniques BES* à impact moyen à *connectivité externe routable*. | Déclencher une alarme ou une alerte en réponse à la détection d'un accès physique non autorisé à un *système de contrôle des accès physiques,* à l'intention du personnel désigné dans le plan d'intervention en cas d'*incident de cybersécurité* lié au *BES*, dans les 15 minutes suivant la détection. | Exemple non limitatif de pièces justificatives : des énoncés dans le plan de sécurité physique précisant qu'une alarme ou une alerte est déclenchée en réponse à la détection d'un accès physique non autorisé à un *système de contrôle des accès physiques*, et des pièces justificatives additionnelles qui attestent que l'alarme ou l'alerte a été déclenchée et communiquée conformément au plan d'intervention en cas d'*incident de cybersécurité* lié au *BES*, comme des journaux d'alarmes ou d'alertes ou des registres de communications par cellulaire ou téléavertisseur, ou d'autres pièces justificatives qui attestent que l'alarme ou l'alerte a été déclenchée et communiquée. |

| Tableau E1 (CIP-006-6) – Plan de sécurité physique | | | |
|---|---|---|---|
| **Alinéa** | **Systèmes visés** | **Exigences** | **Mesures** |
| 1.8 | *Systèmes électroniques BES* à impact élevé et :<br>1. les EACMS associés ; et<br>2. les PCA associés.<br>*Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et :<br>1. les EACMS associés ; et<br>2. les PCA associés. | Consigner (par des moyens automatisés ou par du personnel qui contrôle l'entrée) l'accès de chaque personne ayant un accès physique autorisé sans accompagnement dans chaque *périmètre de sécurité physique,* avec l'information permettant d'identifier la personne et de connaître la date et l'heure de l'accès. | Exemple non limitatif de pièces justificatives : des énoncés dans le plan de sécurité physique décrivant la consignation et l'enregistrement des accès physiques à chaque *périmètre de sécurité physique* et des pièces justificatives additionnelles attestant que cette consignation a été mise en œuvre, comme des registres d'accès physique aux *périmètres de sécurité physique* indiquant la personne ainsi que la date et l'heure de l'accès au *périmètre de sécurité physique*. |
| 1.9 | *Systèmes électroniques BES* à impact élevé et :<br>1. les EACMS associés ; et<br>2. les PCA associés.<br>*Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et :<br>1. les EACMS associés ; et<br>2. les PCA associés. | Conserver les registres d'accès physique des personnes ayant un accès physique autorisé sans accompagnement à un *périmètre de sécurité physique* pendant au moins 90 jours civils. | Exemple non limitatif de pièces justificatives : documents datés, comme des registres des accès physiques aux *périmètres de sécurité physique* indiquant la date et l'heure de l'accès au *périmètre de sécurité physique*. |
| 1.10 | Systèmes électroniques BES à impact élevé et :<br>• les PCA associés.<br>*Systèmes électroniques BES* à impact moyen aux *centres de* | Restreindre l'accès physique aux câbles et autres composants de communication non programmables qui servent à interrelier des *actifs électroniques* visés situés dans un | Exemples non limitatifs de pièces justificatives : documents attestant la mise en œuvre par l'entité responsable des restrictions d'accès physique (câblage et composants sous |

| Tableau E1 (CIP-006-6) – Plan de sécurité physique | | | |
|---|---|---|---|
| **Alinéa** | **Systèmes visés** | **Exigences** | **Mesures** |
| | *contrôle* et :<br>• les PCA associés. | même *périmètre de sécurité électronique*, si ces câbles et composants se trouvent à l'extérieur d'un *périmètre de sécurité physique*.<br>En l'absence de restriction d'accès physique à de tels câblages et composants, l'entité responsable doit documenter et mettre en œuvre une ou plusieurs des mesures suivantes :<br>• cryptage des données qui transitent par ces câbles et composants ; ou<br>• surveillance de l'état de la liaison de communication constituée par ces câbles et composants, avec déclenchement d'une alarme ou d'une alerte sur détection d'une défaillance de communication à l'intention du personnel désigné dans le plan d'intervention en cas d'*incident de cybersécurité* lié au *BES*, dans les 15 minutes suivant la détection ; ou<br>• protection logique d'une efficacité équivalente. | conduit ou enfermés dans des chemins de câbles, etc.), du cryptage des données, de la surveillance ou d'une protection logique d'une efficacité équivalente. |

**E2.** Chaque entité responsable doit mettre en œuvre un ou plusieurs programmes de contrôle des visiteurs documentés qui, collectivement, couvrent tous les alinéas du tableau E2 (CIP-006-6) – Programme de contrôle des visiteurs. *[Facteur de risque de non-conformité : moyen] [Horizon : exploitation le même jour]*

**M2.** Les pièces justificatives doivent comprendre un ou plusieurs programmes de contrôle des visiteurs documentés qui, collectivement, couvrent tous les alinéas applicables du tableau E2 (CIP-006-6) – Programme de contrôle des visiteurs ; d'autres pièces justificatives doivent attester la mise en œuvre selon la colonne Mesures du tableau.

| Tableau E2 (CIP-006-6) – Programme de contrôle des visiteurs | | | |
|---|---|---|---|
| **Alinéa** | **Systèmes visés** | **Exigences** | **Mesures** |
| 2.1 | *Systèmes électroniques BES* à impact élevé et :<br>1. les EACMS associés ; et<br>2. les PCA associés.<br>*Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et :<br>1. les EACMS associés ; et<br>2. les PCA associés. | Exiger un accompagnement continu des visiteurs (personnes à qui l'accès est accordé, mais n'ayant pas un accès physique autorisé sans accompagnement) à l'intérieur de chaque *périmètre de sécurité physique*, sauf dans des *circonstances CIP exceptionnelles*. | Exemple non limitatif de pièces justificatives : des énoncés dans un programme de contrôle des visiteurs exigeant un accompagnement continu des visiteurs à l'intérieur des *périmètres de sécurité physique* ainsi que des pièces justificatives additionnelles attestant que cette mesure a été mise en œuvre, comme des registres de visiteurs. |
| 2.2 | *Systèmes électroniques BES* à impact élevé et :<br>1. les EACMS associés ; et<br>2. les PCA associés.<br>*Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et :<br>1. les EACMS associés ; et<br>2. les PCA associés. | Exiger la consignation manuelle ou automatique de l'entrée de tout visiteur dans un *périmètre de sécurité physique* ainsi que de sa sortie, notamment la date et l'heure de la première entrée et de la dernière sortie, le nom du visiteur et le nom de son répondant, sauf dans des *circonstances CIP exceptionnelles*. | Exemple non limitatif de pièces justificatives : des énoncés dans un programme de contrôle des visiteurs qui exige un accompagnement continu des visiteurs à l'intérieur des *périmètres de sécurité physique* et des pièces justificatives additionnelles attestant que cette mesure a été mise en œuvre, comme des registres de visiteurs datés renfermant les données pertinentes. |

| Tableau E2 (CIP-006-6) – Programme de contrôle des visiteurs | | | |
|---|---|---|---|
| **Alinéa** | **Systèmes visés** | **Exigences** | **Mesures** |
| 2.3 | *Systèmes électroniques BES* à impact élevé et :<br>1. les EACMS associés ; et<br>2. les PCA associés.<br>*Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et :<br>1. les EACMS associés ; et<br>2. les PCA associés. | Conserver les registres des visiteurs durant au moins 90 jours civils. | Exemple non limitatif de pièces justificatives : documentation attestant que les registres des visiteurs ont été conservés durant au moins 90 jours civils. |

**E3.** Chaque entité responsable doit mettre en œuvre un ou plusieurs programmes documentés de maintenance et d'essai des *systèmes de contrôle des accès physiques* qui, collectivement, couvrent tous les alinéas applicables du tableau E3 (CIP-006-6) – Programme de maintenance et d'essais.
*[Facteur de risque de non-conformité : moyen] [Horizon : planification à long terme]*

**M3.** Les pièces justificatives doivent comprendre tous les programmes documentés de maintenance et d'essai des *systèmes de contrôle des accès physiques* qui, collectivement, couvrent tous les alinéas applicables du tableau E3 (CIP-006-6) – Programme de maintenance et d'essais ; d'autres pièces justificatives doivent attester la mise en œuvre selon la colonne Mesures du tableau.

**Tableau E3 (CIP-006-6) – Programme de maintenance et d'essais des systèmes de contrôle des accès physiques**

| Partie | Systèmes visés | Exigences | Mesures |
|---|---|---|---|
| 3.1 | *Systèmes de contrôle des accès physiques* (PACS) associés à :<br>• des *systèmes électroniques BES* à impact élevé ; ou<br>• des *systèmes électroniques BES* à impact moyen à *connectivité externe routable*.<br>Équipements et dispositifs installés localement aux *périmètres de sécurité physique* associés à :<br>• des *systèmes électroniques BES* à impact élevé ; ou<br>• des *systèmes électroniques BES* à impact moyen à *connectivité externe routable*. | Les opérations de maintenance et d'essai de chaque *système de contrôle des accès physiques* et de chaque équipement ou dispositif installé localement au *périmètre de sécurité physique* doivent être effectuées au moins une fois tous les 24 mois civils afin d'assurer leur bon fonctionnement. | Exemple non limitatif de pièces justificatives : un programme de maintenance et d'essai exigeant l'essai, au moins une fois tous les 24 mois civils, de chaque *système de contrôle des accès physiques* et des équipements ou dispositifs installés localement à un *périmètre de sécurité physique* visé, et des pièces justificatives additionnelles attestant que les essais ont été effectués, comme des registres de maintenance datés, ou tout autre document attestant que la maintenance et les essais ont été effectués pour chaque système et dispositif visé au moins une fois tous les 24 mois civils. |

## C. Conformité

### 1. Processus de surveillance de la conformité

#### 1.1. Responsable des mesures pour assurer la conformité

Selon la définition des règles de procédure de la NERC, le terme « *responsable des mesures* » (CEA) désigne la NERC ou l'entité régionale dans leurs rôles respectifs de surveillance de la conformité aux normes de fiabilité de la NERC.

#### 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 attestant sa conformité pendant la période complète écoulée depuis le dernier audit.

L'entité responsable doit conserver les données ou pièces justificatives attestant sa conformité selon les modalités indiquées ci-après, à moins que son CEA lui demande de conserver certaines pièces justificatives 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 de conformité

Déclarations de non-conformité

Plaintes

#### 1.4. Autres informations sur la conformité

Aucune.

## 2. Tableau des éléments de conformité

| Ex. | Horizon | VRF | Niveaux de gravité de la non-conformité (CIP-006-6) | | | |
|---|---|---|---|---|---|---|
| | | | VSL faible | VSL modéré | VSL élevé | VSL critique |
| **E1** | **Planification à long terme**<br>**Exploitation le même jour** | **Moyen** | | | | L'entité responsable n'a documenté ou mis en œuvre aucun plan de sécurité physique. (E1)<br>OU<br>L'entité responsable n'a pas documenté ou mis en œuvre de mesures opérationnelles ou administratives permettant de restreindre l'accès physique. (1.1)<br>OU<br>L'entité responsable a documenté et mis en œuvre des mécanismes de contrôle des accès physiques, mais il n'y a pas au moins un mécanisme de contrôle pour restreindre l'accès aux systèmes |

| Ex. | Horizon | VRF | Niveaux de gravité de la non-conformité (CIP-006-6) | | | |
|---|---|---|---|---|---|---|
| | | | VSL faible | VSL modéré | VSL élevé | VSL critique |
| | | | | | | applicables. (1.2)<br>OU<br>L'entité responsable a documenté et mis en œuvre des mécanismes de contrôle des accès physiques, mais il n'y a pas au moins deux mécanismes de contrôle différents pour restreindre l'accès aux systèmes applicables. (1.3)<br>OU<br>L'entité responsable n'a pas de processus pour surveiller les accès non autorisés à un point d'accès physique d'un *périmètre de sécurité physique*. (1.4)<br>OU<br>L'entité responsable n'a pas de processus pour déclencher une |

| Ex. | Horizon | VRF | Niveaux de gravité de la non-conformité (CIP-006-6) | | | |
|---|---|---|---|---|---|---|
| | | | VSL faible | VSL modéré | VSL élevé | VSL critique |
| | | | | | | alerte en cas de détection d'un accès non autorisé à un point d'accès physique d'un *périmètre de sécurité physique* ou pour communiquer cette alerte au personnel désigné dans un délai de 15 minutes. (1.5)<br><br>OU<br><br>L'entité responsable n'a pas de processus pour surveiller chaque *système de contrôle des accès physiques* à la recherche d'accès physiques non autorisés à un *système de contrôle des accès physiques*. (1.6)<br><br>OU<br><br>L'entité responsable n'a pas de processus pour déclencher une alerte en cas d'accès physique non autorisé |

| Ex. | Horizon | VRF | Niveaux de gravité de la non-conformité (CIP-006-6) | | | |
|---|---|---|---|---|---|---|
| | | | VSL faible | VSL modéré | VSL élevé | VSL critique |
| | | | | | | aux *systèmes de contrôle des accès physiques* ou pour communiquer cette alerte au personnel désigné dans un délai de 15 minutes. (1.7)<br><br>OU<br><br>L'entité responsable n'a pas de processus pour consigner les accès physiques autorisés à chaque *périmètre de sécurité physique*, avec l'information permettant d'identifier la personne ainsi que la date et l'heure de l'accès. (1.8)<br><br>OU<br><br>L'entité responsable n'a pas de processus pour conserver les registres d'accès physique pendant |

| Ex. | Horizon | VRF | Niveaux de gravité de la non-conformité (CIP-006-6) | | | |
|---|---|---|---|---|---|---|
| | | | VSL faible | VSL modéré | VSL élevé | VSL critique |
| | | | | | | 90 jours civils. (1.9)<br>OU<br>L'*entité responsable* n'a pas documenté ni mis en œuvre des restrictions d'accès physique, du cryptage, de la surveillance ou d'autres protections logiques d'une efficacité équivalente pour des câbles et autres composants de communication non programmables qui servent à interrelier des *actifs électroniques* visés situés dans un même *périmètre de sécurité électronique*, si ces câbles et composants se trouvent à l'extérieur d'un *périmètre de* |

| Ex. | Horizon | VRF | Niveaux de gravité de la non-conformité (CIP-006-6) | | | |
|---|---|---|---|---|---|---|
| | | | VSL faible | VSL modéré | VSL élevé | VSL critique |
| | | | | | | *sécurité physique*. (1.10) |
| **E2** | **Exploitation le même jour** | **Moyen** | Sans objet | Sans objet | Sans objet | L'entité responsable n'a pas adopté ou mis en œuvre un programme de contrôle des visiteurs qui exige un accompagnement continu des visiteurs à l'intérieur de tout *périmètre de sécurité physique.* (2.1)<br>OU<br>L'entité responsable n'a pas adopté ou mis en œuvre un programme de contrôle des visiteurs qui exige la consignation de la date et l'heure de la première entrée et de la dernière sortie du visiteur, le nom du visiteur et le nom de |

| Ex. | Horizon | VRF | Niveaux de gravité de la non-conformité (CIP-006-6) | | | |
|---|---|---|---|---|---|---|
| | | | VSL faible | VSL modéré | VSL élevé | VSL critique |
| | | | | | | son répondant. (2.2)<br>OU<br>L'entité responsable n'a pas adopté ou mis en œuvre un programme de contrôle des visiteurs pour conserver les registres des visiteurs durant au moins 90 jours. (2.3) |
| **E3** | **Planification à long terme** | **Moyen** | L'entité responsable a documenté et mis en œuvre un programme de maintenance et d'essai des *systèmes de contrôle des accès physiques* et des équipements ou dispositifs installés localement au *périmètre de sécurité physique,* mais a terminé l'essai exigé dans un délai de plus de 24 mois civils et d'au plus 25 mois civils. | L'entité responsable a documenté et mis en œuvre un programme de maintenance et d'essai des *systèmes de contrôle des accès physiques* et des équipements ou dispositifs installés localement au *périmètre de sécurité physique,* mais a terminé l'essai exigé dans un délai de plus de 25 mois civils et d'au plus 26 mois civils. | L'entité responsable a documenté et mis en œuvre un programme de maintenance et d'essai des *systèmes de contrôle des accès physiques* et des équipements ou dispositifs installés localement au *périmètre de sécurité physique,* mais a terminé l'essai exigé dans un délai de plus de 26 mois civils et d'au plus 27 mois civils. | L'entité responsable n'a pas documenté et mis en œuvre un programme de maintenance et d'essai des *systèmes de contrôle des accès physiques* et des équipements ou dispositifs installés localement au *périmètre de sécurité physique.* (3.1)<br>OU<br>L'entité responsable a |

| Ex. | Horizon | VRF | Niveaux de gravité de la non-conformité (CIP-006-6) | | | |
|---|---|---|---|---|---|---|
| | | | VSL faible | VSL modéré | VSL élevé | VSL critique |
| | | | (3.1) | (3.1) | (3.1) | documenté et mis en œuvre un programme de maintenance et d'essai des *systèmes de contrôle des accès physiques* et des équipements ou dispositifs installés localement au *périmètre de sécurité physique,* mais n'a pas terminé l'essai exigé dans un délai de 27 mois civils. (3.1) |

## D. Différences régionales

Aucune.

## E. Interprétations

Aucune.

## F. Documents connexes

Aucun.

## Historique des versions

| Version | Date | Intervention | Suivi des modifications |
|---|---|---|---|
| 1 | 16 janvier 2006 | E3.2 — Remplacement de « Control Center » par « control center » dans la version anglaise. | 24 mars 2006 |
| 2 | 30 septembre 2009 | Modifications visant à clarifier les exigences et à mettre les éléments de conformité en concordance avec les plus récentes directives sur l'établissement des éléments de conformité des normes.<br>Suppression de la mention sur la prise en compte des considérations d'affaires.<br>Remplacement de l'organisation régionale de fiabilité par l'entité régionale comme entité responsable.<br>Reformulation de la date d'entrée en vigueur.<br>Remplacement de « Responsabilité de la surveillance de la conformité » par « Responsabilité du contrôle de la conformité ». | |
| 3 | 16 décembre 2009 | Changement du numéro de version de -2 à -3.<br>À l'exigence 1.6, suppression de la phrase traitant de la mise hors service d'un composant ou d'un système en vue d'effectuer la vérification conformément à l'ordonnance de la FERC du 30 septembre 2009. | |

| Version | Date | Intervention | Suivi des modifications |
|---|---|---|---|
| 3 | 16 décembre 2009 | Approbation par le Conseil d'administration de la NERC. | |
| 3 | 31 mars 2010 | Approbation par la FERC. | |
| 4 | 24 janvier 2011 | Approbation par le Conseil d'administration de la NERC. | |
| 5 | 26 novembre 2012 | Adoption par le Conseil d'administration de la NERC. | Modification en coordination avec les autres normes CIP et révision du format selon le modèle RBS. |
| 5 | 22 novembre 2013 | Ordonnance de la FERC approuvant CIP-006-5. | |
| 5 | 9 juillet 2014 | Lettre d'ordonnance de la FERC approuvant les révisions des VRF et des VSL de certaines normes CIP. | L'exigence E3 de la norme CIP-006-5 passe de faible à moyen. |
| 6 | 13 novembre 2014 | Adoption par le Conseil d'administration de la NERC. | |
| 6 | 21 janvier 2016 | Ordonnance de la FERC émise approuvant CIP-003-6. Dossier no. RM15-14-000 | |

## 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) présente 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, les normes CIP sur la cybersécurité de la NERC s'y appliquent. Il est à noter qu'en ce qui concerne les *distributeurs*, la section 4.1 limite l'applicabilité 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 qui, selon la section 4.1, est visée par les exigences de la norme. Comme il est indiqué à la section d'exemption 4.2.3.5, la présente norme ne s'applique pas aux entités responsables qui n'ont pas de *systèmes électroniques BES* à impact élevé ou moyen selon la catégorisation de la norme CIP-002-5.1. 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* » dans le glossaire de la NERC indique déjà qu'il s'agit d'*éléments* du *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 aide à clarifier quels sont les *installations*, systèmes et équipements visés par les normes.

**Généralités**

Même si l'accent de cette norme de fiabilité n'est plus mis sur l'établissement et la gestion d'un périmètre physique complètement étanche (« à six parois »), il est attendu que dans de nombreux cas un périmètre à six parois demeurera le mécanisme principal pour le contrôle et la journalisation des accès aux *systèmes électroniques BES* et le déclenchement des alertes afférentes. Ensemble, les mécanismes décrits ci-après constitueront de fait le plan de sécurité physique permettant de gérer les accès physiques aux *systèmes électroniques BES*.

**Exigence E1**

Les méthodes de contrôle des accès physiques comprennent :

- Carte d'accès : Un dispositif d'accès électronique pour lequel les droits d'accès du détenteur de la carte sont prédéfinis dans une base de données informatique. Les droits d'accès peuvent différer d'un périmètre à un autre.
- Systèmes de verrouillage : Ceux-ci incluent notamment les serrures à « clé à copie restreinte », les serrures magnétiques qui peuvent être déverrouillées à distance et les sas de sécurité.
- Personnel de sécurité : Personne responsable de la surveillance des accès physiques, qui peut se trouver sur place ou dans un poste de surveillance à distance.

- Autres dispositifs d'authentification : Lecteur biométrique, clavier numérique, jeton ou tout autre dispositif équivalent permettant de contrôler l'accès physique au *périmètre de sécurité physique*.

Les méthodes de surveillance des accès physiques comprennent :

- Système d'alarme : Système qui produit une alarme pour indiquer qu'un mouvement a été détecté à l'intérieur d'un périmètre ou qu'une porte, une barrière ou une fenêtre a été ouverte sans autorisation. L'alarme doit être signalée au personnel d'intervention désigné dans un délai d'au plus 15 minutes.
- Postes de garde : Surveillance des points d'accès physique assurée par le personnel chargé de contrôler les accès physiques.

Les méthodes de journalisation des accès comprennent :

- Registre informatisé : Journal électronique produit par le système de contrôle d'accès et d'alerte adopté par l'entité responsable.
- Enregistrement vidéo : Saisie électronique d'images vidéo de qualité suffisante pour permettre l'identification d'une personne.
- Registre manuel : Journal, feuille de signature ou autre relevé des accès physiques tenu par un gardien de sécurité ou une autre personne autorisée à contrôler et à surveiller les accès physiques.

L'ordonnance 706 de la FERC, paragraphe 572, donne pour directive d'utiliser au moins deux mécanismes différents et complémentaires pour le contrôle des accès physiques afin d'assurer une défense en profondeur. Elle n'exige pas l'utilisation d'un minimum de deux *périmètres de sécurité physique* et elle n'exclut pas l'utilisation de périmètres en couches. En présence d'un périmètre de sécurité physique unique, il serait acceptable d'utiliser au point d'accès une authentification à deux facteurs. Dans ce cas, les mécanismes de contrôle pourraient comprendre par exemple une carte d'accès combinée à un code NIP (élément détenu par l'utilisateur et élément connu de l'utilisateur), une carte d'accès combinée à un lecteur biométrique (élément détenu par l'utilisateur et élément qui le caractérise) ou encore une clé physique combinée à une serrure de porte et à une télécaméra de surveillance, où un gardien disposerait des renseignements nécessaires pour authentifier les personnes, en les observant ou en leur parlant, avant de leur accorder un accès (élément détenu par l'utilisateur et élément qui le caractérise). Il est possible de mettre en œuvre l'authentification à deux facteurs au moyen d'un seul *système de contrôle des accès physiques*, à condition d'utiliser plus d'une méthode d'authentification. En présence d'un périmètre de sécurité physique en couches, il serait acceptable de combiner une barrière verrouillée et un bâtiment de contrôle verrouillé, à condition que l'accès à ces deux points d'entrée ne puisse être autorisé à l'aide du même facteur d'authentification (comme une clé ou une carte d'accès).

Les entités peuvent choisir de situer certains *PACS* à l'intérieur d'un *périmètre de sécurité physique* pour contrôler les accès aux *systèmes électroniques BES* visés. Ces *PACS* n'ont pas à respecter les alinéas 1.1, 1.6 et 1.7 de l'exigence E1 en plus de ce qui s'applique déjà au *périmètre de sécurité physique*.

Le nouvel alinéa 1.10 de l'exigence E1 de la norme CIP-006-6 met en œuvre la prescription du paragraphe 150 de l'ordonnance 791 de la FERC. Cette exigence vise la protection du câblage et des composants de communication non programmables situés à l'intérieur d'un *périmètre de sécurité électronique* (*ESP*), mais qui se prolonge à l'extérieur d'un *périmètre de sécurité physique* (*PSP*). Cette protection, qui rejoint la description faite dans la demande de validation de l'interprétation fournie à PacifiCorp sur la norme CIP-006-2, présentée par la NERC et acceptée par la FERC, doit être réalisée soit par la protection physique des câbles et composants qui sortent d'un *PSP* (par exemple au moyen de conduits ou de chemins de câbles sécurisés), soit par le cryptage des données, par la surveillance des circuits ou par une protection logique d'une efficacité équivalente. Il s'agit de faire en sorte que les protections physiques réduisent la possibilité de sabotage ou d'accès direct aux dispositifs non programmables. Les conduits, les chemins de câbles sécurisés et les armoires de communication sécurisées sont des exemples de ces types de protection. Ces mesures de sécurité physique doivent être mises en œuvre façon à permettre de détecter ou de constater après coup le sabotage possible du câblage et des composants non programmables. Il pourrait s'agir d'un simple cadenas sur une armoire de communication si l'entité est en mesure de constater que le cadenas a été coupé. Un autre moyen pourrait être un câblage armé ou encore le tube en acier inoxydable ou en aluminium qui protège la fibre à l'intérieur d'un câble de garde à fibre optique (CGFO). Lorsqu'on utilise l'une de ces diverses méthodes, il faut prendre soin de protéger toute la longueur du câblage, y compris les points de raccordement qui peuvent se trouver à l'extérieur d'un *PSP*.

Cette partie de l'exigence vise uniquement les portions du câblage et des composants de communication non programmables qui se trouvent à l'extérieur du *PSP*, mais à l'intérieur de l'*ESP*. Dès que ce câblage et ces composants de communication non programmables sont situés à l'intérieur du *PSP*, cette partie de l'exigence ne s'applique plus.

L'exigence porte spécifiquement sur la protection physique du câblage et des composants de communication, puisqu'elle fait partie d'une norme sur la sécurité physique et que la lacune de protection indiquée dans l'ordonnance 791 de la FERC concerne la protection physique. Cependant, cette partie de l'exigence reconnaît qu'il existe plusieurs manières d'assurer la protection du câblage et des composants de communication non programmables. En particulier, l'exigence permet à l'entité d'opter pour une solution autre qu'une protection physique dans une situation où l'entité ne peut pas mettre en œuvre une protection physique, ou si elle choisit simplement de ne pas mettre en œuvre une telle protection. L'entité n'est nullement tenue de justifier ou d'expliquer pourquoi elle a opté pour des protections logiques plutôt que pour les mesures physiques indiquées dans l'exigence.

Les mesures de protection non physique indiquées à l'alinéa 1.10 de l'exigence E1 de la norme CIP-006-6 (cryptage et surveillance des circuits) ont été jugées acceptables dans la demande de validation de l'interprétation fournie à PacifiCorp sur la norme CIP-006-2, présentée par la NERC et acceptée par la FERC (RD10-13-000). Si une entité choisit de mettre en œuvre « une protection logique d'une efficacité équivalente » au lieu des mécanismes de protection indiqués dans la norme, l'entité devrait normalement documenter pourquoi elle considère cette protection comme étant d'une efficacité équivalente. La NERC explique dans sa requête sur l'interprétation fournie à PacifiCorp sur la norme CIP-006-2 que les mesures concernent

l'accès ainsi que le sabotage physique. Par conséquent, l'entité peut choisir d'indiquer comment sa protection peut assurer la détection du sabotage. L'entité peut aussi choisir d'expliquer comment sa protection est équivalente aux autres options logiques présentées dans la norme relativement à la triade « confidentialité, intégrité et disponibilité ». L'entité peut trouver utile de soumettre ses plans à l'entité régionale avant la mise en œuvre, mais elle n'est pas tenue de le faire.

Cette exigence ne spécifie pas de protection physique pour des équipements de tiers, comme l'indique l'ordonnance 791-A de la FERC. L'exigence accorde à l'entité la latitude voulue pour concevoir son *ESP* et aussi pour le prolonger à l'extérieur de son *PSP* au moyen des mécanismes logiques spécifiés à la partie 1.10 de l'exigence E1 de la norme CIP-006-6, notamment le cryptage (option indiquée nommément dans l'ordonnance 791-A de la FERC). Ces mécanismes devraient offrir aux *systèmes électroniques BES* de l'entité une protection suffisante pour qu'il ne soit pas nécessaire d'appliquer des mesures à des équipements de tiers lorsque l'entité utilise des liaisons de communication louées.

En plus du câblage, les composants visés par cette partie de l'exigence sont les composants situés à l'extérieur d'un *PSP* et qui pourraient presque être considérés comme des *actifs électroniques BES* ou des *actifs électroniques protégés*, sauf qu'ils ne répondent pas à la définition d'*actif électronique* puisqu'ils ne sont pas programmables. Exemples non limitatifs de tels composants non programmables : commutateurs, concentrateurs, panneaux de répartition, convertisseurs de support, adaptateurs de port et raccords non gérés.

**Exigence E2**

Les données d'accès des visiteurs doivent être consignées une seule fois par visite et non chaque fois que le visiteur entre dans le *périmètre de sécurité physique* et qu'il en sort durant sa visite, et ce, afin de permettre au visiteur de sortir temporairement du périmètre au besoin (pour aller récupérer un objet à l'extérieur, par exemple) sans avoir à s'enregistrer chaque fois pour y entrer de nouveau.

La SDT a également établi qu'il faudrait consigner le nom d'un répondant en mesure de fournir des renseignements supplémentaires sur une visite dans l'éventualité où l'on aurait besoin de réponses à certaines questions. Ce répondant peut être l'accompagnateur du visiteur, mais il n'est pas nécessaire de consigner le nom de toutes les personnes qui ont accompagné un visiteur.

**Exigence E3**

Cette exigence introduit les essais à effectuer sur l'équipement et les dispositifs installés localement pour assurer le contrôle des accès aux *périmètres de sécurité physique*, ainsi que le déclenchement d'alertes et la consignation de données les concernant. Il s'agit notamment des détecteurs de mouvement, des mécanismes de verrouillage électroniques et des lecteurs de carte d'accès, qui ne sont pas considérés comme faisant partie du *système de contrôle des accès physiques*, mais qui sont nécessaires à la protection des *systèmes électroniques BES*.

## Justification :

Pendant l'élaboration de cette norme, des zones de texte ont été incorporées à celle-ci pour exposer la justification de ses diverses parties. Après l'approbation par le Conseil d'administration, le contenu de ces zones de texte a été transféré ci-après.

**Justification de l'exigence E1 :**

Chaque entité responsable doit s'assurer de restreindre et de gérer adéquatement les accès physiques à tous les *systèmes électroniques BES*. Les entités peuvent choisir de situer certains *PACS* à l'intérieur d'un *périmètre de sécurité physique* pour contrôler les accès aux *systèmes électroniques BES* visés. Ces *PACS* n'ont pas à respecter les alinéas 1.1, 1.6 et 1.7 de l'exigence E1 en plus de ce qui s'applique déjà au *périmètre de sécurité physique*.

Quant à l'alinéa 1.10 de l'exigence E1, lorsque des câbles ou autres composants non programmables du réseau de communication d'un *centre de contrôle* ne peuvent pas être sécurisés dans un *périmètre de sécurité physique* (*PSP*), il faut prendre des mesures pour assurer l'intégrité des *systèmes électroniques BES*. Si des trajets de communication sont exposés à l'extérieur d'un *PSP*, il faut mettre en place des protections physiques ou logiques afin de réduire la probabilité que des attaques par interposition puissent compromettre l'intégrité des *actifs électroniques BES* raccordés ou des *PCA* qui doivent résider dans des *PSP*. Bien qu'il convienne d'envisager d'abord une protection physique du câblage et des composants de communication non programmables, la SDT comprend que certaines configurations se prêtent mal à des restrictions d'accès physique et que les entités responsables sont en mesure de défendre raisonnablement leurs composants de communication exposés physiquement au moyen de protections logiques supplémentaires.

**Justification de l'exigence E2 :**

Il s'agit de contrôler quand le personnel n'ayant pas un accès physique autorisé sans accompagnement peut se trouver à l'intérieur d'un *périmètre de sécurité physique* protégeant des *systèmes électroniques BES*, ou des *systèmes de contrôle ou de surveillance des accès électroniques*, selon le tableau E2.

**Justification de l'exigence E3 :**

Il s'agit de faire en sorte que tous les dispositifs et *systèmes de contrôle des accès physiques* continuent de fonctionner correctement.

Annexe QC-CIP-006-6
Dispositions particulières de la norme CIP-006-6 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 — Sécurité physique des systèmes électroniques BES

2. **Numéro :** CIP-006-6

3. **Objet :** Aucune disposition particulière

4. **Applicabilité :**

**4.1. Entités Fonctionnelles**

Aucune disposition particulière

**4.2. 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.

**Exemptions additionnelles**

Sont exemptés de l'application de la présente norme :

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

5. **Date d'entrée en vigueur au Québec :**

**5.1.** Adoption de la norme par la Régie de l'énergie : 31 octobre 2017

**5.2.** Adoption de l'annexe par la Régie de l'énergie : 31 octobre 2017

**5.3.** Date d'entrée en vigueur de la norme et de l'annexe au Québec : 1er janvier 2018

| Norme | Date de mise en application au Québec | | |
|---|---|---|---|
| | Entités visées par la version 1 des normes CIP adoptées par la Régie | Entités exemptées de l'application de la version 1 des normes CIP en vertu des dispositions particulières associées à ces normes | Entités qui possèdent des installations de production à vocation industrielle |
| CIP-006-6 | 2018-01-01 | 2018-10-01 | 2019-04-01 |

**6. Contexte :**

Aucune disposition particulière

## B. Exigences et mesures

Aucune disposition particulière

## C. Conformité

**1. Processus de surveillance de la conformité**

**1.1. Responsable des mesures pour assurer la conformité**

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

**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

## Justification

Aucune disposition particulière

## Historique des versions

| Révision | Date | Intervention | Suivi des modifications |
|---|---|---|---|
| 0 | 31 octobre 2017 | Nouvelle annexe. | Nouvelle |