

## A. Introduction

1. **Titre :** Cybersécurité – Mécanismes de gestion de la sécurité
2. **Numéro :** CIP-003-6
3. **Objet :** Définir des mécanismes de gestion de la sécurité cohérents et viables qui établissent les responsabilités et l'imputabilité à l'égard de la protection des *systèmes électroniques BES* contre les compromissions qui pourraient entraîner un fonctionnement incorrect ou des instabilités 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 systèmes, *installations*, 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 par 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* est 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-003-6 :

**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 *périmètres de sécurité électroniques* (ESP) 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.

**5. Dates d'entrée en vigueur :**

Voir le plan de mise en œuvre de la norme CIP-003-6.

**6. Contexte :**

La norme CIP-003 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*.

Le mot « politique » désigne un ou plusieurs documents écrits qui servent à communiquer les buts, objectifs et attentes de gestion de l'entité responsable quant à la manière dont celle-ci entend protéger ses systèmes électroniques BES. L'adoption de politiques permet aussi d'établir un cadre de gouvernance global qui favorise le développement d'une culture de sécurité et de conformité aux lois, règlements et normes.

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, moyen et faible. Par exemple, un même programme de sensibilisation à la cybersécurité pourrait répondre aux exigences en formation du personnel concernant plusieurs *systèmes électroniques BES*.

Les mesures présentent des exemples de pièces justificatives attestant 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 doivent 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 *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.

## B. Exigences et mesures

- E1.** Chaque entité responsable doit réexaminer et faire approuver par un *cadre supérieur CIP*, au moins une fois tous les 15 mois civils, une ou plusieurs politiques de cybersécurité documentées qui, collectivement, couvrent les thèmes suivants :  
[Facteur de risque de non-conformité : moyen] [Horizon : planification de l'exploitation]
- 1.1** Pour ses systèmes électroniques BES à impact élevé ou moyen, le cas échéant :
- 1.1.1.** personnel et formation (CIP-004) ;
  - 1.1.2.** *périmètres de sécurité électronique* (CIP-005), y compris l'*accès distant interactif* ;
  - 1.1.3.** sécurité physique des *systèmes électroniques BES* (CIP-006) ;
  - 1.1.4.** gestion de la sécurité des systèmes (CIP-007) ;
  - 1.1.5.** déclaration des incidents et planification des mesures d'intervention (CIP-008) ;
  - 1.1.6.** plans de rétablissement des *systèmes électroniques BES* (CIP-009) ;
  - 1.1.7.** gestion des changements de configuration et analyses de vulnérabilité (CIP-010) ;
  - 1.1.8.** protection de l'information (CIP-011) ; et
  - 1.1.9.** déclaration et réponse aux *circonstances CIP exceptionnelles*.
- 1.2** Pour ses actifs qui comportent des *systèmes électroniques BES* à impact faible selon les critères de la norme CIP-002, le cas échéant :
- 1.2.1.** sensibilisation à la cybersécurité ;
  - 1.2.2.** mesures de sécurité physique ;
  - 1.2.3.** contrôle des accès électroniques pour toute *connectivité externe routable à impact faible* (LERC) et la *connectivité par lien commuté* ; et
  - 1.2.4.** intervention en cas d'*incident de cybersécurité*.
- M1.** Exemples non limitatifs de pièces justificatives : documents de politique ; historique de révisions, dossiers d'examen ou preuves de flux de travail provenant d'un système de gestion documentaire qui attestent le réexamen de chaque politique de cybersécurité au moins une fois tous les 15 mois civils ; et approbation documentée de chaque politique de cybersécurité par le *cadre supérieur CIP*.
- E2.** Chaque entité responsable qui détient au moins un actif comportant des *systèmes électroniques BES* à impact faible, selon les critères de la norme CIP-002, doit mettre en œuvre pour ses *systèmes électroniques BES* à impact faible un ou plusieurs plans de

cybersécurité documentés conformes à toutes les sections de l'annexe 1.

*[Facteur de risque de non-conformité : faible] [Horizon : planification de l'exploitation]*

Remarque : Un inventaire, une liste ou une identification distincte des *systèmes électroniques BES* à impact faible ou de leurs *actifs électroniques BES* n'est pas exigé. Des listes d'utilisateurs autorisés ne sont pas exigées.

- M2.** Les pièces justificatives doivent comporter chacun des plans de cybersécurité qui, collectivement, couvrent toutes les sections de l'annexe 1 ; d'autres pièces justificatives doivent attester la mise en œuvre des plans de cybersécurité. L'annexe 2 présente d'autres exemples de pièces justificatives pour chacune des sections de l'annexe 1.
- E3.** Chaque entité responsable doit désigner nominativement un *cadre supérieur CIP* et documenter tout changement dans un délai de 30 jours civils suivant le changement.  
*[Facteur de risque de non-conformité : moyen] [Horizon : planification de l'exploitation]*
- M3.** Exemple non limitatif de pièce justificative : document daté et approuvé par un haut dirigeant indiquant le nom de la personne désignée comme *cadre supérieur CIP*.
- E4.** L'entité responsable doit mettre en œuvre un processus documenté de délégation de pouvoirs, sauf en l'absence de toute délégation. Dans les cas permis par les normes CIP, le *cadre supérieur CIP* peut déléguer ses pouvoirs relatifs à certains actes à un ou plusieurs délégataires. Ces délégations doivent être documentées, et comprendre notamment le nom ou le titre du délégataire, les actes délégués et la date de la délégation ; être approuvées par le *cadre supérieur CIP* ; et être mises à jour dans un délai de 30 jours suivant tout changement à la délégation. Il n'est pas nécessaire de réaffirmer les changements de délégation en cas de changement de délégant.  
*[Facteur de risque de non-conformité : faible] [Horizon : planification de l'exploitation]*
- M4.** Exemple non limitatif de pièce justificative : document daté et approuvé par le *cadre supérieur CIP* indiquant la ou les personnes (nom ou titre) auxquelles est délégué le pouvoir d'approuver ou d'autoriser des actions décrites explicitement.

## 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 pour assurer la conformité* » (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-003-6)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
E1	Planification de l'exploitation	Moyen	<p>L'entité responsable a documenté et mis en œuvre une ou plusieurs politiques de cybersécurité pour ses <i>systèmes électroniques BES</i> à impact élevé et moyen, mais il n'a pas traité de l'un des neuf thèmes indiqués à l'exigence E1. (E1.1)</p> <p>OU</p> <p>L'entité responsable a terminé le réexamen de sa ou ses politiques de cybersécurité documentées pour ses <i>systèmes électroniques BES</i> à impact élevé et moyen selon l'exigence E1, mais dans un délai de plus de 15 mois civils et d'au plus 16 mois civils suivant le réexamen précédent. (E1.1)</p> <p>OU</p> <p>L'entité responsable a fait approuver par le <i>cadre supérieur CIP</i> sa ou ses politiques de cybersécurité</p>	<p>L'entité responsable a documenté et mis en œuvre une ou plusieurs politiques de cybersécurité pour ses <i>systèmes électroniques BES</i> à impact élevé et moyen, mais en omettant deux des neuf thèmes indiqués à l'exigence E1. (E1.1)</p> <p>OU</p> <p>L'entité responsable a terminé le réexamen de sa ou ses politiques de cybersécurité documentées pour ses <i>systèmes électroniques BES</i> à impact élevé et moyen selon l'exigence E1, mais dans un délai de plus de 16 mois civils et d'au plus 17 mois civils suivant le réexamen précédent. (E1.1)</p> <p>OU</p> <p>L'entité responsable a fait approuver par le <i>cadre supérieur CIP</i> sa ou ses politiques de cybersécurité</p>	<p>L'entité responsable a documenté et mis en œuvre une ou plusieurs politiques de cybersécurité pour ses <i>systèmes électroniques BES</i> à impact élevé et moyen, mais en omettant trois des neuf thèmes indiqués à l'exigence E1. (E1.1)</p> <p>OU</p> <p>L'entité responsable a terminé le réexamen de sa ou ses politiques de cybersécurité documentées pour ses <i>systèmes électroniques BES</i> à impact élevé et moyen selon l'exigence E1, mais dans un délai de plus de 17 mois civils et d'au plus 18 mois civils suivant le réexamen précédent. (E1.1)</p> <p>OU</p> <p>L'entité responsable a fait approuver par le <i>cadre supérieur CIP</i> sa ou ses politiques de cybersécurité</p>	<p>L'entité responsable a documenté et mis en œuvre une ou plusieurs politiques de cybersécurité pour ses <i>systèmes électroniques BES</i> à impact élevé et moyen, mais en omettant au moins quatre des neuf thèmes indiqués à l'exigence E1. (E1.1)</p> <p>OU</p> <p>L'entité responsable n'avait aucune politique de cybersécurité documentée pour ses <i>systèmes électroniques BES</i> à impact élevé et moyen, comme le prescrit l'exigence E1. (E1.1)</p> <p>OU</p> <p>L'entité responsable n'a pas terminé le réexamen de sa ou ses politiques de cybersécurité selon l'exigence E1 dans un délai de 18 mois civils suivant le réexamen précédent. (E1)</p> <p>OU</p>



Ex.	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-003-6)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
			documentées pour ses <i>systèmes électroniques BES</i> à impact élevé et moyen selon l'exigence E1, mais dans un délai de plus de 15 mois civils et d'au plus 16 mois civils suivant l'approbation précédente. (E1.1)  OU  L'entité responsable a documenté une ou plusieurs politiques de cybersécurité pour ses actifs qui comportent des <i>systèmes électroniques BES</i> à impact faible selon les critères de la norme CIP-002, mais en omettant un des quatre thèmes indiqués à l'exigence E1. (E1.2)  OU  L'entité responsable a terminé le réexamen, selon l'exigence E1, de sa ou ses politiques de cybersécurité documentées pour ses actifs qui comportent des <i>systèmes électroniques</i>	documentées pour ses <i>systèmes électroniques BES</i> à impact élevé et moyen selon l'exigence E1, mais dans un délai de plus de 16 mois civils et d'au plus 17 mois civils suivant l'approbation précédente. (E1.1)  OU  L'entité responsable a documenté une ou plusieurs politiques de cybersécurité pour ses actifs qui comportent des <i>systèmes électroniques BES</i> à impact faible selon les critères de la norme CIP-002, mais en omettant deux des quatre thèmes indiqués à l'exigence E1. (E1.2)  OU  L'entité responsable a terminé le réexamen, selon l'exigence E1, de sa ou ses politiques de cybersécurité documentées pour ses actifs qui comportent des <i>systèmes électroniques</i>	documentées pour ses <i>systèmes électroniques BES</i> à impact élevé et moyen selon l'exigence E1, mais dans un délai de plus de 17 mois civils et d'au plus 18 mois civils suivant l'approbation précédente. (E1)  OU  L'entité responsable a documenté une ou plusieurs politiques de cybersécurité pour ses actifs qui comportent des <i>systèmes électroniques BES</i> à impact faible selon les critères de la norme CIP-002, mais en omettant trois des quatre thèmes indiqués à l'exigence E1. (E1.2)  OU  L'entité responsable a terminé le réexamen, selon l'exigence E1, de sa ou ses politiques de cybersécurité documentées pour ses actifs qui comportent des <i>systèmes électroniques</i>	L'entité responsable n'a pas fait approuver par le <i>cadre supérieur CIP</i> sa ou ses politiques de cybersécurité documentées pour ses <i>systèmes électroniques BES</i> à impact élevé et moyen selon l'exigence E1 dans un délai de 18 mois civils suivant l'approbation précédente. (E1.1)  OU  L'entité responsable a documenté une ou plusieurs politiques de cybersécurité pour ses actifs qui comportent des <i>systèmes électroniques BES</i> à impact faible selon les critères de la norme CIP-002, mais en omettant les quatre thèmes indiqués à l'exigence E1. (E1.2)  OU  L'entité responsable n'avait aucune politique de cybersécurité documentée, selon l'exigence E1, pour ses actifs qui comportent des

Ex.	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-003-6)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
			<p><i>BES</i> à impact faible selon les critères de la norme CIP-002, mais dans un délai de plus de 15 mois civils et d'au plus 16 mois civils suivant le réexamen précédent. (E1.2)</p> <p>OU</p> <p>L'entité responsable a fait approuver par le <i>cadre supérieur CIP</i>, selon l'exigence E1, sa ou ses politiques de cybersécurité documentées pour ses actifs qui comportent des <i>systèmes électroniques BES</i> à impact faible selon les critères de la norme CIP-002, mais dans un délai de plus de 15 mois civils et d'au plus 16 mois civils suivant l'approbation précédente. (E1.2)</p>	<p><i>BES</i> à impact faible selon les critères de la norme CIP-002, mais dans un délai de plus de 16 mois civils et d'au plus 17 mois civils suivant le réexamen précédent. (E1.2)</p> <p>OU</p> <p>L'entité responsable a fait approuver par le <i>cadre supérieur CIP</i>, selon l'exigence E1, sa ou ses politiques de cybersécurité documentées pour ses actifs qui comportent des <i>systèmes électroniques BES</i> à impact faible selon les critères de la norme CIP-002, mais dans un délai de plus de 16 mois civils et d'au plus 17 mois civils suivant l'approbation précédente. (E1.2)</p>	<p><i>BES</i> à impact faible selon les critères de la norme CIP-002, mais dans un délai de plus de 17 mois civils et d'au plus 18 mois civils suivant le réexamen précédent. (E1.2)</p> <p>OU</p> <p>L'entité responsable a fait approuver par le <i>cadre supérieur CIP</i>, selon l'exigence E1, sa ou ses politiques de cybersécurité documentées pour ses actifs qui comportent des <i>systèmes électroniques BES</i> à impact faible selon les critères de la norme CIP-002, mais dans un délai de plus de 17 mois civils et d'au plus 18 mois civils suivant l'approbation précédente. (E1.2)</p>	<p><i>systèmes électroniques BES</i> à impact faible selon les critères de la norme CIP-002. (E1.2)</p> <p>OU</p> <p>L'entité responsable n'a pas fait approuver par le <i>cadre supérieur CIP</i>, selon l'exigence E1, sa ou ses politiques de cybersécurité documentées pour ses actifs qui comportent des <i>systèmes électroniques BES</i> à impact faible selon les critères de la norme CIP-002, dans un délai de 18 mois civils suivant l'approbation précédente. (E1.2)</p>
E2	Planification de l'exploitation	Faible	<p>L'entité responsable a documenté son ou ses plans de cybersécurité pour ses actifs comportant des <i>systèmes électroniques BES</i> à impact faible, mais n'a pas documenté son plan de sensibilisation à la cybersécurité</p>	<p>L'entité responsable a documenté son ou ses plans de cybersécurité pour ses actifs comportant des <i>systèmes électroniques BES</i> à impact faible, mais n'a pas fait de rappel des pratiques de cybersécurité au moins une fois tous les 15 mois</p>	<p>L'entité responsable a documenté un ou plusieurs plans d'intervention en cas d'<i>incident de cybersécurité</i> dans le cadre de son ou ses plans de cybersécurité pour ses actifs comportant des <i>systèmes électroniques BES</i> à impact faible, mais n'a pas</p>	<p>L'entité responsable n'a pas documenté ou mis en œuvre un ou plusieurs plans de cybersécurité pour ses actifs comportant des <i>systèmes électroniques BES</i> à impact faible conformément à l'annexe 1 portant sur l'exigence E2 de</p>

Ex.	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-003-6)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
			<p>conformément à la section 1 de l'annexe 1 portant sur l'exigence E2 de la norme CIP-003-6. (E2)</p> <p>OU</p> <p>L'entité responsable a documenté son ou ses plans de cybersécurité pour ses actifs comportant des <i>systèmes électroniques BES</i> à impact faible, mais n'a pas documenté un ou plusieurs plans d'intervention en cas d'<i>incident de cybersécurité</i> conformément à la section 4 de l'annexe 1 portant sur l'exigence E2 de la norme CIP-003-6. (E2)</p> <p>OU</p> <p>L'entité responsable a documenté un ou plusieurs plans d'intervention en cas d'<i>incident de cybersécurité</i> dans le cadre de son ou ses plans de cybersécurité pour ses actifs comportant des <i>systèmes électroniques BES</i> à impact faible, mais n'a pas mis à jour chaque plan d'intervention en cas d'<i>incident de cybersécurité</i></p>	<p>civils conformément à la section 1 de l'annexe 1 portant sur l'exigence E2 de la norme CIP-003-6. (E2)</p> <p>OU</p> <p>L'entité responsable a documenté un ou plusieurs plans d'intervention en cas d'<i>incident</i> dans le cadre de son ou ses plans de cybersécurité pour ses actifs comportant des <i>systèmes électroniques BES</i> à impact faible, mais n'a pas inclus le processus de détection, de classement et d'intervention en cas d'<i>incident de cybersécurité</i> conformément à la section 4 de l'annexe 1 portant sur l'exigence E2 de la norme CIP-003-6. (E2)</p> <p>OU</p> <p>L'entité responsable a documenté son ou ses plans de cybersécurité pour ses actifs comportant des <i>systèmes électroniques BES</i> à impact faible, mais n'a pas documenté le processus consistant à déterminer si</p>	<p>mis à l'essai chaque plan d'intervention en cas d'<i>incident de cybersécurité</i> au moins une fois tous les 36 mois civils conformément à la section 4 de l'annexe 1 portant sur l'exigence E2 de la norme CIP-003-6. (E2)</p> <p>OU</p> <p>L'entité responsable a documenté le processus consistant à déterminer si un <i>incident de cybersécurité</i> constaté est un <i>incident de cybersécurité à déclarer</i>, mais n'a pas avisé l'Electricity Sector Information Sharing and Analysis Center (ES-ISAC) conformément à la section 4 de l'annexe 1 portant sur l'exigence E2 de la norme CIP-003-6. (E2)</p> <p>OU</p> <p>L'entité responsable a documenté et mis en œuvre un contrôle des accès électroniques pour les <i>LERC</i>, mais n'a pas mis en place un <i>LEAP</i> ou géré les</p>	la norme CIP-003-6. (E2)

Ex.	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-003-6)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
			<p>dans un délai de 180 jours conformément à la section 4 de l'annexe 1 portant sur l'exigence E2 de la norme CIP-003-6. (E2)</p>	<p>un <i>incident de cybersécurité</i> constaté est un <i>incident de cybersécurité à déclarer</i>, puis à en aviser l'Electricity Sector Information Sharing and Analysis Center (ES-ISAC) conformément à la section 4 de l'annexe 1 portant sur l'exigence E2 de la norme CIP-003-6.</p> <p>OU</p> <p>L'entité responsable a documenté son ou ses plans de cybersécurité pour ses actifs comportant des <i>systèmes électroniques BES</i> à impact faible, mais n'a pas documenté de mesures de sécurité physique conformément à la section 2 de l'annexe 1 portant sur l'exigence E2 de la norme CIP-003-6. (E2)</p> <p>OU</p> <p>L'entité responsable a documenté son ou ses plans de cybersécurité pour ses actifs comportant des <i>systèmes électroniques BES</i> à impact faible, mais n'a pas documenté le contrôle des</p>	<p>accès entrants et sortants conformément à la section 3 de l'annexe 1 portant sur l'exigence E2 de la norme CIP-003-6. (E2)</p> <p>OU</p> <p>L'entité responsable a documenté et mis en œuvre un contrôle des accès électroniques pour ses actifs comportant des <i>systèmes électroniques BES</i> à impact faible, mais n'a pas documenté et mis en place une authentification pour toutes les <i>connectivités par lien commuté</i> (s'il en existe) qui donnent accès à des <i>systèmes électroniques BES</i> à impact faible, conformément à la section 3 de l'annexe 1 portant sur l'exigence E2 de la norme CIP-003-6. (E2)</p> <p>OU</p> <p>L'entité responsable a documenté le contrôle des accès physiques pour ses actifs comportant des <i>systèmes électroniques BES</i> à impact faible, mais n'a pas</p>	

Ex.	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-003-6)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
				accès électroniques conformément à la section 3 de l'annexe 1 portant sur l'exigence E2 de la norme CIP-003-6. (E2)	mis en œuvre les mesures de sécurité physique conformément à la section 2 de l'annexe 1 portant sur l'exigence E2 de la norme CIP-003-6. (E2)	
<b>E3</b>	<b>Planification de l'exploitation</b>	<b>Moyen</b>	L'entité responsable a désigné nominativement un <i>cadre supérieur CIP</i> , mais a documenté un changement concernant celui-ci dans un délai de plus de 30 jours civils et de moins de 40 jours civils suivant ce changement. (E3)	L'entité responsable a désigné nominativement un <i>cadre supérieur CIP</i> , mais a documenté un changement concernant celui-ci dans un délai de plus de 40 jours civils et de moins de 50 jours civils suivant ce changement. (E3).	L'entité responsable a désigné nominativement un <i>cadre supérieur CIP</i> , mais a documenté un changement concernant celui-ci dans un délai de plus de 50 jours civils et de moins de 60 jours civils suivant ce changement. (E3).	L'entité responsable n'a pas désigné nominativement un <i>cadre supérieur CIP</i> .  OU L'entité responsable a désigné nominativement un <i>cadre supérieur CIP</i> , mais n'a pas documenté un changement concernant celui-ci dans un délai de 60 jours civils suivant ce changement.

Ex.	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-003-6)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
E4	Planification de l'exploitation	Faible	L'entité responsable a désigné un délégataire en indiquant son nom, son titre, la date de la délégation et les actes délégués, mais a documenté un changement à la délégation dans un délai de plus de 30 jours civils et de moins de 40 jours civils suivant ce changement. (E4)	L'entité responsable a désigné un délégataire en indiquant son nom, son titre, la date de la délégation et les actes délégués, mais a documenté un changement à la délégation dans un délai de plus de 40 jours civils et de moins de 50 jours civils suivant ce changement. (E4)	L'entité responsable a désigné un délégataire en indiquant son nom, son titre, la date de la délégation et les actes délégués, mais a documenté un changement à la délégation dans un délai de plus de 50 jours civils et de moins de 60 jours civils suivant ce changement. (E4)	<p>L'entité responsable a délégué des pouvoirs relatifs à des actes autorisés par les normes CIP, mais n'a pas mis en œuvre de processus pour la délégation des actes du <i>cadre supérieur CIP</i>. (E4)</p> <p>OU</p> <p>L'entité responsable a désigné un délégataire en indiquant son nom, son titre, la date de la délégation et les actes délégués, mais n'a pas documenté un changement à la délégation dans un délai de 60 jours civils suivant le changement. (E4)</p>

**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 ».	24 mars 2006
2	30 septembre 2009	<p>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.</p> <p>Suppression de la mention sur la prise en compte des considérations d'affaires.</p> <p>Remplacement de l'organisation régionale de fiabilité par l'entité régionale comme entité responsable.</p> <p>Reformulation de la date d'entrée en vigueur.</p> <p>Remplacement de « <i>responsable de la surveillance de la conformité</i> » par « <i>responsable des mesures pour assurer la conformité</i> ».</p>	
3	16 décembre 2009	<p>Changement du numéro de version de -2 à -3.</p> <p>Dans l'exigence E1.6, suppression de la phrase concernant le retrait du service d'un composant ou d'un système aux fins d'essais, en réponse à l'ordonnance de la FERC du 30 septembre 2009.</p>	
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 la norme CIP-003-5.	
6	13 novembre 2014	Adoption par le Conseil d'administration de la NERC.	Mise en œuvre de deux prescriptions de l'ordonnance 791 de la FERC concernant l'obligation de « détecter, évaluer et corriger » ainsi que les réseaux de communication
6	12 février 2015	Adoption par le Conseil d'administration de la NERC.	Remplace la version adoptée par le Conseil le 13 novembre 2014. La version à jour met en œuvre des prescriptions en instance de l'ordonnance 791 relativement aux actifs temporaires et aux <i>systèmes électroniques BES</i> à impact faible.



## CIP-003-6 – Annexe 1

### Exigences des plans de cybersécurité pour les actifs comportant des systèmes électroniques BES à impact faible

Les entités responsables doivent intégrer chacune des sections suivantes aux plans de cybersécurité prescrits à l'exigence E2.

Les entités responsables dont les *systèmes électroniques BES* appartiennent à plusieurs catégories d'impact peuvent utiliser les politiques, procédures et processus adoptés pour leurs *systèmes électroniques BES* à impact élevé ou moyen pour leurs plans de cybersécurité visant les systèmes à faible impact. Chaque entité responsable peut élaborer des plans de cybersécurité pour des actifs individuels ou pour des groupes d'actifs.

- Section 1.** Sensibilisation à la cybersécurité : Chaque entité responsable doit rappeler, au moins une fois tous les 15 mois civils, les pratiques de cybersécurité (lesquelles peuvent comprendre des pratiques de sécurité physiques connexes).
- Section 2.** Mesures de sécurité physique : Chaque entité responsable doit contrôler l'accès physique, d'après les besoins qu'elle détermine elle-même, 1) à l'actif ou aux emplacements des *systèmes électroniques BES* à impact faible à l'intérieur de l'actif, et 2) aux *points d'accès électronique de système électronique BES à impact faible (LEAP)*, s'il en existe.
- Section 3.** Contrôle des accès électroniques : Chaque entité responsable doit :
- 3.1** pour toute *LERC*, mettre en place un *LEAP* afin de permettre uniquement les accès entrants et sortants bidirectionnels par protocole routable nécessaires ; et
  - 3.2** mettre en place une authentification pour toute *connectivité par lien commuté* qui donne accès à des *systèmes électroniques BES* à impact faible, selon les capacités de l'*actif électronique*.
- Section 4.** Intervention en cas d'incident de cybersécurité : Chaque entité responsable doit avoir un ou plusieurs plans d'intervention en cas d'incident de cybersécurité, par actif ou par groupe d'actifs, qui doivent comprendre :
- 4.1** la détection et le classement des *incidents de cybersécurité*, ainsi que les mesures d'intervention ;
  - 4.2** le processus consistant à déterminer si un *incident de cybersécurité* détecté est un *incident de cybersécurité à déclarer*, puis à en aviser l'Electricity Sector Information Sharing and Analysis Center (ES-ISAC), à moins que la loi ne l'interdise ;
  - 4.3** l'établissement des rôles et responsabilités des groupes ou des personnes chargés d'intervenir en cas d'*incident de cybersécurité* ;
  - 4.4** la gestion des *incidents de cybersécurité* ;

- 4.5** la mise à l'essai des plans d'intervention en cas d'*incident de cybersécurité* au moins une fois tous les 36 mois civils : 1) en répondant à un *incident de cybersécurité à déclarer* réel ; 2) en effectuant un exercice d'entraînement ou sur table de réponse à un *incident de cybersécurité à déclarer* ; ou 3) en effectuant un exercice opérationnel de réponse à un *incident de cybersécurité à déclarer* ; et
- 4.6** la mise à jour des plans d'intervention en cas d'*incident de cybersécurité*, au besoin, dans les 180 jours civils suivant la mise à l'essai d'un plan d'intervention en cas d'*incident de cybersécurité* ou suivant un *incident de cybersécurité à déclarer* réel.

## CIP-003-6 – Annexe 2

### Plans de cybersécurité pour les actifs comportant des *systèmes électroniques BES* à impact faible – Exemples de pièces justificatives

Section 1 – Sensibilisation à la cybersécurité – Exemples non limitatifs de pièces justificatives pour la section 1 : documentation attestant que le rappel des pratiques de cybersécurité a été fait au moins une fois tous les 15 mois civils. Les pièces justificatives peuvent porter sur une ou plusieurs des méthodes suivantes :

- communications ciblées (courriels, notes de service, formation en ligne, etc.) ;
- communications générales indirectes (affiches, intranet, brochures, etc.) ; ou
- soutien et rappels de la direction (présentations, réunions, etc.).

Section 2 – Mesures de sécurité physique – Exemples non limitatifs de pièces justificatives pour la section 2 :

- documentation des mécanismes de contrôle d'accès (carte d'accès, serrures, sécurisation de périmètre, etc.), des mesures de surveillance (systèmes d'alarme, surveillance humaine, etc.) ou d'autres mesures de sécurité physique de nature opérationnelle, administrative ou technique pour le contrôle de l'accès physique :
  - a. à l'actif, s'il y a lieu, ou aux emplacements de *système électronique BES* à impact faible à l'intérieur de l'actif ; et
  - b. à l'*actif électronique*, le cas échéant, qui comporte un *LEAP*.

Section 3 – Contrôles des accès électroniques – Exemples non limitatifs de pièces justificatives pour la section 3 :

- documentation attestant que des connexions entrantes et sortantes de tout *LEAP* sont limitées à celles que l'entité responsable juge nécessaires (restriction des adresses IP, des ports ou des services, etc.) ; et documentation du mécanisme d'authentification de la *connectivité par lien commuté* (appels sortants limités à un numéro préprogrammé pour la transmission de données, modems à fonction de rappel, modems télécommandés par le centre de contrôle ou la salle de commande, contrôle d'accès dans le *système électronique BES*, etc.).

Section 4 – Intervention en cas d'incident de cybersécurité – Exemples non limitatifs de pièces justificatives pour la section 4 : documents datés (politiques, procédures, processus, etc.) d'un ou de plusieurs plans d'intervention en cas d'*incident de cybersécurité* établis par actif ou par groupe d'actifs, qui comprennent les actions suivantes :

1. détecter les *incidents de cybersécurité*, les classer et y répondre ; déterminer si un *incident de cybersécurité* détecté est un *incident de cybersécurité à déclarer* et aviser l'Electricity Sector Information Sharing and Analysis Center (ES-ISAC) ;

2. établir et documenter les rôles et responsabilités des groupes ou des personnes chargés d'intervenir en cas d'*incident de cybersécurité* (déclenchement, documentation, surveillance, déclaration, etc.) ;
3. gérer les *incidents de cybersécurité* (confinement, élimination, reprise après incident ou résolution de l'incident, etc.) ;
4. mettre à l'essai le ou les plans, avec documents datés attestant qu'un essai a été fait au moins une fois tous les 36 mois civils ; et
5. mettre à jour au besoin les plans d'intervention en cas d'*incident de cybersécurité* dans les 180 jours civils suivant la mise à l'essai ou suivant un *incident de cybersécurité à déclarer* réel.

## 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. 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.

#### Exigence E1

Lors de l'élaboration des politiques prescrites à l'exigence E1, le nombre de politiques et leur contenu doivent être guidés par la structure de gestion de l'entité responsable et par son contexte opérationnel. Ces politiques peuvent être intégrées à un programme général de sécurité de l'information pour l'ensemble de l'organisation, ou encore à des programmes particuliers. L'entité responsable a le choix d'élaborer une politique de cybersécurité monolithique qui englobe les thèmes prescrits, mais elle peut aussi créer une politique parapluie de haut niveau et confier les détails à des documents de niveau inférieur dans la hiérarchie documentaire. Dans le cas d'une politique parapluie de haut niveau, l'entité responsable devrait fournir la politique parapluie ainsi que les documents complémentaires afin de démontrer la conformité à l'exigence E1 de la norme CIP-003-6.

Si une entité responsable détient des *systèmes électroniques BES* à impact élevé ou moyen, la ou les politiques de cybersécurité doivent couvrir les neuf thèmes prescrits à la partie 1.1 de l'exigence E1 de la norme CIP 003-6. Si une entité responsable a désigné, selon les critères de la norme CIP-002, des actifs comportant des *systèmes électroniques BES* à impact faible, la ou les politiques de cybersécurité doivent couvrir les quatre thèmes prescrits à la partie 1.2 de l'exigence E1.

Les entités responsables qui ont des *systèmes électroniques BES* pour différentes catégories d'impact ne sont pas tenues de créer des politiques de cybersécurité distinctes pour les *systèmes électroniques BES* à impact faible, moyen et élevé. Les entités responsables ont la possibilité d'élaborer des politiques qui s'appliquent à la fois aux trois catégories d'impact.

La mise en œuvre de la politique de cybersécurité n'est pas traitée explicitement dans l'exigence E1 de la norme CIP-003-6, car on considère qu'elle se manifestera dans la bonne mise en œuvre des normes CIP-003 à CIP-011. Les entités responsables sont toutefois invitées à ne pas limiter la portée de leurs politiques de cybersécurité aux seules exigences des normes de fiabilité de la NERC sur la cybersécurité, mais plutôt à élaborer une politique de cybersécurité globale appropriée à leur organisation. Les éléments d'une politique qui s'étendent au-delà de la portée des normes de fiabilité de la NERC sur la cybersécurité ne seront pas considérés comme donnant lieu à des infractions potentielles ; ils aideront plutôt à témoigner de la culture de conformité au sein de de l'organisation et de sa posture de cybersécurité.

Dans le contexte de la partie 1.1, l'entité responsable devrait tenir compte des points suivants pour chacun des thèmes obligatoires dans sa ou ses politiques de cybersécurité visant ses *systèmes électroniques BES* à impact moyen et élevé :

### 1.1.1 Personnel et formation (CIP-004)

- Position de l'organisation sur ce qui constitue une enquête acceptable sur les antécédents
- Mesures disciplinaires possibles pour les infractions à cette politique
- Gestion des comptes

### 1.1.2 Périmètres de sécurité électronique (CIP-005), y compris l'accès distant interactif

- Position de l'organisation sur l'utilisation des réseaux sans fil
- Désignation des méthodes d'authentification acceptables
- Désignation des ressources fiables et non fiables
- Surveillance et consignation des accès et des sorties aux *points d'accès électroniques*
- Tenue à jour des logiciels antimaliciels avant l'exécution de l'*accès distant interactif*
- Tenue à jour des correctifs pour les systèmes d'exploitation et pour les applications qui exécutent l'*accès distant interactif*
- Désactivation des postes de travail VPN avec séparation des flux (*split tunneling*) ou à double résidence (*dual-homed*) avant l'exécution de l'*accès distant interactif*
- Pour les fournisseurs, les contractuels ou les consultants, le recours à des clauses contractuelles qui exigent le respect des mesures de contrôle d'*accès distant interactif* de l'entité responsable

### 1.1.3 Sécurité physique des *systèmes électroniques BES* (CIP-006)

- Stratégie de protection des *actifs électroniques* contre les accès physiques non autorisés

- Méthodes acceptables de contrôle des accès physiques
  - Surveillance et consignation des accès physiques
- 1.1.4 Gestion de la sécurité des systèmes (CIP-007)
- Stratégies de renforcement des systèmes
  - Méthodes acceptables d'authentification et de contrôle d'accès
  - Politiques sur les mots de passe comprenant longueur, complexité, mise en application et prévention des attaques exhaustives
  - Surveillance et consignation des activités des *systèmes électroniques BES*
- 1.1.5 Déclaration des incidents et planification des mesures d'intervention (CIP-008)
- Détection des incidents de cybersécurité
  - Notifications appropriées en cas de découverte d'un incident
  - Obligations de signaler les *incidents de cybersécurité*
- 1.1.6 Plans de rétablissement des systèmes électroniques BES (CIP-009)
- Disponibilité des composants de rechange
  - Disponibilité des sauvegardes système
- 1.1.7 Gestion des changements de configuration et analyses de vulnérabilité (CIP-010)
- Demandes de changement
  - Approbation des changements
  - Processus de réparation
- 1.1.8 Protection de l'information (CIP-011)
- Méthodes de contrôle d'accès à l'information
  - Notification des divulgations non autorisées
  - Accès à l'information selon le principe du besoin de savoir
- 1.1.9 Déclaration des circonstances CIP exceptionnelles et mesures d'intervention
- Processus de recours à des procédures spéciales en cas de *circonstance CIP exceptionnelle*
  - Processus de tolérance des dérogations qui n'enfreignent pas les exigences CIP

Les exigences relatives aux dérogations aux politiques de sécurité d'une entité responsable ont été retirées puisqu'il s'agit d'un enjeu de gestion générale qui ne relève pas des exigences de fiabilité. Il s'agit d'une exigence de politique interne et non d'une exigence de fiabilité. Cependant, les entités responsables sont invitées à maintenir cette pratique dans le cadre de leurs politiques de cybersécurité.

Dans le cas présent, et pour toutes les approbations subséquentes exigées par les normes de fiabilité CIP de la NERC, l'entité responsable est libre d'utiliser des approbations en version papier ou électronique, pourvu que la preuve soit suffisante pour garantir l'authenticité de l'approbateur.

### **Exigence E2**

À partir de la liste des actifs comportant des *systèmes électroniques BES* à impact faible établie selon la norme CIP-002, chaque entité responsable doit créer, documenter et mettre en œuvre un ou plusieurs plans de cybersécurité fondés sur des critères objectifs et visant à protéger les *systèmes électroniques BES* à impact faible. Les protections requises par l'exigence E2 sont liées au degré de risque pour le *BES* en cas de mauvaise utilisation ou d'indisponibilité des *systèmes électroniques BES* à impact faible. Le but recherché est que les protections exigées fassent partie d'un programme qui vise les *systèmes électroniques BES* à impact faible de façon collective, au niveau de l'actif ou du site (actifs comportant des *systèmes électroniques BES* à impact faible), et non au niveau des appareils ou des systèmes individuels.

Le plan de cybersécurité doit couvrir quatre grands thèmes, présentés à l'annexe 1 : 1) la sensibilisation à la cybersécurité, 2) les mesures de sécurité physique, 3) le contrôle des accès électroniques pour les *LERC* et la *connectivité par lien commuté*, et 4) l'intervention en cas d'*incident de cybersécurité*.

### **Exigence E2, annexe 1**

Comme il est indiqué, l'annexe 1 présente les sections à inclure dans tout plan de cybersécurité. Il s'agit de donner aux entités qui ont une combinaison de *systèmes électroniques BES* à impact faible, moyen et élevé la possibilité, si elles le souhaitent, d'appliquer à leurs *systèmes électroniques BES* à impact faible (ou à une partie de ceux-ci) les programmes qu'elles ont établis pour les *systèmes électroniques BES* à impact moyen ou élevé, plutôt que de devoir gérer deux programmes différents. Des précisions et éclaircissements pour chacun des quatre thèmes de l'annexe 1 sont présentés ci-après.

### **Exigence E2, section 1 de l'annexe 1 – Sensibilisation à la cybersécurité**

Le programme de sensibilisation à la cybersécurité oblige les entités à rappeler les bonnes pratiques de cybersécurité à leur personnel au moins une fois tous les 15 mois civils. L'entité est libre de choisir les thèmes à couvrir et la manière de communiquer les rappels sur ces thèmes. Quant aux pièces justificatives de conformité, l'entité responsable doit pouvoir présenter le matériel de sensibilisation utilisé, selon la ou les méthodes de communication (affiches, courriels, sujets abordés aux réunions de service, etc.). L'entité responsable n'est pas obligée de tenir des listes de destinataires ni de confirmer la réception par le personnel du matériel de sensibilisation.

Bien que la sensibilisation concerne en particulier la cybersécurité, des thèmes non technologiques ne sont pas à exclure pour autant. Des thèmes appropriés de sécurité physique (sensibilisation au talonnage, protection des cartes d'accès physique, campagnes d'incitation à signaler tout fait suspect, etc.) renforcent aussi la sensibilisation à la cybersécurité. Le but recherché est d'aborder des thèmes pertinents aux différents aspects de la protection des



*systèmes électroniques BES.*

### **Exigence E2, section 2 de l'annexe 1 – Mesures de sécurité physique**

L'entité responsable doit documenter et mettre en œuvre des mesures de contrôle de l'accès physique 1) aux *systèmes électroniques BES* à impact faible à l'intérieur d'actifs qui comportent de tels systèmes, et 2) aux *LEAP*, s'il en existe. Si le *LEAP* est situé à l'intérieur de l'actif du *BES* et qu'il hérite des mêmes mesures de contrôle d'accès selon la section 2, l'entité responsable peut en tenir compte dans ses politiques ou ses plans de cybersécurité afin d'éviter une documentation redondante des mêmes mesures.

L'entité responsable est libre de choisir les méthodes à utiliser pour atteindre l'objectif de contrôler l'accès physique aux actifs comportant des *systèmes électroniques BES* à impact faible, aux *systèmes électroniques BES* à impact faible eux-mêmes, ou encore aux *LEAP*, s'il en existe. L'entité responsable peut utiliser une ou plusieurs mesures de contrôle d'accès, mesures de surveillance ou autres mesures de sécurité physique de nature opérationnelle, administrative ou technique. Les entités peuvent appliquer des mesures de contrôle d'accès physique à des périmètres étendus (clôtures avec barrières verrouillées, gardiens, politiques d'accès aux sites, etc.) ou encore à des zones plus circonscrites où sont situés les *systèmes électroniques BES* à impact faible, comme les salles de commande ou les centres de contrôle. Il n'est pas exigé d'avoir des programmes d'autorisation des utilisateurs et des listes d'utilisateurs autorisés à un accès physique, bien que ces mesures soient à envisager pour répondre à l'objectif de sécurité.

L'objectif visé est de contrôler l'accès physique d'après les besoins déterminés par l'entité responsable. Les besoins peuvent être documentés au niveau des politiques d'accès au site ou aux systèmes, y compris les *LEAP*. L'exigence n'oblige pas l'entité à spécifier un besoin pour chaque accès ou autorisation d'accès d'un utilisateur.

La surveillance comme mesure de sécurité physique peut servir de complément ou de solution de rechange au contrôle d'accès. Exemples non limitatifs de mesures de surveillance :

- 1) systèmes d'alarme sensibles au mouvement ou à l'entrée dans la zone contrôlée ou
- 2) surveillance humaine de la zone contrôlée. La surveillance n'oblige pas nécessairement à tenir des registres, mais pourrait comprendre la détection qu'un accès physique a eu lieu ou été tenté (alarme de porte, surveillance humaine, etc.). Il n'est pas nécessaire d'avoir une surveillance pour chaque *système électronique BES* à impact faible, mais la surveillance doit être au niveau approprié pour atteindre l'objectif de sécurité.

### **Exigence E2, section 3 de l'annexe 1 – Contrôle des accès électroniques**

La section 3 exige la mise en place de protections périmétriques pour les *systèmes électroniques BES* à impact faible lorsque ceux-ci ont une communication bidirectionnelle par protocole routable ou une *connectivité par lien commuté* avec des appareils situés à l'extérieur de l'actif dans lequel se trouvent des *systèmes électroniques BES* à impact faible. Les protections périmétriques contrôlent les communications soit vers un actif comportant des *systèmes électroniques BES* à impact faible, soit vers les *systèmes électroniques BES* à impact faible eux-mêmes, afin de réduire les risques associés à une communication non contrôlée au moyen de protocoles routables ou d'une *connectivité par lien commuté*. Le terme « contrôle

des accès électroniques » est employé dans son sens général, soit celui de contrôle passif des accès, et non dans le sens technique particulier qui évoque la mise en œuvre de mécanismes d'authentification, d'autorisation et d'audit. L'entité responsable n'est pas obligée d'établir une communication *LERC* ou un *LEAP* en l'absence de communication bidirectionnelle par protocole routable ou de *connectivité par lien commuté* ; dans un tel cas, l'entité peut documenter l'absence d'une telle communication dans son ou ses plans de cybersécurité visant les actifs à impact faible.

Les termes définis *LERC* et *LEAP* sont utilisés pour éviter toute confusion avec des termes semblables associés aux *systèmes électroniques BES* à impact moyen ou élevé (par exemple « *connectivité externe routable* » ou « *point d'accès électronique* »). Afin de mettre les normes à l'abri des changements et des complications technologiques à l'avenir, la définition de *LERC* exclut nommément « les communications point à point entre dispositifs électroniques intelligents qui utilisent des protocoles de communication routables pour assurer des fonctions de commande ou de protection à délai critique entre des actifs de poste de transport comportant des *systèmes électroniques BES* à impact faible », comme la messagerie CEI 61850. Les communications ainsi exclues ne sont pas celles des *centres de contrôle*, mais plutôt celles entre les dispositifs électroniques intelligents eux-mêmes. Une entité responsable qui utilise cette technologie n'est pas tenue de mettre en place un *LEAP*. Cette exception a été ajoutée afin de ne pas compromettre les fonctions à délai critique associées à cette technologie, et de ne pas empêcher le recours futur à de telles fonctions afin d'améliorer la fiabilité au motif qu'elles utiliseraient un protocole routable.

Lorsqu'il s'agit de déterminer si un *système électronique BES* à impact faible comporte une *LERC*, il convient de se référer à la définition de ce terme : « accès interactif direct amorcé par l'utilisateur ou connexion directe entre appareils, vers un ou des *systèmes électroniques BES* à impact faible à partir d'un *actif électronique* situé à l'extérieur de l'actif qui comporte ce ou ces *systèmes électroniques BES* à impact faible, au moyen d'une liaison bidirectionnelle utilisant un protocole routable ». Dans cette définition, les mots « direct » et « directe » servent à indiquer qu'il y a une *LERC* si une personne utilise un autre appareil situé à l'extérieur de l'actif qui comporte le *système électronique BES* à impact faible, et que cette personne peut se connecter (pour ouvrir une session, configurer, lire, interagir, etc.) avec le *système électronique BES* à impact faible au moyen d'une seule session bidirectionnelle avec protocole routable de bout en bout, même s'il y a conversion entre une liaison série et un protocole routable. Une *LERC* existe aussi dans le cas inverse où la personne utilise le *système électronique BES* à impact faible et se connecte à un appareil situé à l'extérieur de l'actif comportant des *systèmes électroniques BES* à impact faible, au moyen d'une seule session bidirectionnelle avec protocole routable de bout en bout. En outre, l'expression « liaison directe entre appareils » indique qu'il y a une *LERC* si l'entité responsable a des appareils qui sont situés à l'extérieur de l'actif comportant le *système électronique BES* à impact faible et qui établissent une communication bidirectionnelle avec protocole routable avec le *système électronique BES* à impact faible, en accès entrant ou sortant.

Lorsqu'elle repère un *LEAP*, l'entité responsable a une certaine latitude quant au choix de l'interface pour l'*actif électronique* qui contrôle la *LERC*. Exemples non limitatifs : l'interface interne (tournée vers les *systèmes électroniques BES* à impact faible) d'un pare-feu externe ou

hôte, l'interface interne d'un routeur muni d'une liste de contrôle d'accès, ou un autre appareil de sécurité. L'entité a aussi une certaine latitude quant à l'emplacement du *LEAP*. Il n'est pas exigé que le *LEAP* soit situé dans l'actif qui comporte les *systèmes électroniques BES* à impact faible. En outre, l'entité n'est pas obligée d'établir un *LEAP* physique unique par actif comportant des *systèmes électroniques BES* à impact faible. L'entité responsable peut avoir un même *actif électronique* regroupant plusieurs *LEAP* qui contrôlent la *LERC* de plusieurs actifs comportant des *systèmes électroniques BES* à impact faible. Cependant, le fait de situer l'actif électronique regroupant plusieurs *LEAP* dans un emplacement externe, avec derrière lui plusieurs actifs comportant des *systèmes électroniques BES* à impact faible, ne doit pas avoir pour effet de rendre possible un accès non contrôlé aux actifs comportant des *systèmes électroniques BES* à impact faible qui partagent l'*actif électronique* regroupant le ou les *LEAP*.

Dans le modèle de référence 4, la communication passe par un convertisseur IP-série. Il y a effectivement une *LERC* dans ce modèle de référence, car le convertisseur IP-série dans ce cas ne fait rien d'autre que prolonger la communication entre le *système électronique BES* à impact faible et l'*actif électronique* situé à l'extérieur de l'actif comportant le *système électronique BES* à impact faible. Par contre, dans le modèle de référence 6, un *actif électronique* est disposé de manière à réaliser une coupure ou une interruption complète qui ne permet pas aux données de l'utilisateur ou de l'appareil d'aboutir directement au *système électronique BES* à impact faible. L'*actif électronique* dans le modèle de référence 6 empêche l'accès au *système électronique BES* à impact faible à partir de l'*actif électronique* situé à l'extérieur de l'actif comportant le *système électronique BES* à impact faible. En somme, si le convertisseur IP-série déployé ne sert qu'à relayer les données transmises, cette communication de relayage de données est alors une *LERC* et un *LEAP* est requis. Cependant, si le convertisseur IP-série impose une quelconque authentification du flux de données dans l'actif comportant le *système électronique BES* à impact faible avant que la communication puisse aboutir au *système électronique BES* à impact faible, alors ce type de mise en œuvre de convertisseur IP-série n'est pas une *LERC*.

Un *actif électronique* comportant une ou plusieurs interfaces qui remplissent seulement la fonction d'un *LEAP* ne répond pas à la définition de *système de contrôle ou de surveillance des accès électroniques (EACMS)* associé aux *systèmes électroniques BES* à impact moyen ou élevé, et est dispensé des exigences applicables à un *EACMS*. Cependant, un *actif électronique* peut avoir certaines interfaces qui jouent le rôle d'un *LEAP* et d'autres interfaces qui jouent le rôle d'un *point d'accès électronique (EAP)* pour des *systèmes électroniques BES* à impact moyen ou élevé. Dans ce cas, l'*actif électronique* serait aussi assujéti aux exigences applicables à l'*EACMS* associé aux *systèmes électroniques BES* à impact moyen ou élevé.

Exemples non limitatifs de contrôles d'accès adéquats :

- Toute *LERC* de l'actif franchit un *LEAP* qui applique des autorisations d'accès entrant et sortant explicites, ou une méthode équivalente par laquelle les liaisons entrantes et sortantes sont limitées aux seuls éléments (adresses IP, ports, services, etc.) que l'entité responsable juge nécessaires.
- Comme l'illustre le modèle de référence 1 ci-dessous, le *système électronique BES* à impact faible comporte un pare-feu hôte qui contrôle les accès entrants et sortants.

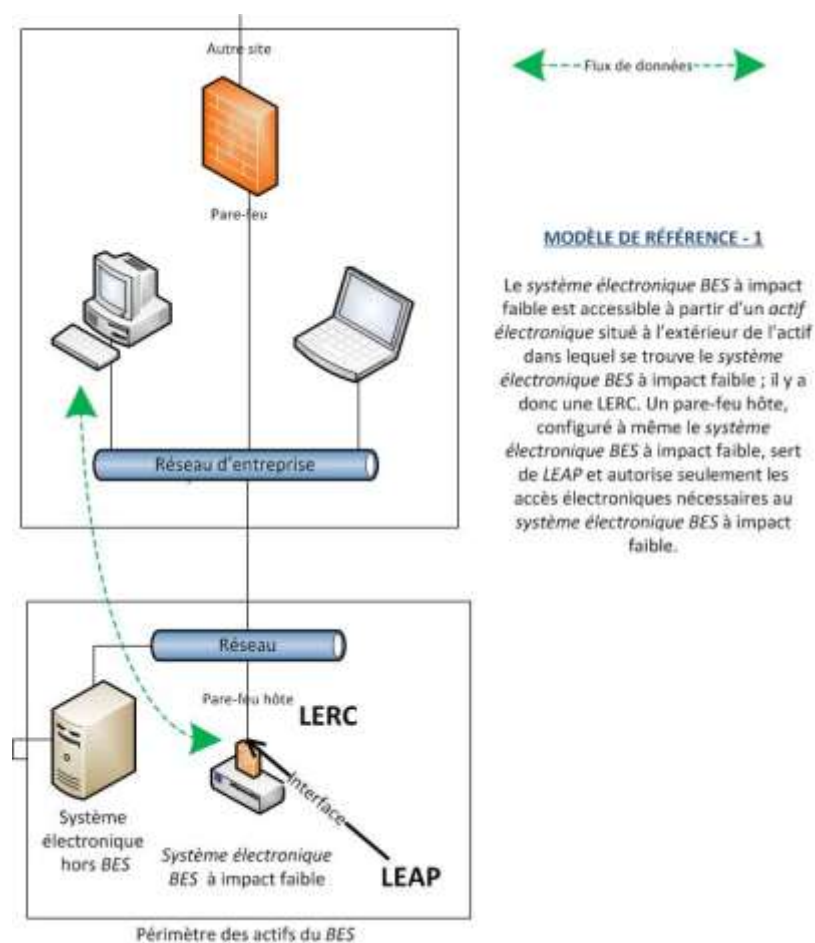
Dans ce modèle, il est également possible que le pare-feu hôte soit situé dans un *actif électronique* hors *BES*. Le but recherché est que le pare-feu hôte contrôle les accès entrants et sortants entre le *système électronique BES* à impact faible et l'*actif électronique* situé dans le réseau d'entreprise.

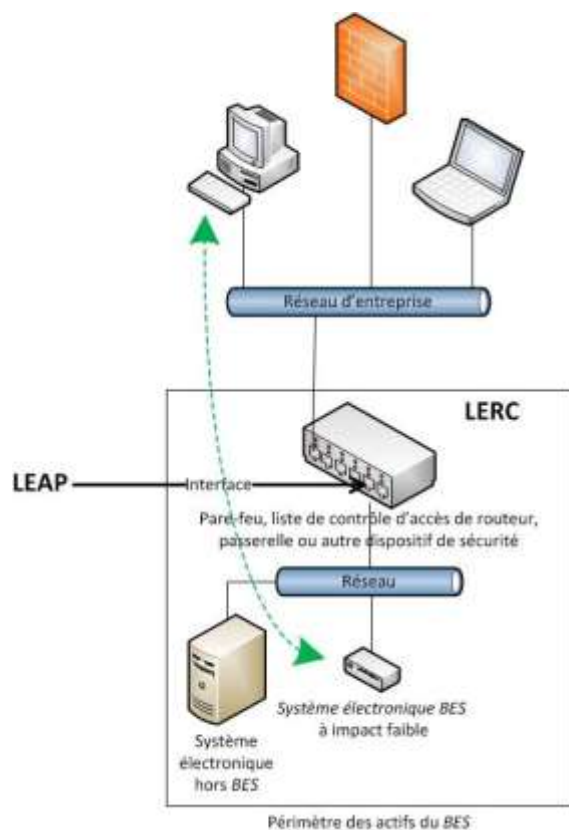
- Dans le modèle de référence 5 ci-dessous, un *actif électronique* hors *BES* est interposé entre le *système électronique BES* à impact faible situé dans le réseau du poste électrique et l'*actif électronique* situé dans le réseau d'entreprise. Le but recherché est que l'*actif électronique* hors *BES* assure une « coupure de protocole », de sorte que l'accès au *système électronique BES* à impact faible se fasse seulement à partir de l'*actif électronique* hors *BES* situé à l'intérieur de l'*actif* comportant le *système électronique BES* à impact faible.
- La *connectivité par lien commuté* avec un *système électronique BES* à impact faible autorise seulement les appels sortants (pas de réponse automatique) vers un numéro préprogrammé pour l'envoi de données. S'il y a *connectivité par lien commuté* entrante, elle est réalisée par un modem à fonction de rappel ou par un modem qui doit être télécommandé par le centre de contrôle ou la salle de commande, qui offre une certaine forme de contrôle d'accès ; sinon, le *système électronique BES* à impact faible doit avoir un contrôle d'accès.

Exemples non limitatifs de situations où les contrôles d'accès seraient insuffisants pour satisfaire à cette exigence :

- Un actif a une *connectivité par lien commuté* et un *système électronique BES* à impact faible est accessible par un modem à réponse automatique qui relie tout appelant à l'*actif électronique*, lequel est muni d'un mot de passe par défaut. Il n'y a pas de véritable contrôle d'accès dans cette situation.
- Un actif comporte une *LERC*, car un *système électronique BES* à l'intérieur de cet actif est équipé d'une carte sans fil reliée à un réseau de télécommunications public, ce qui rend le *système électronique BES* accessible par une adresse IP publique. Essentiellement, les *systèmes électroniques BES* à impact faible ne doivent pas être accessibles à partir d'Internet ou de moteurs de recherche comme Shodan.
- Dans le modèle de référence 5, si l'on utilise seulement des cartes d'interface à double résidence ou multiréseaux sans désactiver le réacheminement IP dans l'*actif électronique* hors *BES* à l'intérieur de la zone DMZ afin d'assurer une coupure entre le *système électronique BES* à impact faible et le réseau d'entreprise, l'exigence de « contrôle » des accès électroniques entrants et sortants ne serait pas respectée en supposant l'absence d'un pare-feu hôte ou d'un autre appareil de sécurité pour cet *actif électronique* hors *BES*.

Les schémas ci-après présentent des modèles de référence qui illustrent comment on détermine s'il y a une *LERC* et comment mettre en place un *LEAP*. Ces schémas présentent plusieurs configurations possibles, mais les entités responsables pourront avoir d'autres configurations non illustrées.

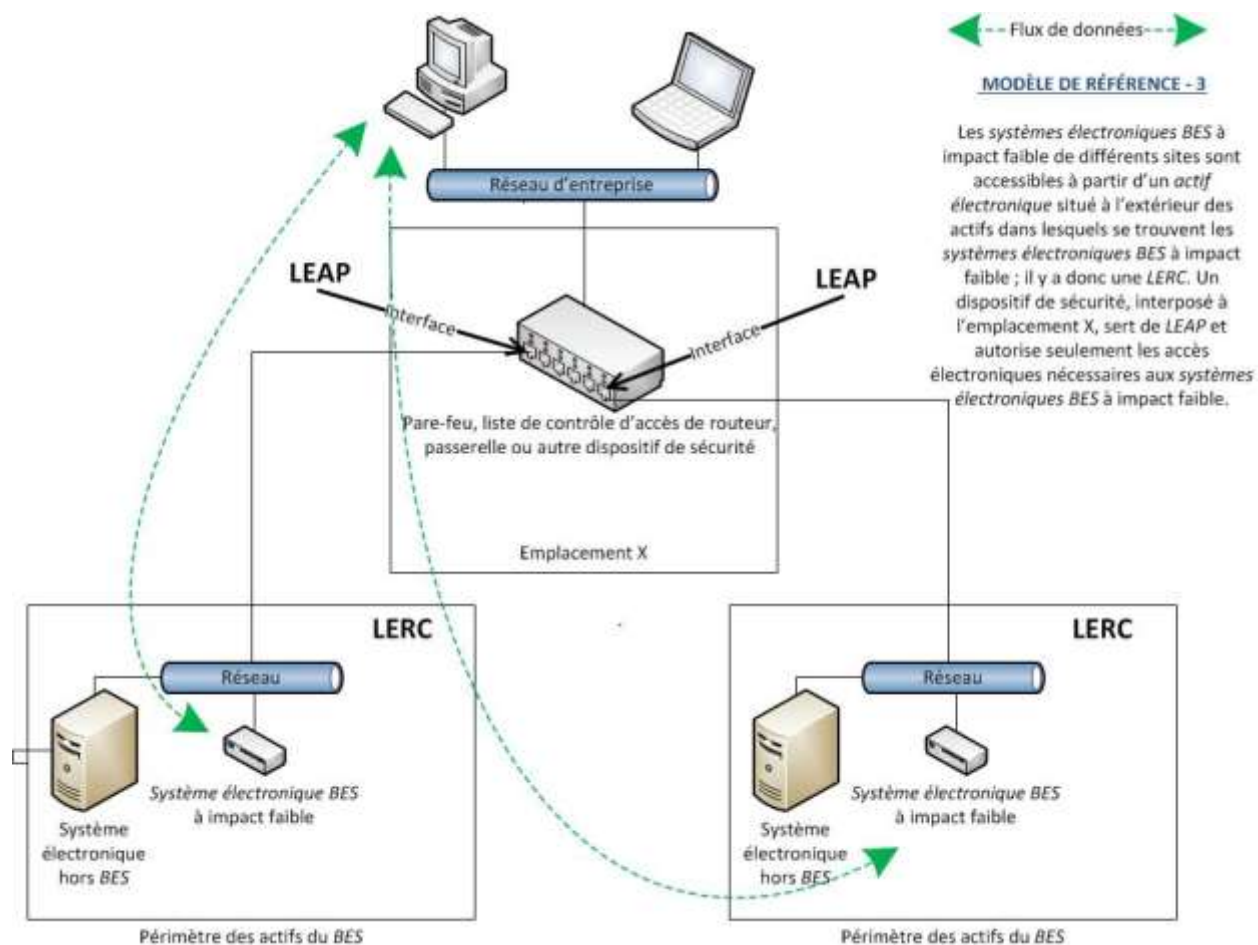


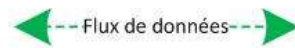
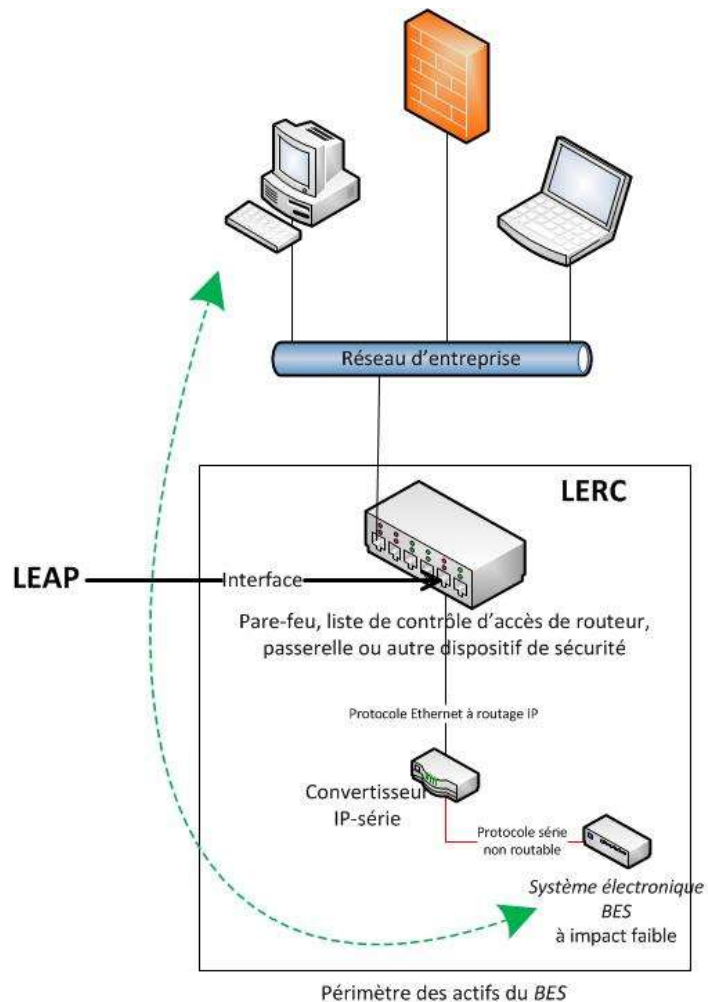


← Flux de données →

### MODÈLE DE RÉFÉRENCE - 2

Le système électronique BES à impact faible est accessible à partir d'un actif électronique situé à l'extérieur de l'actif dans lequel se trouve le système électronique BES à impact faible ; il y a donc une LERC. Un dispositif de sécurité, interposé entre le réseau d'entreprise et le système électronique BES à impact faible, sert de LEAP et autorise seulement les accès électroniques nécessaires au système électronique BES à impact faible.

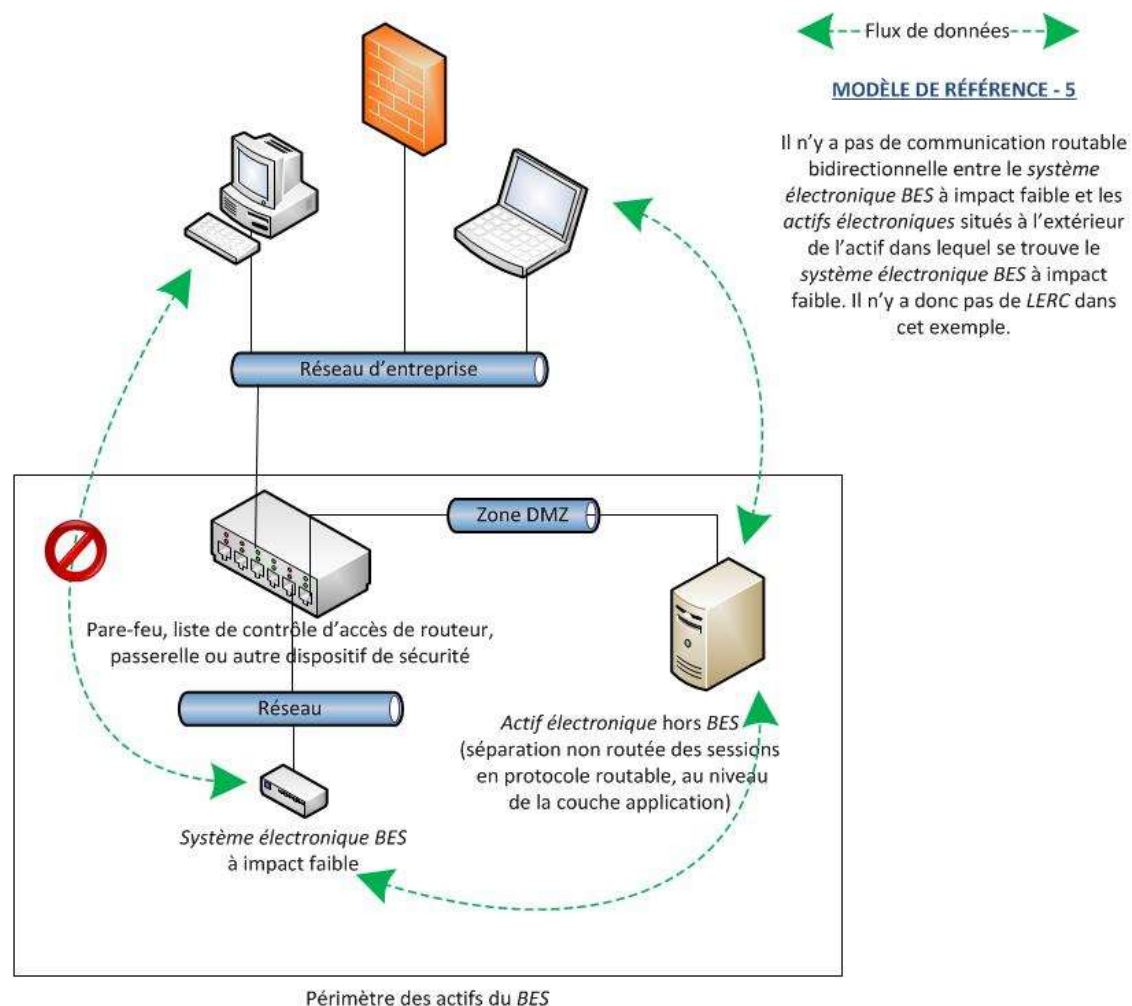


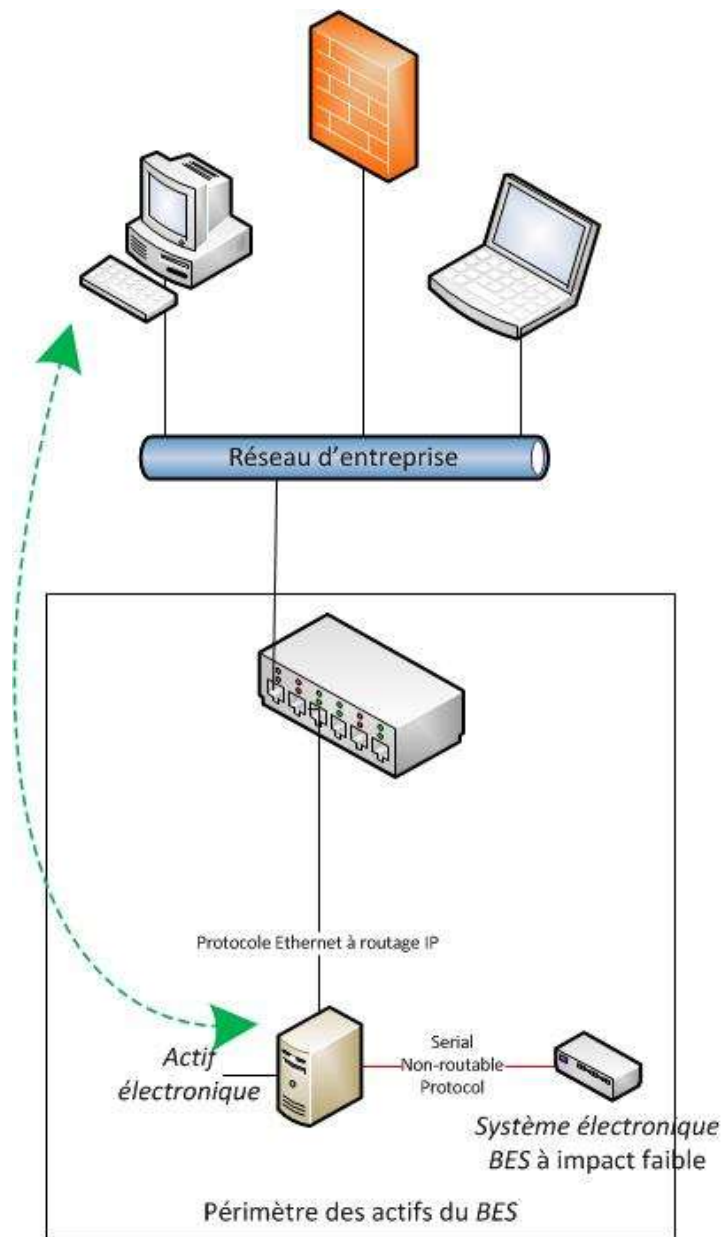


## MODÈLE DE RÉFÉRENCE - 4

Le système électronique BES à impact faible est accessible à partir d'un *actif électronique* situé à l'extérieur de l'actif dans lequel se trouve le système électronique BES à impact faible. Il y a une LERC, car le convertisseur IP-série prolonge la communication entre l'*actif électronique* du réseau d'entreprise et le système électronique BES à impact faible, lequel est directement adressable de l'extérieur. Un dispositif de sécurité, interposé entre le réseau d'entreprise et le système électronique BES à impact faible, autorise seulement les accès électroniques nécessaires au système électronique BES à impact faible.



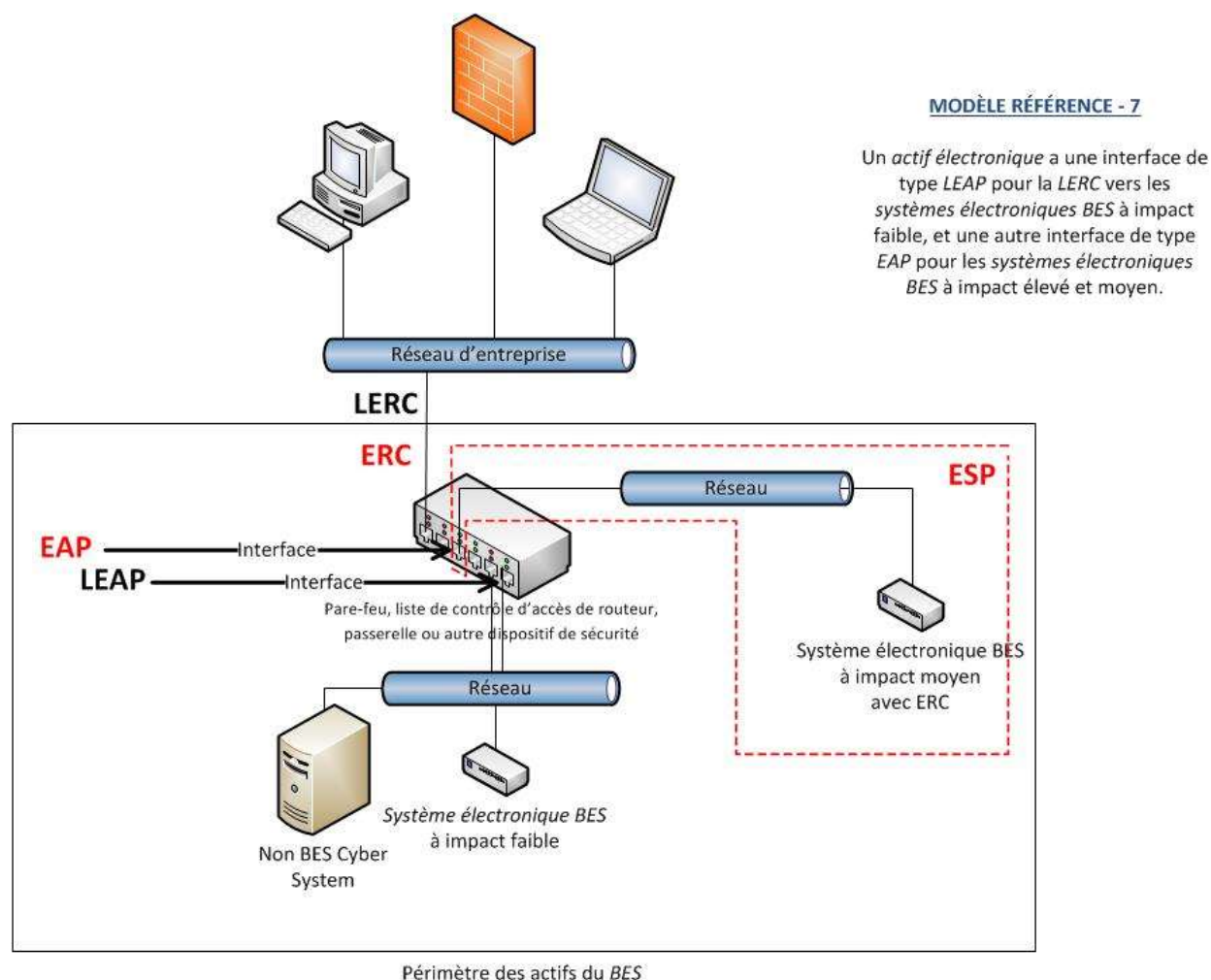




← Flux de données →

#### MODÈLE DE RÉFÉRENCE - 6

Dans cet exemple, un *actif électronique* bloque l'accès direct au *système électronique BES à impact faible*. Il y a une coupure au niveau de la couche 7 (couche application), ou encore l'*actif électronique* exige une authentification, puis établit une nouvelle liaison avec le *système électronique BES à impact faible*. Il n'y a donc pas de LERC dans cet exemple.



### Exigence E2, section 4 de l'annexe 1 – Intervention en cas d'incident de cybersécurité

L'entité doit avoir un ou plusieurs plans d'intervention en cas d'*incident de cybersécurité* documentés couvrant chacun des thèmes indiqués à la section 4. Si, dans le cours normal des activités, on observe des opérations suspectes à un actif qui comporte des *systèmes électroniques BES* à impact faible, l'entité mettra en œuvre un plan d'intervention en cas d'*incident de cybersécurité* qui guidera son action et l'amènera à signaler l'incident s'il atteint le niveau d'un *incident de cybersécurité à déclarer*.

Les entités sont libres de segmenter leurs plans d'intervention en cas d'*incident de cybersécurité* exigés à la section 4 de l'annexe 1 par actif ou par groupe d'actifs. Il n'est pas nécessaire que les plans soient établis par site d'actifs ou par *système électronique BES* à impact faible. Les entités peuvent choisir d'adopter un seul plan à l'échelle de l'entreprise pour remplir leurs obligations relativement aux *systèmes électroniques BES* à impact faible.

Les plans doivent être mis à l'essai à intervalles de 36 mois. Il ne s'agit pas d'un exercice par *actif électronique BES* à impact faible ou par type d'*actif électronique BES*, mais plutôt un exercice pour chaque plan d'intervention en cas d'incident créé par l'entité pour satisfaire à cette exigence. Un *incident de cybersécurité à déclarer* réel compte comme essai, au même titre que d'autres essais par simulation. Les exercices dirigés par la NERC, comme la participation à

GridEx, seraient aussi acceptables comme essais pourvu que le plan d'action de l'entité soit exécuté. Cette exigence oblige les entités à tenir à jour leurs plans d'intervention en cas d'*incident de cybersécurité*, et en particulier à les modifier si nécessaire dans les 180 jours suivant un essai ou un incident réel.

Pour les *systèmes électroniques BES* à impact faible, la seule partie de la définition d'*incident de cybersécurité* qui s'appliquerait est la suivante : « acte malveillant ou incident suspect qui perturbe ou avait pour but de perturber le fonctionnement d'un *système électronique BES* ». L'autre partie de cette définition ne doit pas servir à exiger le recours à des *périmètres de sécurité électronique* ou à des *périmètres de sécurité physique* pour les *systèmes électroniques BES* à impact faible.

### Exigence E3

L'esprit de l'exigence E3 de la norme CIP-003-6 reste pratiquement inchangé par rapport aux versions antérieures de la norme. La description spécifique du *cadre supérieur CIP* est maintenant comprise dans les termes définis, ce qui évite de l'expliciter dans le texte de la norme de fiabilité et de devoir créer des renvois à la norme dans d'autres documents. Le *cadre supérieur CIP* est appelé à jouer un rôle clé pour assurer la planification stratégique appropriée, la sensibilisation des dirigeants et du conseil d'administration et la gouvernance générale du programme.

### Exigence E4

Comme l'indique la justification de l'exigence E4 de la norme CIP-003-6, cette exigence vise à démontrer une chaîne d'autorité et d'imputabilité claire en matière de sécurité. L'intention de l'équipe de rédaction (SDT) était de ne pas imposer une structure organisationnelle particulière ; elle laisse plutôt à l'entité responsable une ample marge de manœuvre pour adapter cette exigence à sa structure organisationnelle existante. Une entité responsable peut satisfaire à cette exigence au moyen d'un seul ou de plusieurs documents de délégation. L'entité responsable peut aussi déléguer les pouvoirs de délégation eux-mêmes pour augmenter la souplesse de mise en œuvre dans son organisation. Dans un tel cas, les délégations peuvent être dispersées dans de multiples documents, pourvu que l'ensemble de ces documents décrive une chaîne d'autorité claire qui remonte au *cadre supérieur CIP*. De plus, le *cadre supérieur CIP* pourrait aussi choisir de ne déléguer aucun pouvoir et de respecter cette exigence sans recourir à des documents de délégation.

L'entité responsable doit tenir à jour la documentation relative au *cadre supérieur CIP* et à ses délégations, afin d'éviter que des individus n'exercent des pouvoirs non documentés. Cependant, il n'est pas nécessaire de réaffirmer les délégations si le délégant change de poste ou est remplacé. Par exemple, supposons que Pierre Untel soit désigné comme *cadre supérieur CIP* et qu'il délègue une tâche au directeur de la maintenance des postes électriques. Si Pierre Untel est remplacé comme *cadre supérieur CIP*, la documentation du *cadre supérieur CIP* doit être mise à jour dans le délai prescrit, mais la délégation existante au directeur de la maintenance des postes électriques reste en vigueur telle qu'elle a été approuvée par le *cadre supérieur CIP* précédent, Pierre Untel.

### 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

Une ou plusieurs politiques de sécurité assurent une mise en œuvre efficace des exigences des normes de fiabilité sur la cybersécurité. Ces politiques visent à constituer les bases de la gestion et de la gouvernance pour toutes les exigences applicables aux *systèmes électroniques BES* de l'entité responsable. L'entité responsable peut démontrer par ses politiques que ses dirigeants appuient les mesures d'imputabilité et de responsabilisation nécessaires pour une mise en œuvre efficace des exigences.

Le réexamen et l'approbation annuels des politiques de cybersécurité assurent la tenue à jour de ces politiques et réaffirment périodiquement l'engagement des dirigeants envers la protection de leurs *systèmes électroniques BES*.

#### Justification de l'exigence E2

En réponse à l'ordonnance 791 de la FERC, l'exigence E2 demande aux entités d'élaborer et de mettre en œuvre des plans de cybersécurité afin d'atteindre des objectifs précis en matière de mécanismes de sécurité pour leurs actifs comportant des *systèmes électroniques BES* à impact faible. Les plans de cybersécurité couvrent quatre thèmes : 1) la sensibilisation à la cybersécurité ; 2) les mesures de sécurité physique ; 3) le contrôle des accès électroniques ; et 4) l'intervention en cas d'*incident de cybersécurité*. Ces plans, combinés aux politiques de cybersécurité spécifiées à la partie 1.2 de l'exigence E1, présentent un cadre pour la mise en place de mesures opérationnelles, administratives et techniques visant les *systèmes électroniques BES* à impact faible.

Considérant la diversité des *systèmes électroniques BES* à impact faible dans l'ensemble du *BES*, l'annexe 1 offre aux entités responsables une certaine latitude quant à la manière d'appliquer les mécanismes de sécurité pour atteindre les objectifs de sécurité. En outre, comme beaucoup d'entités responsables ont des *systèmes électroniques BES* pour plusieurs catégories d'impact, rien dans l'exigence ne leur interdit d'utiliser leurs politiques, procédures et processus applicables aux *systèmes électroniques BES* à impact moyen ou élevé pour les mécanismes de sécurité visant les *systèmes électroniques BES* à impact faible, comme l'explique en détail l'annexe 1 relative à l'exigence E2.

Les entités responsables utiliseront leurs actifs comportant des *systèmes électroniques BES* à impact faible (désignés selon les critères de la norme CIP-002) pour déterminer les sites ou emplacements associés à des *systèmes électroniques BES* à impact faible. Cependant, les entités responsables ne sont nullement obligées de tenir des listes de leurs *systèmes électroniques BES* à impact faible et des actifs électroniques connexes, ni de tenir une liste des utilisateurs autorisés.

### **Justification de l'exigence E3**

La désignation du *cadre supérieur CIP* et sa documentation assurent une autorité et une imputabilité claires pour le programme CIP dans l'organisation, en réponse à la recommandation 43 du rapport sur la panne de courant de 2003. La description des responsabilités du *cadre supérieur CIP* figure au *glossaire de la NERC*, de telle sorte que ce terme peut être utilisé dans l'ensemble des normes CIP sans renvoi explicite.

Le paragraphe 296 de l'ordonnance 706 de la FERC pose la question de savoir si le cadre supérieur désigné devrait être un dirigeant de la société ou l'équivalent. Comme l'indique la définition du terme, le *cadre supérieur CIP* « dispose de l'autorité et de la responsabilité pour mener et gérer la mise en œuvre et le respect des exigences de cet ensemble de normes », ce qui assure que le cadre supérieur détient une autorité suffisante au sein de l'entité responsable pour que la cybersécurité reçoive toute l'attention nécessaire. En outre, étant donné la variété des modèles de gestion des entités responsables (entités municipales, coopératives, organismes fédéraux, entreprises privées d'utilité publique, etc.), la SDT est d'avis que l'exigence que le *cadre supérieur CIP* soit « un dirigeant de la société ou l'équivalent » serait extrêmement difficile à interpréter et à mettre en application de manière homogène.

### **Justification de l'exigence E4**

Cette exigence vise à assurer une imputabilité claire au sein de l'organisation pour certains points relatifs à la sécurité. Elle fait aussi en sorte que les délégations soient tenues à jour et que nul n'exerce de pouvoirs sans délégation documentée.

Aux paragraphes 379 et 381 de son ordonnance 706, la FERC indique que la recommandation 43 du rapport sur la panne de courant de 2003 réclame « des chaînes d'autorité et d'imputabilité claires en matière de sécurité ». C'est ce qui a amené la SDT à clarifier l'exigence en matière de délégation, de manière que la chaîne d'autorité en question soit claire et que les délégations de pouvoir soient dûment documentées.

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 — Mécanismes de gestion de la sécurité
2. **Numéro :** CIP-003-6
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 : xx mois 20xx

5.2. Adoption de l'annexe par la Régie de l'énergie : xx mois 20xx

5.3. Date d'entrée en vigueur proposée de la norme et de l'annexe au Québec :

Norme	Entité	Dates d'implantation aux États-Unis	Date d'entrée en vigueur proposée au Québec		Justification
			Impacts moyen et élevé	Impacts faible	
<ul style="list-style-type: none"> <li>CIP-003-6</li> <li>CIP-003-6, E1, l'alinéa 1.1</li> </ul>	Entités visées par la version 1 des normes CIP adoptées par la Régie.	2016-07-01	2017-07-01	2017-07-01	Uniformisation des pratiques avec les autres juridictions.
	Entités exemptées de l'application de la version 1 des normes CIP en vertu des dispositions particulières associées à ces normes.		2018-10-01	2019-10-01	Donner le temps nécessaire à la mise en œuvre de la version 6 des normes CIP aux entités qui étaient exemptées de l'application de la version 1.
	Entités qui possèdent des installations de production à vocation industrielle		2019-04-01	2020-04-01	Donner le temps nécessaire à la mise en œuvre de la version 6 des normes CIP aux entités qui étaient exemptées de l'application de la version 1.
<ul style="list-style-type: none"> <li>CIP-003-6, E1, l'alinéa 1.2</li> <li>CIP-003-6,</li> </ul>	Entités visées par la version 1 des normes CIP adoptées par la Régie.	2017-04-01	2017-07-01	2018-07-01	Uniformisation des pratiques avec les autres juridictions.



Norme	Entité	Dates d'implantation aux États-Unis	Date d'entrée en vigueur proposée au Québec		Justification
			Impacts moyen et élevé	Impacts faible	
E2 • CIP-003-6, Annexe 1, Sect.1 • CIP-003-6, Annexe 1, Sect.4	Entités exemptées de l'application de la version 1 des normes CIP en vertu des dispositions particulières associées à ces normes.		2018-10-01	2019-10-01	Donner le temps nécessaire à la mise en œuvre de la version 6 des normes CIP aux entités qui étaient exemptées de l'application de la version 1.
	Entités qui possèdent des installations de production à vocation industrielle		2019-04-01	2020-04-01	Donner le temps nécessaire à la mise en œuvre de la version 6 des normes CIP aux entités qui étaient exemptées de l'application de la version 1.
• CIP-003-6, Annexe 1, Sect.2 • CIP-003-6,	Entités visées par la version 1 des normes CIP adoptées par la Régie.	2018-09-01	2018-09-01	2018-09-01	Uniformisation des pratiques avec les autres juridictions.

Norme	Entité	Dates d'implantation aux États-Unis	Date d'entrée en vigueur proposée au Québec		Justification
			Impacts moyen et élevé	Impacts faible	
Annexe 1, Sect.3	Entités exemptées de l'application de la version 1 des normes CIP en vertu des dispositions particulières associées à ces normes.		2018-10-01	2019-10-01	Donner le temps nécessaire à la mise en œuvre de la version 6 des normes CIP aux entités qui étaient exemptées de l'application de la version 1.
	Entités qui possèdent des installations de production à vocation industrielle		2019-04-01	2020-04-01	Donner le temps nécessaire à la mise en œuvre de la version 6 des normes CIP aux entités qui étaient exemptées de l'application de la version 1.

La norme doit être mise en vigueur en même temps que l'ajout des termes de glossaire « connectivité externe routable à impact faible » et « point d'accès électronique de système électronique BES à impact faible ».

**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

## **Annexe 1**

Aucune disposition particulière

## **Annexe 2**

Aucune disposition particulière

## **Principes directeurs et fondements techniques**

Aucune disposition particulière

## **Justification**

Aucune disposition particulière

### Historique des versions

Révision	Date d'adoption	Intervention	Suivi des modifications
0	xx-mois-xx	Nouvelle annexe.	Nouvelle