Normes de fiabilité (version française)

A. Introduction

1. **Titre :** Cybersécurité – Mécanismes de gestion de la sécurité

2. **Numéro :** CIP-003-8

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 de la présente norme, les entités fonctionnelles indiquées ci-après sont appelées collectivement « entités responsables ». Si certaines exigences visent plus spécifiquement une entité fonctionnelle ou un sous-ensemble 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 systèmes, *installations* et équipements suivants pour la protection ou la remise en charge du *BES* :

   4.1.2.1. Système de délestage de *charge* en sous-fréquence (DSF) ou 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 des délestages automatiques de *charge* de 300 MW ou plus sous la commande d'un système commun détenu par l'entité responsable, sans intervention humaine.

   4.1.2.2. *Automatisme de réseau* (*RAS*) visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou de l'*entité régionale*.

   4.1.2.3. *Système de protection* de réseau de *transport* (à l'exclusion des systèmes de DSF et de DST) visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou de l'*entité régionale*.

   4.1.2.4. *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 de la fiabilité***

   4.1.6. ***Exploitant de réseau de transport***

   4.1.7. ***Propriétaire d'installation de transport***

4.2.*Installations* : Dans le contexte de la présente norme, les systèmes, *installations* et équipements suivants détenus par une entité responsable indiquée à la section 4.1 sont visés par ces exigences. Si certaines exigences visent plus spécifiquement un type ou un sous-ensemble de systèmes, d'*installations* ou d'équipements, ceux-ci sont précisés explicitement.

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

4.2.1.1. 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 des délestages automatiques de *charge* de 300 MW ou plus sous la commande d'un système commun détenu par l'entité responsable, sans intervention humaine.

4.2.1.2. *Automatisme de réseau* (*RAS*) visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou de l'*entité régionale*.

4.2.1.3. *Système de protection* de réseau de *transport* (à l'exclusion des systèmes de DSF et de DST) visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou de l'*entité régionale*.

4.2.1.4. *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-003-8 :

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 électronique* (*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, conformément 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-003-8.

6. Contexte :

La norme CIP-003 fait partie d'une série de normes CIP sur la cybersécurité qui exigent l'inventaire et la catégorisation initiales des *systèmes électroniques BES* ainsi que des mesures organisationnelles, opérationnelles et administratives pour atténuer 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, mais 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 dans les exigences et les 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 de DSF et de DST. Ce seuil particulier de 300 MW pour les systèmes de DSF et de DST provient de la version 1 des normes CIP sur la cybersécurité. Ce seuil demeure à 300 MW puisqu'il concerne spécifiquement les systèmes de DST et de DSF, qui constituent des efforts de dernier recours pour sauver le *BES*. Un examen des tolérances des systèmes de 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 de 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 des *circonstances CIP exceptionnelles* et mesures d'intervention.

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 ;

1.2.4. intervention en cas d'*incident de cybersécurité* ;

1.2.5. atténuation des risques liés à l'introduction de programmes malveillants à partir d'*actifs électroniques temporaires* et de *supports de stockage amovibles* ; et

1.2.6. déclaration des *circonstances CIP exceptionnelles* et mesures d'intervention.

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 comprenant 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 désignation 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 visant à surveiller et à assurer la conformité avec les 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 les 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 de la conformité et d'application des normes

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.

Niveau de gravité de la non-conformité (VSL)

Ex.	Horizon	VRF	Niveau de gravité de la non-conformité (CIP-003-8)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
E1.	**Planification de l'exploitation**	**Moyen**	L'entité responsable a documenté et mis en œuvre une ou plusieurs politiques de cybersécurité pour ses *systèmes électroniques BES* à impact élevé et moyen, mais en omettant l'un des neuf thèmes indiqués à l'exigence E1. (E1.1) OU L'entité responsable a terminé le réexamen de sa ou ses politiques de cybersécurité documentées pour ses *systèmes électroniques BES* 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) OU L'entité responsable a fait approuver par le *cadre supérieur CIP* sa ou ses politiques de cybersécurité documentées pour ses *systèmes électroniques*	L'entité responsable a documenté et mis en œuvre une ou plusieurs politiques de cybersécurité pour ses *systèmes électroniques BES* à impact élevé et moyen, mais en omettant deux des neuf thèmes indiqués à l'exigence E1. (E1.1) OU L'entité responsable a terminé le réexamen de sa ou ses politiques de cybersécurité documentées pour ses *systèmes électroniques BES* 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) OU L'entité responsable a fait approuver par le *cadre supérieur CIP* sa ou ses politiques de cybersécurité documentées pour ses *systèmes électroniques*	L'entité responsable a documenté et mis en œuvre une ou plusieurs politiques de cybersécurité pour ses *systèmes électroniques BES* à impact élevé et moyen, mais en omettant trois des neuf thèmes indiqués à l'exigence E1. (E1.1) OU L'entité responsable a terminé le réexamen de sa ou ses politiques de cybersécurité documentées pour ses *systèmes électroniques BES* 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) OU L'entité responsable a fait approuver par le *cadre supérieur CIP* sa ou ses politiques de cybersécurité documentées pour ses *systèmes électroniques*	L'entité responsable a documenté et mis en œuvre une ou plusieurs politiques de cybersécurité pour ses *systèmes électroniques BES* à impact élevé et moyen, mais en omettant au moins quatre des neuf thèmes indiqués à l'exigence E1. (E1.1) OU L'entité responsable n'avait aucune politique de cybersécurité documentée pour ses *systèmes électroniques BES* à impact élevé et moyen, comme le prescrit l'exigence E1. (E1.1) OU 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) OU L'entité responsable n'a pas fait approuver par le *cadre*

Ex.	Horizon	VRF	Niveau de gravité de la non-conformité (CIP-003-8)			
			VSL faible	**VSL modéré**	**VSL élevé**	**VSL critique**
			BES 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 *systèmes électroniques BES* à impact faible selon les critères de la norme CIP-002, mais en omettant un des six 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 *systèmes électroniques BES* 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	*BES* 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 *systèmes électroniques BES* à impact faible selon les critères de la norme CIP-002, mais en omettant deux des six 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 *systèmes électroniques BES* à impact faible selon les critères de la norme CIP-002, mais dans un délai de plus de 16 mois civils et	*BES* 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 *systèmes électroniques BES* à impact faible selon les critères de la norme CIP-002, mais en omettant trois des six 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 *systèmes électroniques BES* à impact faible selon les critères de la norme CIP-002, mais dans un délai de plus de 17 mois civils et	*supérieur CIP* sa ou ses politiques de cybersécurité documentées pour ses *systèmes électroniques BES* 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 *systèmes électroniques BES* à impact faible selon les critères de la norme CIP-002, mais en omettant au moins quatre des six 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 *systèmes électroniques BES* à impact faible selon les

Ex.	Horizon	VRF	Niveau de gravité de la non-conformité (CIP-003-8)			
			VSL faible	**VSL modéré**	**VSL élevé**	**VSL critique**
			suivant le réexamen précédent. (E1.2) OU L'entité responsable a fait approuver par le *cadre supérieur CIP*, selon l'exigence E1, sa ou ses politiques de cybersécurité documentées pour ses actifs qui comportent des *systèmes électroniques BES* 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)	d'au plus 17 mois civils suivant le réexamen précédent. (E1.2) OU L'entité responsable a fait approuver par le *cadre supérieur CIP*, selon l'exigence E1, sa ou ses politiques de cybersécurité documentées pour ses actifs qui comportent des *systèmes électroniques BES* 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)	d'au plus 18 mois civils suivant le réexamen précédent. (E1.2) OU L'entité responsable a fait approuver par le *cadre supérieur CIP*, selon l'exigence E1, sa ou ses politiques de cybersécurité documentées pour ses actifs qui comportent des *systèmes électroniques BES* 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)	critères de la norme CIP-002. (E1.2) OU L'entité responsable n'a pas fait approuver par le *cadre supérieur CIP*, selon l'exigence E1, sa ou ses politiques de cybersécurité documentées pour ses actifs qui comportent des *systèmes électroniques BES* à impact faible selon les critères de la norme CIP-002 dans un délai de 18 mois civils suivant l'approbation précédente. (E1.2)
E2.	**Planification de l'exploitation**	**Faible**	L'entité responsable a documenté son ou ses plans de cybersécurité pour ses actifs comportant des *systèmes électroniques BES* à impact faible, mais n'a pas documenté son plan de sensibilisation à la cybersécurité conformément à la section 1 de l'annexe 1	L'entité responsable a documenté son ou ses plans de cybersécurité pour ses actifs comportant des *systèmes électroniques BES* à impact faible, mais n'a pas fait de rappel des pratiques de cybersécurité au moins une fois tous les 15 mois civils conformément à la section 1 de l'annexe 1	L'entité responsable a documenté le contrôle des accès physiques pour ses actifs comportant des *systèmes électroniques BES* à impact faible, mais n'a pas mis en place les mesures de sécurité physique conformément à la section 2 de l'annexe 1 portant sur l'exigence E2. (E2)	L'entité responsable n'a pas documenté et mis en œuvre un ou plusieurs plans de cybersécurité pour ses actifs comportant des *systèmes électroniques BES* à impact faible conformément à l'annexe 1 portant sur l'exigence E2. (E2)

Ex.	Horizon	VRF	Niveau de gravité de la non-conformité (CIP-003-8)			
			VSL faible	**VSL modéré**	**VSL élevé**	**VSL critique**
			portant sur l'exigence E2. (E2) OU L'entité responsable a mis en place un contrôle des accès électroniques, mais n'a pas documenté son ou ses plans de cybersécurité concernant le contrôle des accès électroniques conformément à la section 3 de l'annexe 1 portant sur l'exigence E2. (E2) OU L'entité responsable a documenté son ou ses plans de cybersécurité pour ses actifs comportant des *systèmes électroniques BES* à impact faible, mais n'a pas documenté un ou plusieurs plans d'intervention en cas d'*incident de cybersécurité* conformément à la section 4 de l'annexe 1 portant sur l'exigence E2. (E2) OU	portant sur l'exigence E2. (E2) OU L'entité responsable a documenté son ou ses plans de cybersécurité pour ses actifs comportant des *systèmes électroniques BES* 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. (E2) OU L'entité responsable a documenté son ou ses plans de cybersécurité pour ses actifs comportant des *systèmes électroniques BES* à impact faible, mais n'a pas documenté de mesures de contrôle des accès électroniques conformément à la section 3 de l'annexe 1 portant sur l'exigence E2. (E2) OU	OU L'entité responsable a documenté son ou ses plans de cybersécurité pour le contrôle des accès électroniques à ses actifs comportant des *systèmes électroniques BES* à impact faible, mais n'a pas limité les communications aux seuls accès entrants et sortants nécessaires conformément à la section 3.1 de l'annexe 1 portant sur l'exigence E2. (E2) OU L'entité responsable a documenté un ou plusieurs plans d'intervention en cas d'*incident de cybersécurité* dans le cadre de son ou ses plans de cybersécurité pour ses actifs comportant des *systèmes électroniques BES* à impact faible, mais n'a pas mis à l'essai chaque plan d'intervention en cas d'*incident de cybersécurité* au moins une fois tous les 36 mois civils conformément à la	

Ex.	Horizon	VRF	Niveau de gravité de la non-conformité (CIP-003-8)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
			L'entité responsable a documenté un ou plusieurs plans d'intervention en cas d'*incident de cybersécurité* dans le cadre de son ou ses plans de cybersécurité pour ses actifs comportant des *systèmes électroniques BES* à impact faible, mais n'a pas mis à jour chaque plan d'intervention en cas d'*incident de cybersécurité* dans un délai de 180 jours conformément à la section 4 de l'annexe 1 portant sur l'exigence E2. (E2) OU L'entité responsable a documenté son ou ses plans concernant les *actifs électroniques temporaires* et les *supports de stockage amovibles*, mais n'a pas géré ses *actifs électroniques temporaires* conformément à la section 5.1 de l'annexe 1 portant sur l'exigence E2. (E2) OU L'entité responsable a documenté son ou ses plans	L'entité responsable a documenté son ou ses plans de cybersécurité portant sur le contrôle des accès électroniques, mais n'a pas mis en place une authentification pour toute *connectivité par lien commuté* donnant accès à un ou des *systèmes électroniques BES* à impact faible, selon les capacités de l'*actif électronique*, conformément à la section 3.2 de l'annexe 1 portant sur l'exigence E2. (E2) OU L'entité responsable a documenté un ou plusieurs plans d'intervention en cas d'incident dans le cadre de son ou ses plans de cybersécurité pour ses actifs comportant des *systèmes électroniques BES* à impact faible, mais n'a pas inclus le processus de détection, de classement et d'intervention en cas d'*incident de cybersécurité* conformément à la section 4 de l'annexe 1	section 4 de l'annexe 1 portant sur l'exigence E2. (E2) OU L'entité responsable a documenté le processus consistant à déterminer si un *incident de cybersécurité* constaté est un *incident de cybersécurité à déclarer*, mais n'a pas avisé l'Electricity Information Sharing and Analysis Center (E-ISAC) conformément à la section 4 de l'annexe 1 portant sur l'exigence E2. (E2) OU L'entité responsable a documenté son ou ses plans pour les *actifs électroniques temporaires* et les *supports de stockage amovibles*, mais n'a pas mis en place de mesures pour atténuer le risque lié à l'introduction de programmes malveillants à partir d'*actifs électroniques temporaires* gérés par l'entité responsable conformément à la section 5.1 de	

Ex.	Horizon	VRF	Niveau de gravité de la non-conformité (CIP-003-8)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
			concernant les *actifs électroniques temporaires*, mais n'a pas documenté les mesures applicables aux *supports de stockage amovibles* conformément à la section 5.3 de l'annexe 1 portant sur l'exigence E2. (E2)	portant sur l'exigence E2. (E2) OU L'entité responsable a documenté son ou ses plans de cybersécurité pour ses actifs comportant des *systèmes électroniques BES* à impact faible, mais n'a pas documenté le processus consistant à déterminer si un *incident de cybersécurité* constaté est un *incident de cybersécurité à déclarer*, puis à en aviser l'Electricity Information Sharing and Analysis Center (E-ISAC) conformément à la section 4 de l'annexe 1 portant sur l'exigence E2. (E2) OU L'entité responsable a documenté son ou ses plans pour les *actifs électroniques temporaires* et les *supports de stockage amovibles*, mais n'a pas documenté de mesures pour atténuer le risque lié à l'introduction de programmes malveillants à partir d'*actifs électroniques*	l'annexe 1 portant sur l'exigence E2. (E2) OU L'entité responsable a documenté son ou ses plans pour les *actifs électroniques temporaires* et les *supports de stockage amovibles*, mais n'a pas mis en place de mesures pour atténuer le risque lié à l'introduction de programmes malveillants à partir d'*actifs électroniques temporaires* gérés par une tierce partie autre que l'entité responsable conformément à la section 5.2 de l'annexe 1 portant sur l'exigence E2. (E2) OU L'entité responsable a documenté son ou ses plans pour les *actifs électroniques temporaires* et les *supports de stockage amovibles*, mais n'a pas mis en place de mesures pour neutraliser la menace d'un programme malveillant détecté sur un *support de stockage amovible* avant de	

Ex.	Horizon	VRF	Niveau de gravité de la non-conformité (CIP-003-8)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
				temporaires gérés par l'entité responsable conformément aux sections 5.1 et 5.3 de l'annexe 1 portant sur l'exigence E2. (E2) OU L'entité responsable a documenté son ou ses plans pour les *actifs électroniques temporaires* et les *supports de stockage amovibles*, mais n'a pas documenté de mesures pour atténuer le risque lié à l'introduction de programmes malveillants à partir d'*actifs électroniques temporaires* gérés par une tierce partie autre que l'entité responsable conformément à la section 5.2 de l'annexe 1 portant sur l'exigence E2. (E2) OU L'entité responsable a documenté son ou ses plans concernant les *actifs électroniques temporaires* et les *supports de stockage amovibles*, mais n'a pas mis en place de mesures	connecter celui-ci à un *système électronique BES* à impact faible conformément à la section 5.3 de l'annexe 1 portant sur l'exigence E2. (E2)	

Ex.	Horizon	VRF	Niveau de gravité de la non-conformité (CIP-003-8)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
				applicables aux *supports de stockage amovibles* conformément à la section 5.3 de l'annexe 1 portant sur l'exigence E2. (E2)		
E3.	**Planification de l'exploitation**	**Moyen**	L'entité responsable a désigné nominativement un *cadre supérieur CIP*, 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 *cadre supérieur CIP*, 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 *cadre supérieur CIP*, 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 *cadre supérieur CIP*. OU L'entité responsable a désigné nominativement un *cadre supérieur CIP*, mais n'a pas documenté un changement concernant celui-ci dans un délai de 60 jours civils suivant ce changement. (E3)

Ex.	Horizon	VRF	Niveau de gravité de la non-conformité (CIP-003-8)			
			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)	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 *cadre supérieur CIP*. (E4) OU 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)

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	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. Suppression de la mention sur la prise en compte des considérations d'affaires. Remplacement de l'organisation régionale de fiabilité par l'*entité régionale* comme entité responsable. Reformulation de la date d'entrée en vigueur. Remplacement de « *responsable de la surveillance de la conformité* » par « *responsable des mesures pour assurer la conformité* ».	
3	16 décembre 2009	Changement du numéro de version de -2 à -3. 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.	
3	16 décembre 2009	Approbation par le Conseil d'administration de la NERC.	
3	31 mars 2010	Approbation par la FERC.	

Version	Date	Intervention	Suivi des modifications
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.	Remplacement de 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 *systèmes électroniques BES* à impact faible.
6	21 janvier 2016	Ordonnance de la FERC approuvant la norme CIP-003-6 (dossier RM15-14-000).	
7	9 février 2017	Adoption par le Conseil d'administration de la NERC.	Révision en réponse à des prescriptions de l'ordonnance 822 de la FERC concernant 1) la définition de *LERC* et 2) les actifs temporaires.

Version	Date	Intervention	Suivi des modifications
7	19 avril 2018	Ordonnance de la FERC approuvant la norme CIP-003-7 (dossier RM17-11-000).	
8	9 mai 2019	Adoption par le Conseil d'administration de la NERC.	Suppression des références aux plans de défense. Changements en réponse aux prescriptions de l'ordonnance 843 de la FERC concernant l'atténuation des risques liés aux programmes malveillants.
8	31 juillet 2019	Ordonnance de la FERC approuvant la norme CIP-003-8 (dossier RM19-5-000).	

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) à tout *actif électronique* qu'elle décide d'affecter, conformément à la section 3.1, au contrôle des accès électroniques.

Section 3. Contrôle des accès électroniques : Pour chaque actif comportant un ou des *systèmes électroniques BES* à impact faible selon les critères de la norme CIP-002, l'entité responsable doit mettre en place un contrôle des accès électroniques qui :

3.1 autorisent uniquement les accès entrants et sortants nécessaires, selon l'évaluation de l'entité responsable, pour toute communication :

i. entre un ou des *systèmes électroniques BES* à impact faible et tout *actif électronique* situé à l'extérieur de l'actif comportant un ou des *systèmes électroniques BES* à impact faible ;

ii. assurée par un protocole routable en entrée ou en sortie de l'actif comportant le ou les *systèmes électroniques BES* à impact faible ; et

iii. ne servant pas à des fonctions de commande ou de protection à délai critique entre des dispositifs électroniques intelligents (par exemple, des communications utilisant le protocole R-GOOSE de la norme CEI TR-61850-90-5) ;

3.2 authentifient toute *connectivité par lien commuté* donnant 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 Information Sharing and Analysis Center (E-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.

Section 5. Atténuation des risques liés à l'introduction de programmes malveillants à partir d'*actifs électroniques temporaires* ou de *supports de stockage amovibles* : Chaque entité responsable doit mettre en œuvre, sauf en cas de *circonstances CIP exceptionnelles*, un ou des plans visant à réaliser l'objectif d'atténuer le risque lié à l'introduction de programmes malveillants dans les *systèmes électroniques BES* à impact faible à partir d'*actifs électroniques temporaires* ou de *supports de stockage amovibles*. Ce ou ces plans doivent comprendre :

5.1 pour tout *actif électronique temporaire* géré par l'entité responsable, le recours à un ou plusieurs des moyens suivants, utilisés en permanence ou à la demande (selon les capacités de l'*actif électronique temporaire*) :

- logiciel antivirus, avec mises à jour manuelles ou systématiques des signatures ou des séquences de code ;
- liste blanche d'applications ; ou
- autres moyens d'atténuer le risque lié à l'introduction de programmes malveillants ;

5.2 pour tout *actif électronique temporaire* géré par une tierce partie autre que l'entité responsable :

5.2.1 l'application d'une ou de plusieurs des mesures suivantes avant de connecter l'*actif électronique temporaire* à un *système électronique BES* à impact faible (selon les capacités de l'*actif électronique temporaire*) :

- examen du degré de maintien à jour de l'antivirus ;
- examen de la procédure de mise à jour de l'antivirus adoptée par la tierce partie ;
- examen de l'utilisation par la tierce partie de listes blanches d'applications ;
- examen de l'utilisation de systèmes d'exploitation et de logiciels exécutables uniquement à partir de supports non inscriptibles ;

- examen des mesures de renforcement du système d'exploitation adoptées par la tierce partie ; ou
- autres moyens d'atténuation du risque lié à l'introduction de programmes malveillants ;

5.2.2 pour toute méthode utilisée conformément à la section 5.2.1, les entités responsables doivent déterminer si des mesures d'atténuation supplémentaires sont nécessaires, et les mettre en œuvre avant de connecter l'*actif électronique temporaire* ;

5.3 pour les *supports de stockage amovibles*, le recours à chacun des moyens suivants :

5.3.1 mesures permettant de détecter les programmes malveillants sur les *supports de stockage amovibles* au moyen d'un *actif électronique* autre qu'un *système électronique BES* ; et

5.3.2 mesures permettant de neutraliser la menace d'un programme malveillant détecté sur un *support de stockage amovible* avant de connecter ce support à un *système électronique BES* à impact faible.

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 tout *actif électronique* désigné par l'entité responsable comme assurant un contrôle des accès électroniques selon la section 3.1 de l'annexe 1, s'il y a lieu.

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

1. documentation attestant qu'à chaque actif ou groupe d'actifs comportant des *systèmes électroniques BES* à impact faible, toute communication routable entre un ou plusieurs de ces *systèmes électroniques BES* à impact faible et un ou des *actifs électroniques* à l'extérieur de l'actif en question est limitée par un contrôle des accès électroniques aux seuls accès électroniques entrants et sortants que l'entité responsable juge nécessaires, sauf si l'entité peut démontrer qu'il s'agit d'une communication utilisée pour des fonctions de commande ou de protection à délai critique entre des dispositifs électroniques intelligents. Exemples non limitatifs de pièces justificatives : schémas montrant le contrôle des communications entrantes et sortantes entre le ou les *systèmes électroniques BES* à impact faible et un ou des *actifs électroniques* situés à l'extérieur de l'actif comportant ce ou ces *systèmes électroniques BES*, ou des listes de contrôle des accès électroniques mises en œuvre (contrôles d'accès par adresse IP, par ports ou par service, passerelles unidirectionnelles, etc.) ;
2. 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 Information Sharing and Analysis Center (E-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.

Section 5. Atténuation des risques liés à l'introduction de programmes malveillants à partir d'*actifs électroniques temporaires* ou de *supports de stockage amovibles* :

1. Exemples non limitatifs de pièces justificatives attestant la conformité avec la section 5.1 : documentation des moyens utilisés pour atténuer le risque lié à l'introduction de programmes malveillants, comme des logiciels antivirus et des processus de gestion des mises à jour des signatures ou des séquences de code, des pratiques de liste blanche d'applications, des processus de restriction des communications ou d'autres moyens d'atténuation appropriés. Si un *actif électronique temporaire* n'a pas la capacité de mettre en place certains moyens d'atténuation du risque lié à l'introduction de programmes malveillants, les pièces justificatives peuvent comprendre une documentation du fournisseur ou de l'entité responsable indiquant que l'*actif électronique temporaire* n'a pas cette capacité.
2. Exemples non limitatifs de pièces justificatives attestant la conformité avec la section 5.2.1 : documentation provenant de systèmes de gestion des changements, courriels ou procédures qui documentent un examen du degré de maintien à jour des antivirus installés ; notes de service, courriels, documentation de système, politiques ou contrats d'une tierce partie autre que l'entité responsable qui décrivent le processus de mise à jour des antivirus, l'utilisation d'une liste blanche d'applications, l'utilisation de systèmes d'exploitation sur support externe ou le renforcement du système d'exploitation par la tierce partie ; pièces justificatives provenant de systèmes de gestion des changements, courriels ou contrats indiquant que l'entité responsable juge acceptables les pratiques de la tierce partie ; ou documentation d'autres moyens d'atténuation du risque lié à l'introduction de programmes malveillants pour les *actifs électroniques temporaires* gérés par la tierce partie. Si un *actif électronique temporaire* n'a pas la capacité de mettre en place certains moyens d'atténuation du risque lié à l'introduction de programmes malveillants, les pièces justificatives peuvent comprendre une documentation de l'entité responsable ou de la tierce partie indiquant que l'*actif électronique temporaire* n'a pas cette capacité.

Exemples non limitatifs de pièces justificatives attestant la conformité avec la section 5.2.2 de l'annexe 1 : documentation provenant de systèmes de gestion des changements, courriels ou contrats attestant qu'un examen a été effectué pour déterminer le besoin de mesures d'atténuation supplémentaires, et que ces mesures, le cas échéant, ont été mises en œuvre avant la connexion de l'*actif électronique temporaire* géré par une tierce partie autre que l'entité responsable.

3. Exemples non limitatifs de pièces justificatives attestant la conformité avec la section 5.3.1 : processus documentés des moyens de détection des programmes malveillants, comme les résultats de balayage paramétré pour les *supports de stockage amovibles* ou la mise en œuvre du balayage à la demande. Exemples non limitatifs de pièces justificatives attestant la conformité avec la section 5.3.2 : processus documentés des moyens d'atténuation du risque lié aux programmes malveillants détectés sur les *supports de stockage amovibles*, comme les journaux créés par les mécanismes de détection qui montrent les résultats du balayage et indiquent la neutralisation des programmes malveillants détectés sur les *supports de stockage amovibles*, ou une confirmation documentée par l'entité que les *supports de stockage amovibles* sont considérés comme exempts de tout programme malveillant.

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 estla liste des entités fonctionnelles de la NERC auxquelles s'applique la norme. Si l'entité est enregistrée au titre d'une ou de plusieurs des entités fonctionnelles énumérées à la section 4.1., alors les normes CIP sur la cybersécurité de la NERC s'appliquent. Il est à noter qu'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 désignée à la section 4.1. qui 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 comprenne déjà l'appartenance au *BES*, l'utilisation additionnelle du terme « *BES* » vise ici à renforcer la portée d'applicabilité pour ces *installations*, en particulier dans cette section sur l'applicabilité. Cela établit quels sont les *installations*, systèmes et équipements visés par les normes.

Exigence E1

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 globale de haut niveau et confier les détails à des documents de niveau inférieur dans la hiérarchie documentaire. Dans le cas d'une politique globale de haut niveau, l'entité responsable devrait fournir la politique globale ainsi que les documents complémentaires afin de démontrer la conformité avec l'exigence E1 de la norme CIP-003-8.

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 l'alinéa 1.1 de l'exigence E1 de la norme CIP 003-8. Si une entité responsable a répertorié, 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 six thèmes prescrits à l'alinéa 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-003-8, 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 l'alinéa 1.1, l'entité responsable peut 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

Dans le contexte de l'alinéa 1.2, l'entité responsable peut tenir compte des points suivants pour chacun des thèmes obligatoires dans sa ou ses politiques de cybersécurité visant ses *systèmes électroniques BES* à impact faible, le cas échéant :

1.2.1 Sensibilisation à la cybersécurité

- Mesures de sensibilisation à la sécurité
- Détermination des groupes visés par les mesures de sensibilisation à la cybersécurité

1.2.2 Mesures de sécurité physique

- Approches acceptables pour la sélection des mesures de sécurité physique

1.2.3 Contrôle des accès électroniques

- Approches acceptables pour la sélection des moyens de contrôle des accès électroniques

1.2.4 Intervention en cas d'*incident de cybersécurité*

- Détection des *incidents de cybersécurité*
- Notifications appropriées en cas de découverte d'un incident
- Obligations de signaler les *incidents de cybersécurité*

1.2.5 Atténuation des risques liés à l'introduction de programmes malveillants à partir d'*actifs électroniques temporaires* ou de *supports de stockage amovibles*

- Utilisation acceptable des *actifs électroniques temporaires* et des *supports de stockage amovibles*

- Méthodes visant à atténuer le risque lié à l'introduction de programmes malveillants dans les *systèmes électroniques BES* à impact faible à partir d'*actifs électroniques temporaires* et de *supports de stockage amovibles*
- Méthodes pour demander des *actifs électroniques temporaires* et des *supports de stockage amovibles*

1.2.6 Déclaration des *circonstances CIP exceptionnelles* et mesures d'intervention

- Processus de déclaration d'une *circonstance CIP exceptionnelle*
- Processus d'intervention en cas de *circonstance CIP exceptionnelle* déclarée

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

L'exigence E2 vise à obliger chaque entité responsable à créer, à documenter et à mettre en œuvre un ou plusieurs plans de cybersécurité afin de réaliser l'objectif de sécurité pour la protection des *systèmes électroniques BES* à impact faible. Les protections requises sont conçues dans le cadre d'un programme qui s'applique aux *systèmes électroniques BES* à impact faible de façon collective, au niveau des actifs (à partir de la liste des actifs comportant des *systèmes électroniques BES* à impact faible établie selon la norme CIP-002), et non au niveau de chaque dispositif ou système.

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. Les plans de cybersécurité établis selon l'exigence E2 amènent les entités responsables à documenter la manière dont elles abordent les différents thèmes présentés. Les plans de cybersécurité peuvent renvoyer à d'autres politiques et procédures qui montrent de quelle manière l'entité responsable entend répondre à chacun des thèmes ; ou encore, l'entité responsable peut élaborer des plans de cybersécurité très complets qui contiennent tous les détails des moyens mis en œuvre. Pour respecter l'exigence, il faut que le plan de cybersécurité contienne (textuellement ou par renvoi) suffisamment de détails quant aux moyens adoptés pour répondre à chacun des thèmes.

Des précisions et éclaircissements pour chacun des 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 attestant la conformité, l'entité responsable doit pouvoir présenter le matériel de sensibilisation utilisé, selon la ou les méthodes de communication employées (affiches, courriels, sujets abordés aux réunions de service, etc.). L'intention de l'équipe de rédaction n'est pas d'obliger les entités

responsables à tenir des listes de destinataires ni à 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 place des mesures de contrôle des accès physiques 1) à l'actif ou aux emplacements des *systèmes électroniques BES* à impact faible à l'intérieur de l'actif et 2) à tout *actif électronique* qu'elle décide d'affecter, conformément à la section 3.1 de l'annexe 1, au contrôle des accès électroniques. Si des *actifs électroniques* affectés au contrôle des accès électroniques sont situés à l'intérieur du même actif que le ou les *actifs électroniques BES* à impact faible et qu'ils héritent des mêmes mesures de contrôle des accès physiques et du même besoin déterminé selon la section 2, l'entité responsable peut en tenir compte dans ses politiques ou dans ses plans de cybersécurité de manière à éviter une documentation redondante des mêmes mesures.

L'entité responsable est libre de choisir les méthodes utilisées pour réaliser l'objectif de contrôle des accès physiques 1) aux actifs comportant des *systèmes électroniques BES* à impact faible, ou encore aux *systèmes électroniques BES* à impact faible eux-mêmes, et 2) à tout *actif électronique* affecté par l'entité responsable, le cas échéant, au contrôle des accès électroniques. 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*.

L'objectif de sécurité est de contrôler l'accès physique d'après les besoins déterminés par l'entité responsable. Le besoin d'accès physique peut être documenté au niveau des politiques ; l'intention de l'équipe de rédaction n'est pas d'obliger l'entité à spécifier un besoin pour chaque accès ou autorisation d'accès physique d'un utilisateur.

La surveillance comme mesure de sécurité physique peut servir de complément ou de solution de rechange au contrôle d'accès physique. 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.). L'intention de l'équipe de rédaction n'est pas de rendre nécessaire une surveillance pour chaque *système électronique BES* à impact faible, mais plutôt une surveillance au niveau approprié pour réaliser l'objectif de sécurité en matière de contrôle d'accès physique.

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 réaliser l'objectif de sécurité.

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

La section 3 demande la mise en place d'un contrôle des accès électroniques pour tout actif comportant un ou des *systèmes électroniques BES* à impact faible s'il existe une communication par protocole

routable ou une *connectivité par lien commuté* entre un ou des *actifs électroniques* situés à l'extérieur de cet actif et un ou des *systèmes électroniques BES* à impact faible situés à l'intérieur de cet actif. Ce contrôle des accès électroniques vise à réduire les risques associés à une communication non contrôlée utilisant des protocoles routables ou une *connectivité par lien commuté*.

Dans le contexte de la section 3.1 de l'annexe 1, il est à noter que l'obligation de restreindre les accès électroniques entrants et sortants à ceux qui sont jugés nécessaires s'applique uniquement aux communications qui répondent aux trois critères de la section 3.1 de l'annexe 1. L'entité responsable doit évaluer les communications et si les trois critères sont satisfaits, elle doit documenter et mettre en place une ou des mesures de contrôle des accès électroniques.

Les entités responsables ont une certaine latitude dans le choix des mesures de contrôle des accès électroniques qui répondent à leurs besoins opérationnels tout en réalisant l'objectif de sécurité consistant à autoriser uniquement les accès électroniques entrants et sortants nécessaires entre un ou des *systèmes électroniques BES* à impact faible et un ou des *actifs électroniques* situés à l'extérieur de l'actif comportant ce ou ces *systèmes électroniques BES* à impact faible, si ces accès se font par protocole routable.

Il s'agit essentiellement pour les entités responsables de déterminer s'il y a communication entre un ou des *systèmes électroniques BES* à impact faible et un ou des *actifs électroniques* situés à l'extérieur de l'actif comportant ce ou ces *systèmes électroniques BES* à impact faible, et si cette communication utilise un protocole routable en entrée ou en sortie de l'actif ou encore une *connectivité par lien commuté* vers le ou les *systèmes électroniques BES* à impact faible. Si une telle communication existe, les entités responsables doivent documenter et mettre en place une ou des mesures de contrôle des accès électroniques. Dans le cas d'une communication par protocole routable qui sert à des fonctions de commande ou de protection à délai critique entre des dispositifs électroniques intelligents selon le critère d'exemption aux présentes, les entités responsables doivent documenter cette communication, mais ne sont pas tenues de mettre en place un contrôle des accès électroniques.

Sont visés par cette exigence les actifs qui, selon les critères de la norme CIP-002, comportent un ou des *systèmes électroniques BES* à impact faible ; la détermination d'une communication par protocole routable ou d'une *connectivité par lien commuté* dépend donc des caractéristiques de l'actif. Cependant, l'exigence ne s'applique pas aux communications qui, bien qu'implantées dans l'actif comportant le ou les *systèmes électroniques BES* à impact faible, n'autorisent aucun accès entrant ou sortant aux *systèmes électroniques BES* à impact faible de cet actif.

Exemption de l'exigence de contrôle des accès électroniques

Afin d'éviter d'éventuelles entraves technologiques, il a été décidé que l'obligation de contrôle des accès électroniques ne s'applique pas aux communications entre dispositifs électroniques intelligents qui utilisent des protocoles de communication routables pour assurer des fonctions de commande ou de protection à délai critique, par exemple le protocole R-GOOSE de la norme CEI TR-61850-09-5. Dans ce contexte, l'expression « à délai critique » désigne généralement les fonctions qui seraient vulnérables au délai de transit créé dans la communication par les mesures de contrôle des accès électroniques. Cette exemption ne s'applique pas aux communications SCADA, puisque le taux d'échantillonnage est habituellement de 2 secondes ou plus ; bien qu'elles soient techniquement « à délai critique », les communications SCADA par protocole routable ne sont pas vraiment sensibles aux délais créés par les mesures de contrôle des accès électroniques. Exemple de communications à délai critique qui seraient exemptées : les communications visant à commander le déclenchement d'un disjoncteur dans un délai de quelques cycles. Une entité responsable qui utilise cette technologie n'est pas tenue de mettre en place les mesures de contrôle des accès électroniques prescrites ici. Cette exemption a été ajoutée afin

de ne pas compromettre les fonctions à délai critique associées à cette technologie, et de ne pas entraver le recours futur à de telles fonctions afin d'améliorer la fiabilité au motif qu'elles utiliseraient un protocole routable.

Critères pour déterminer s'il y a communication par protocole routable

Pour déterminer si un contrôle des accès électroniques est exigé, l'entité responsable doit déterminer s'il y a communication entre un ou des *systèmes électroniques BES* à impact faible et un ou des *actifs électroniques* situés à l'extérieur de l'actif comportant ce ou ces *systèmes électroniques BES* à impact faible, et si cette communication utilise un protocole routable en entrée ou en sortie de l'actif.

Lorsqu'il s'agit de déterminer si un protocole routable est utilisé en entrée ou en sortie de l'actif comportant le ou les *systèmes électroniques BES* à impact faible, l'entité responsable dispose d'une certaine latitude. Une approche possible consiste pour l'entité responsable à définir une « frontière électronique » pour l'actif comportant un ou des *systèmes électroniques BES* à impact faible. Il ne s'agit pas ici d'un *périmètre de sécurité électronique*, mais d'une démarcation où l'on constate une communication par protocole routable, en entrée ou en sortie de l'actif en question, entre un *système électronique BES* à impact faible situé à l'intérieur de cet actif et un ou des *actifs électroniques* situés à l'extérieur de cet actif, et donc le besoin d'un contrôle des accès électroniques. Cette frontière électronique peut varier selon le type d'actif (*centre de contrôle*, poste électrique, ressource de production, etc.) et les particularités de sa configuration. Si l'entité responsable adopte cette approche, elle doit définir la « frontière électronique » de façon que le ou les *systèmes électroniques BES* à impact faible présents dans l'actif soient situés à l'intérieur de cette frontière. Cet exercice vise strictement à établir quelles communications par protocole routable et quels réseaux sont internes ou locaux par rapport à l'actif et lesquels sont externes ou situés à l'extérieur de l'actif.

Dans certains cas, l'entité responsable peut considérer que ce qui est interne ou externe à l'actif comportant un ou des *systèmes électroniques BES* à impact faible va clairement de soi lorsqu'il s'agit de déterminer les communications qui existent entre des *actifs électroniques* situés à l'extérieur de l'actif en question et des *systèmes électroniques BES* à impact faible situés à l'intérieur de cet actif. Par exemple, si un ou des *systèmes électroniques BES* à impact faible communiquent avec un *actif électronique* situé à des kilomètres de distance et que la démarcation est claire et sans équivoque, l'entité responsable peut décider de ne pas définir une « frontière électronique », mais de se référer simplement à cette démarcation sans équivoque pour mettre en place des mesures de contrôle des accès électroniques entre le ou les *systèmes électroniques BES* à impact faible situés à l'intérieur de l'actif et le ou les *actifs électroniques* situés à l'extérieur de l'actif.

Détermination des contrôles des accès électroniques

Après avoir déterminé qu'il y a communication routable entre un ou des *systèmes électroniques BES* à impact faible et un ou des *actifs électroniques* situés à l'extérieur de l'actif comportant ce ou ces *systèmes électroniques BES* à impact faible et que cette communication utilise un protocole routable en entrée ou en sortie de l'actif en question, l'entité responsable doit documenter et mettre en place la ou les mesures de contrôle des accès électroniques qu'elle juge adéquates. Il s'agit d'autoriser uniquement les accès électroniques entrants et sortants « nécessaires » selon l'évaluation de l'entité responsable. Quelle que soit la manière choisie pour documenter l'autorisation des accès entrants et sortants et leur nécessité, l'entité responsable doit être en mesure de les justifier. La justification des accès électroniques entrants et sortants jugés « nécessaires » peut être documentée à même le ou les plans de cybersécurité de l'entité responsable, dans un commentaire sur une liste de contrôle d'accès, dans une base de données, sur une feuille de chiffrier ou dans d'autres politiques ou procédures associées aux contrôles des accès électroniques.

Schémas conceptuels

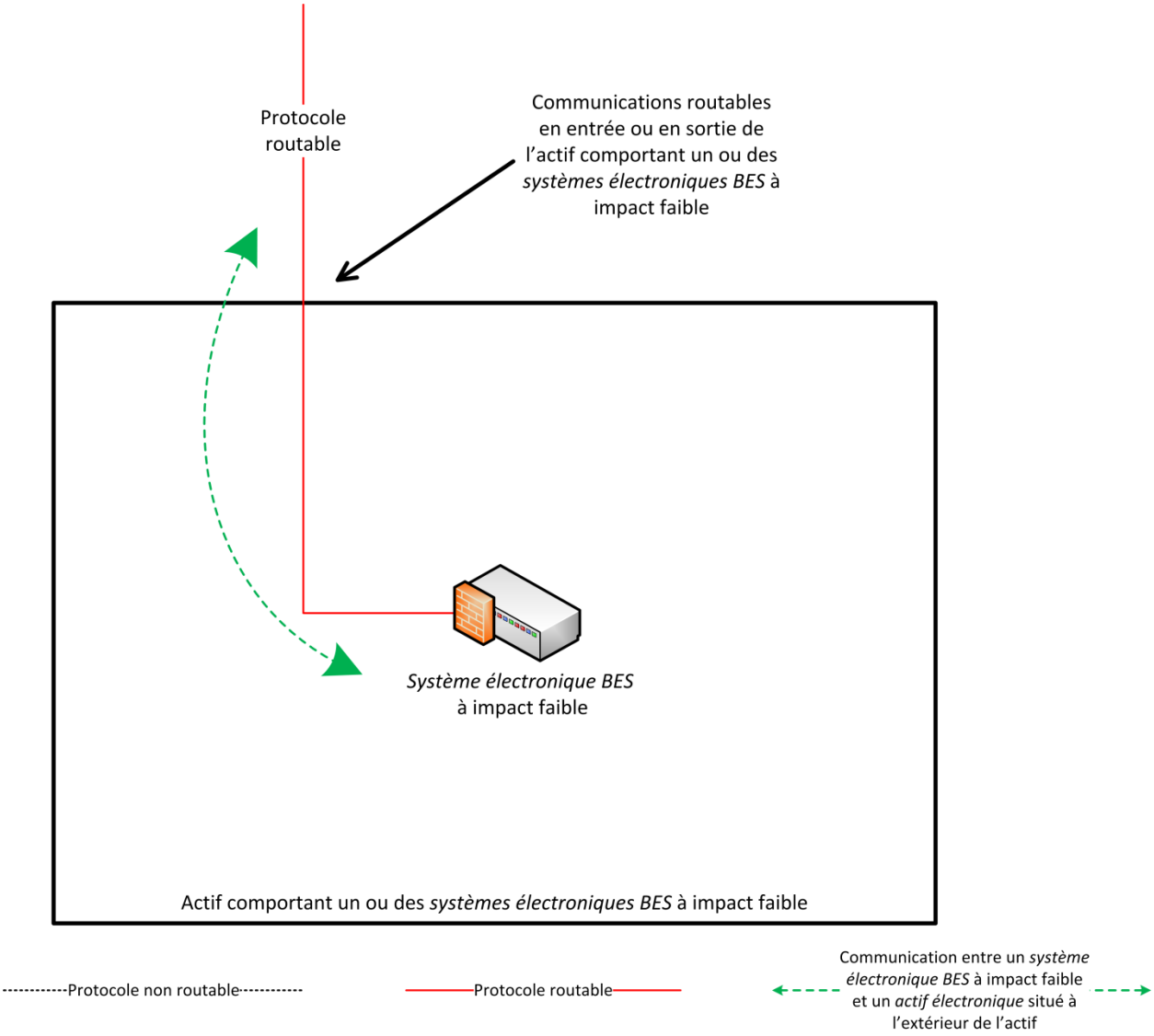
Les schémas des pages suivantes présentent des exemples conceptuels qui illustrent diverses situations de contrôle des accès électroniques. Quels que soient les concepts ou les configurations choisis par l'entité responsable, le but recherché est de réaliser l'objectif de sécurité suivant : autoriser uniquement les accès électroniques entrants et sortants nécessaires pour les communications par protocole routable entre des *systèmes électroniques BES* à impact faible et des *actifs électroniques* situés à l'extérieur de l'actif comportant ce ou ces *systèmes électroniques BES* à impact faible, en entrée ou en sortie de l'actif en question.

REMARQUES :

- Ces schémas ne représentent pas la totalité des concepts applicables.
- La même légende est utilisée pour tous les schémas ; cependant, chaque schéma ne comporte pas nécessairement tous les éléments de la légende.

Modèle de référence 1 – Autorisations d'accès entrant et sortant sur hôte

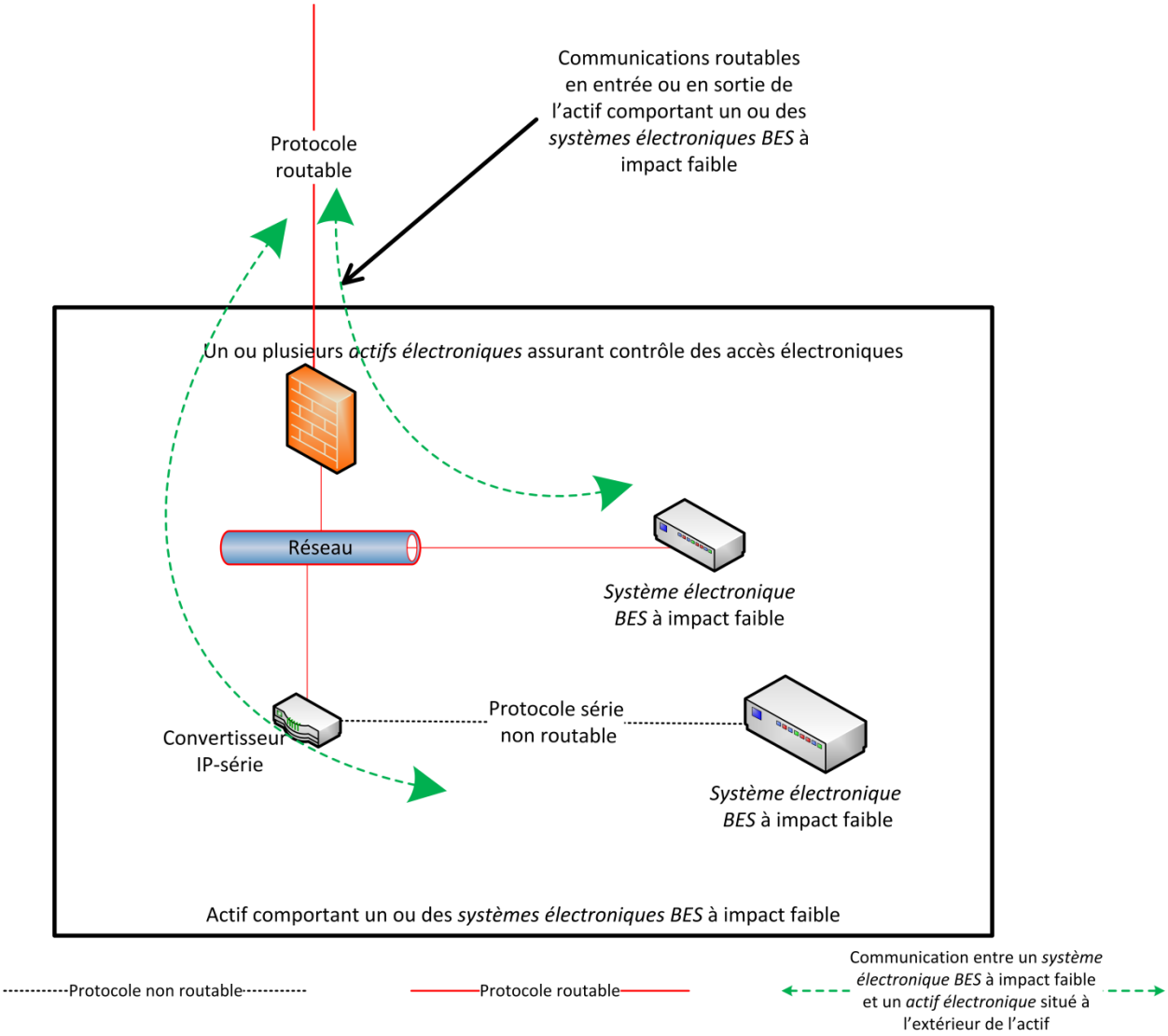
L'entité responsable peut opter pour une technologie de pare-feu hôte implantée dans le ou les *systèmes électroniques BES* à impact faible afin de gérer les autorisations d'accès électronique en les limitant aux accès entrants et sortants nécessaires entre le ou les *systèmes électroniques BES* à impact faible et le ou les *actifs électroniques* situés à l'extérieur de l'actif comportant ce ou ces *systèmes électroniques BES* à impact faible. Si les autorisations sont mises en œuvre au moyen de listes de contrôle d'accès, l'entité responsable peut restreindre les communications en spécifiant des adresses ou des plages d'adresses d'origine et de destination. L'entité responsable peut aussi restreindre les communications en spécifiant des ports ou des services, compte tenu de la capacité du dispositif de contrôle des accès électroniques, du ou des *systèmes électroniques BES* à impact faible ou des applications.



Modèle de référence 1

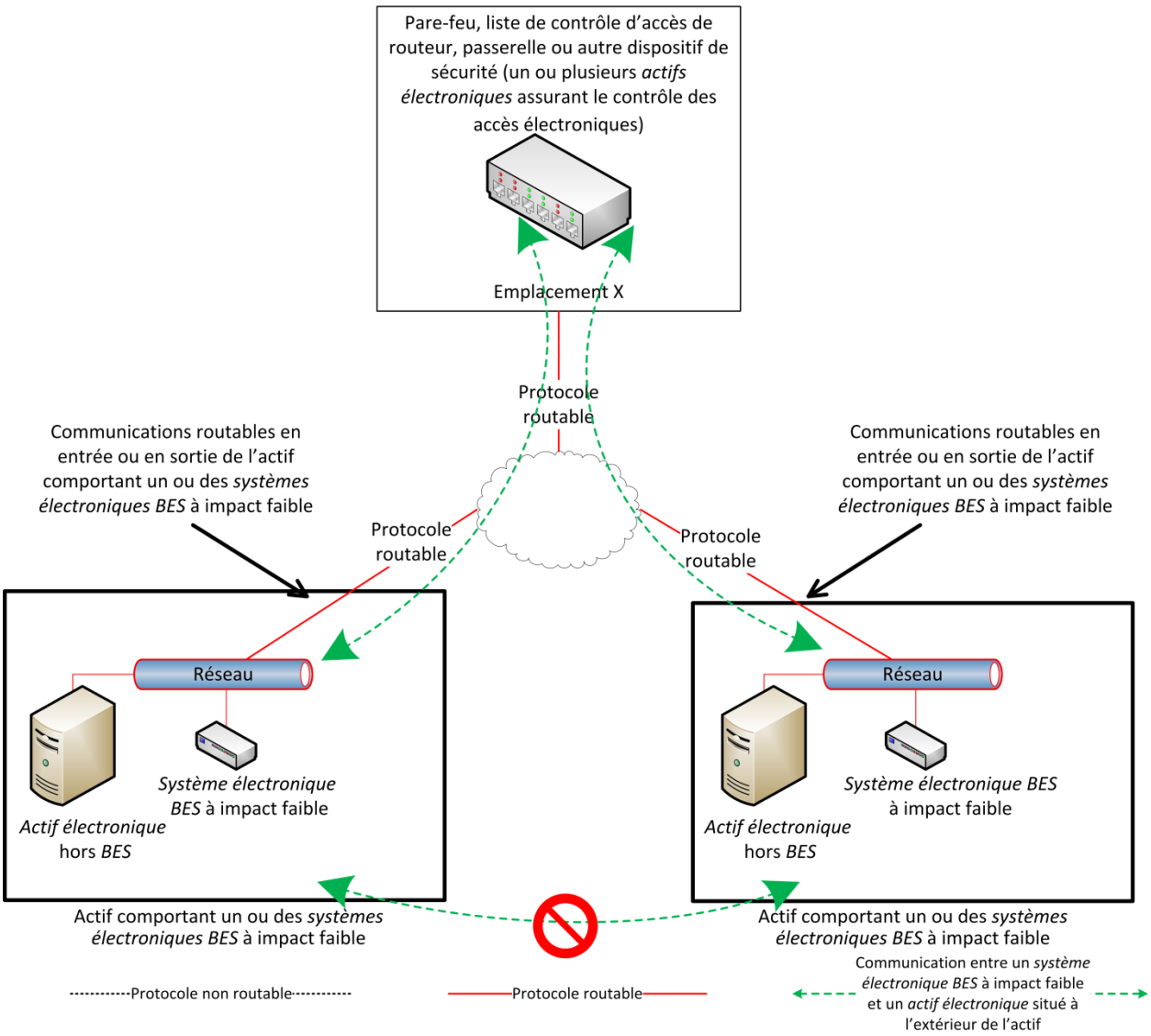
Modèle de référence 2 – Autorisations d'accès entrant et sortant par dispositif réseau

L'entité responsable peut opter pour un dispositif de sécurité qui autorise uniquement les accès électroniques entrants et sortants nécessaires pour le ou les *systèmes électroniques BES* à impact faible situés dans l'actif comportant ce ou ces *systèmes électroniques BES* à impact faible. Dans cet exemple, deux *systèmes électroniques BES* à impact faible sont accessibles par protocole routable en entrée ou en sortie de l'actif comportant ces *systèmes électroniques BES* à impact faible. Le convertisseur IP-série prolonge la session de communication à partir du ou des *actifs électroniques* situés à l'extérieur de l'actif jusqu'au *système électronique BES* à impact faible. Le dispositif de sécurité assure le contrôle des accès électroniques de façon à autoriser uniquement les accès entrants et sortants par protocole routable nécessaires aux *systèmes électroniques BES* à impact faible. Lorsque les autorisations sont mises en œuvre au moyen de listes de contrôle d'accès, l'entité responsable peut restreindre les communications en spécifiant des adresses ou des plages d'adresses d'origine et de destination. L'entité responsable peut aussi restreindre les communications en spécifiant des ports ou des services, compte tenu de la capacité du dispositif de contrôle des accès électroniques, du ou des *systèmes électroniques BES* à impact faible ou des applications.



Modèle de référence 2

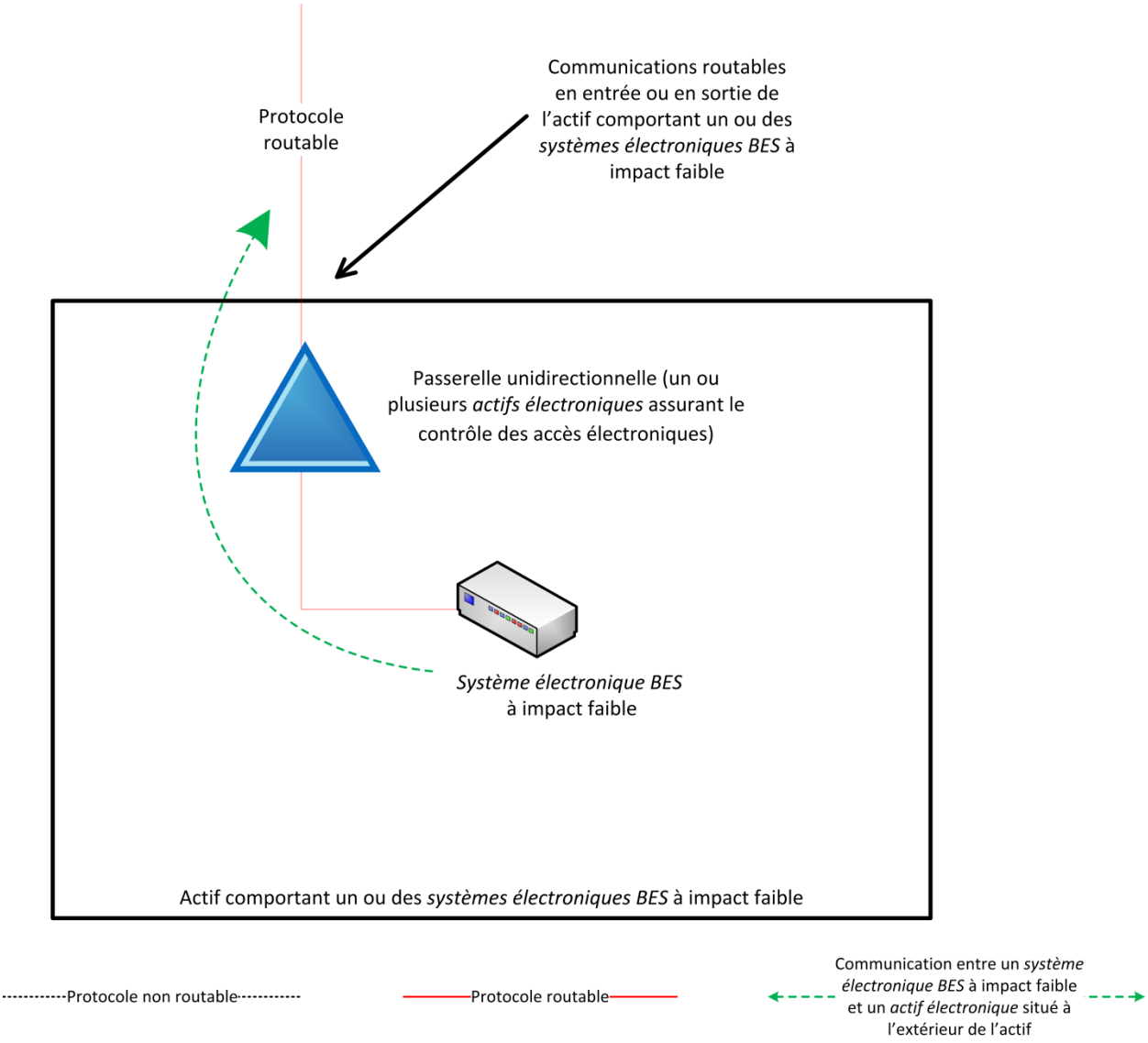
Modèle de référence 3 – Autorisations d'accès entrant et sortant par dispositif réseau centralisé
L'entité responsable peut opter pour un dispositif de sécurité situé à un emplacement centralisé, qui peut ou non être situé dans un autre actif comportant un ou des *systèmes électroniques BES* à impact faible. Le contrôle des accès électroniques ne réside pas nécessairement à l'intérieur de l'actif comportant le ou les *systèmes électroniques BES* à impact faible. Un dispositif de sécurité est en place à l'« emplacement X » pour assurer le contrôle des accès électroniques en autorisant uniquement les accès entrants et sortants par protocole routable nécessaires entre le ou les *systèmes électroniques BES* à impact faible et le ou les *actifs électroniques* situés à l'extérieur de chaque actif comportant un ou des *systèmes électroniques BES* à impact faible. Il faut prendre soin que chacun des accès électroniques entre les actifs transite bien par le ou les *actifs électroniques* désignés par l'entité responsable pour assurer le contrôle des accès électroniques à l'emplacement centralisé. Lorsque les autorisations sont mises en œuvre au moyen de listes de contrôle d'accès, l'entité responsable peut restreindre les communications en spécifiant des adresses ou des plages d'adresses d'origine et de destination. L'entité responsable peut aussi restreindre les communications en spécifiant des ports ou des services, compte tenu de la capacité du dispositif de contrôle des accès électroniques, du ou des *systèmes électroniques BES* à impact faible ou des applications.



Modèle de référence 3

Modèle de référence 4 – Passerelle unidirectionnelle

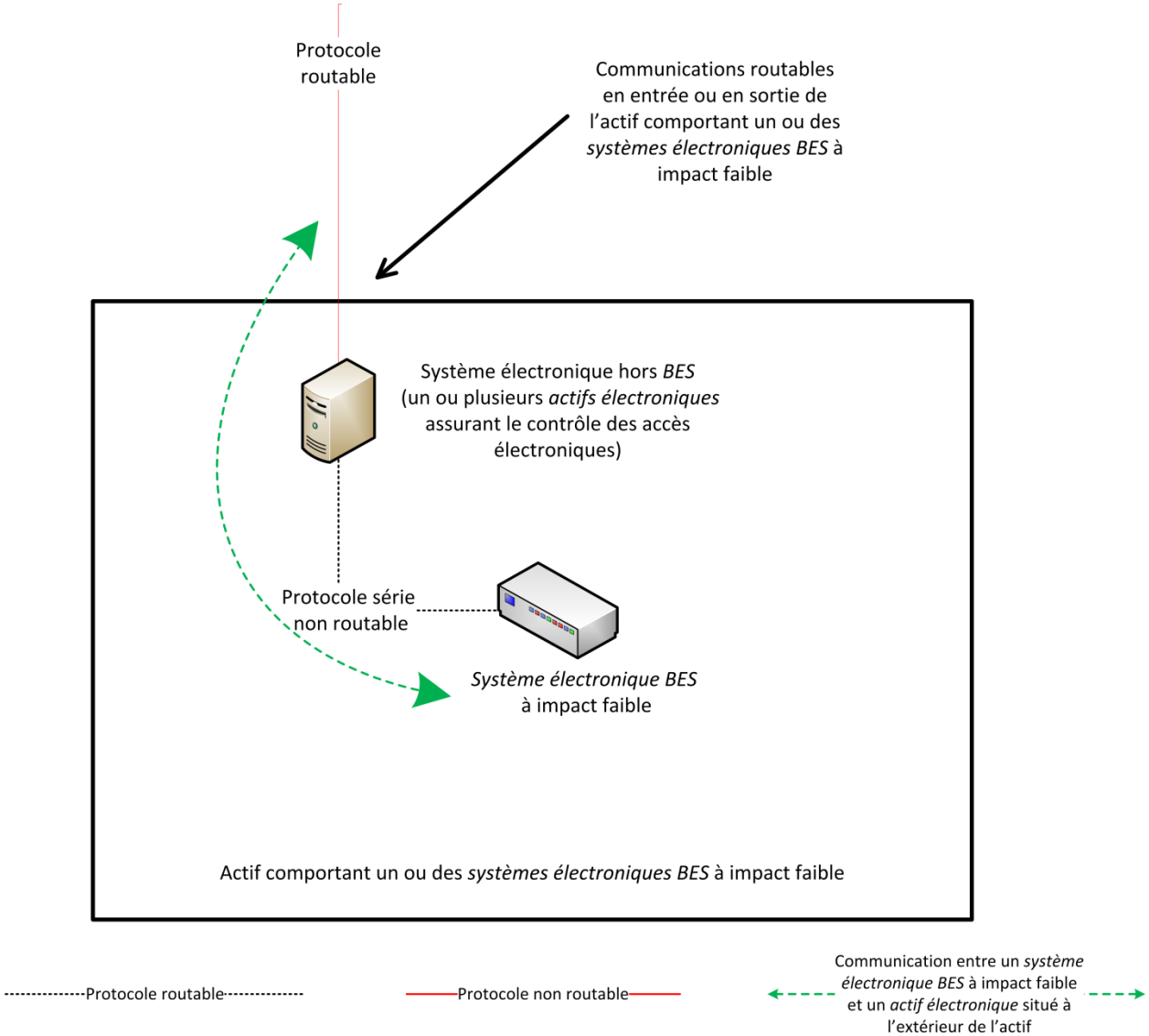
L'entité responsable peut choisir d'utiliser une passerelle unidirectionnelle pour le contrôle des accès électroniques. Le ou les *systèmes électroniques BES* à impact faible ne sont pas accessibles (les données ne peuvent pas les atteindre) au moyen de la communication par protocole routable en entrée de l'actif, car les données ne peuvent circuler que dans un seul sens. La passerelle unidirectionnelle est configurée pour autoriser uniquement les accès sortants nécessaires au moyen du protocole routable en sortie de l'actif.



Modèle de référence 4

Modèle de référence 5 – Authentification de l'utilisateur

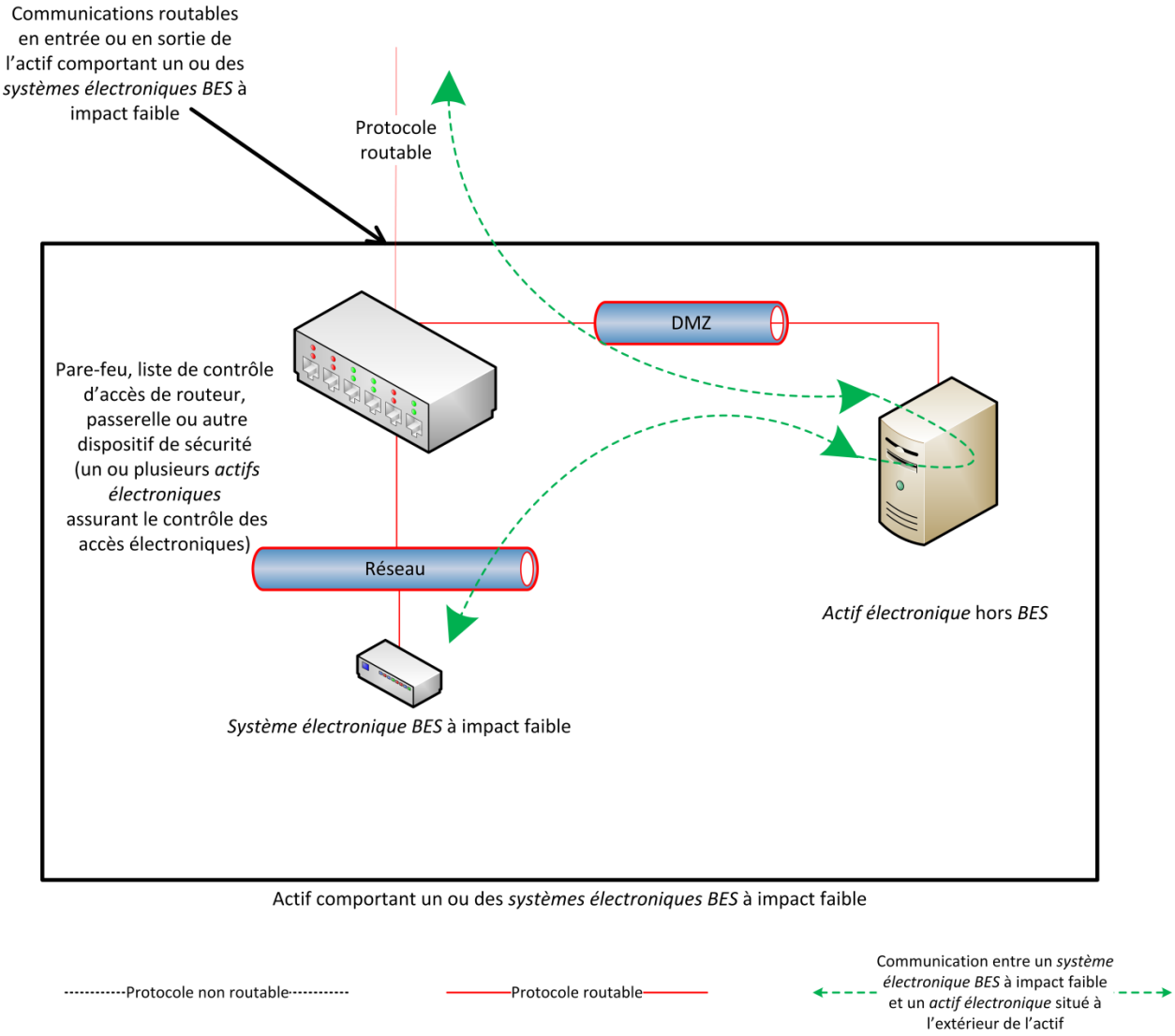
Ce modèle de référence illustre la latitude laissée à l'entité responsable dans le choix des moyens de contrôle des accès électroniques, pourvu que l'objectif de sécurité de l'exigence soit réalisé. L'entité responsable peut choisir d'utiliser un *actif électronique* hors *BES* situé dans l'actif comportant le *système électronique BES* à impact faible afin d'exiger une authentification pour toute communication à partir d'*actifs électroniques* situés à l'extérieur de l'actif. Le système électronique hors *BES* chargé de l'authentification permet uniquement à une communication authentifiée d'accéder aux *systèmes électroniques BES* à impact faible ; il réalise ainsi la première moitié de l'objectif de sécurité, en autorisant uniquement les accès électroniques entrants nécessaires. En outre, le système électronique hors *BES* chargé de l'authentification est configuré de façon à autoriser seulement les communications sortantes nécessaires, réalisant ainsi la deuxième moitié de l'objectif de sécurité. Souvent, dans cette architecture de réseau, l'accès sortant serait contrôlé par l'interdiction de toute communication à partir du *système électronique BES* à impact faible. Cette configuration peut être avantageuse si les seules communications prévues se font par accès interactif commandé par l'utilisateur.



Modèle de référence 5

Modèle de référence 6 – Accès indirect

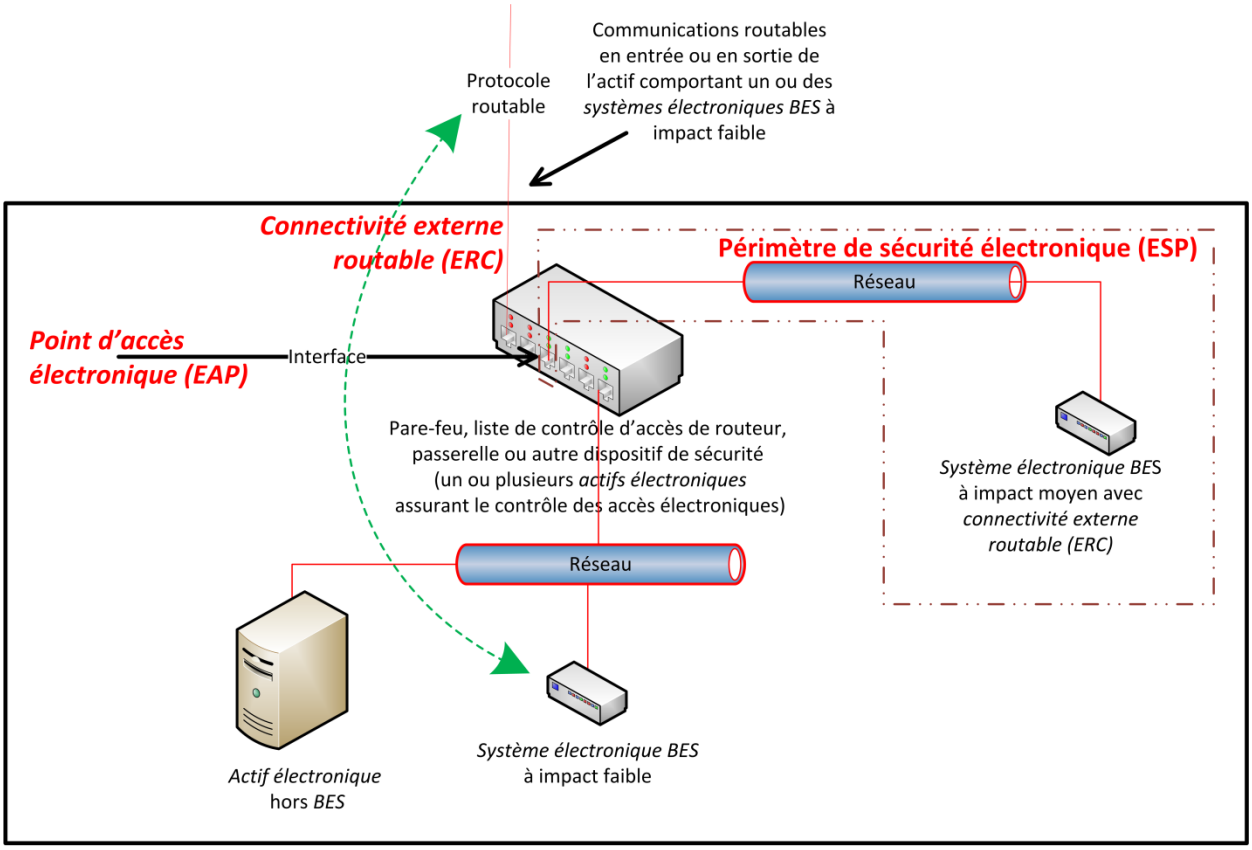
Dans la mise en place des mesures de contrôle des accès électroniques, l'entité responsable peut constater qu'il existe un accès indirect entre un *système électronique BES* à impact faible et un *actif électronique* situé à l'extérieur de l'actif comportant ce *système électronique BES* à impact faible, par l'intermédiaire d'un *actif électronique* hors *BES* situé à l'intérieur de l'actif en question. Cet accès indirect répond au critère d'une communication entre un *système électronique BES* à impact faible et un *actif électronique* situé à l'extérieur de l'actif comportant ce *système électronique BES* à impact faible. Dans ce modèle de référence, l'entité responsable devra mettre en place un contrôle des accès électroniques qui autorise uniquement les accès électroniques entrants et sortants nécessaires pour le *système électronique BES* à impact faible. Comme pour les autres modèles de référence présentés, l'accès électronique dans ce modèle de référence est contrôlé au moyen du dispositif de sécurité qui restreint les communications entrantes ou sortantes de l'actif.



Modèle de référence 6

Modèle de référence 7 – Contrôles des accès électroniques pour les actifs comportant des *systèmes électroniques BES* à impact faible et une *connectivité externe routable*

Ce modèle de référence présente non seulement un accès entrant et sortant par protocole routable entre l'actif comportant un ou des *systèmes électroniques BES* à impact faible et un ou des *actifs électroniques* situés à l'extérieur de l'actif en question, mais aussi une *connectivité externe routable* puisque l'actif accessible par protocole routable comporte au moins un *système électronique BES* à impact moyen et un *système électronique BES* à impact faible. L'entité responsable peut choisir d'utiliser une interface dans le *système de contrôle ou de surveillance des accès électroniques* (*EACMS*) à impact moyen afin d'assurer le contrôle des accès électroniques aux fins de la norme CIP-003. L'*EACMS* remplit donc plusieurs fonctions : celle d'*EACMS* à impact moyen et celle de contrôle des accès électroniques pour un actif comportant des *systèmes électroniques BES* à impact faible.

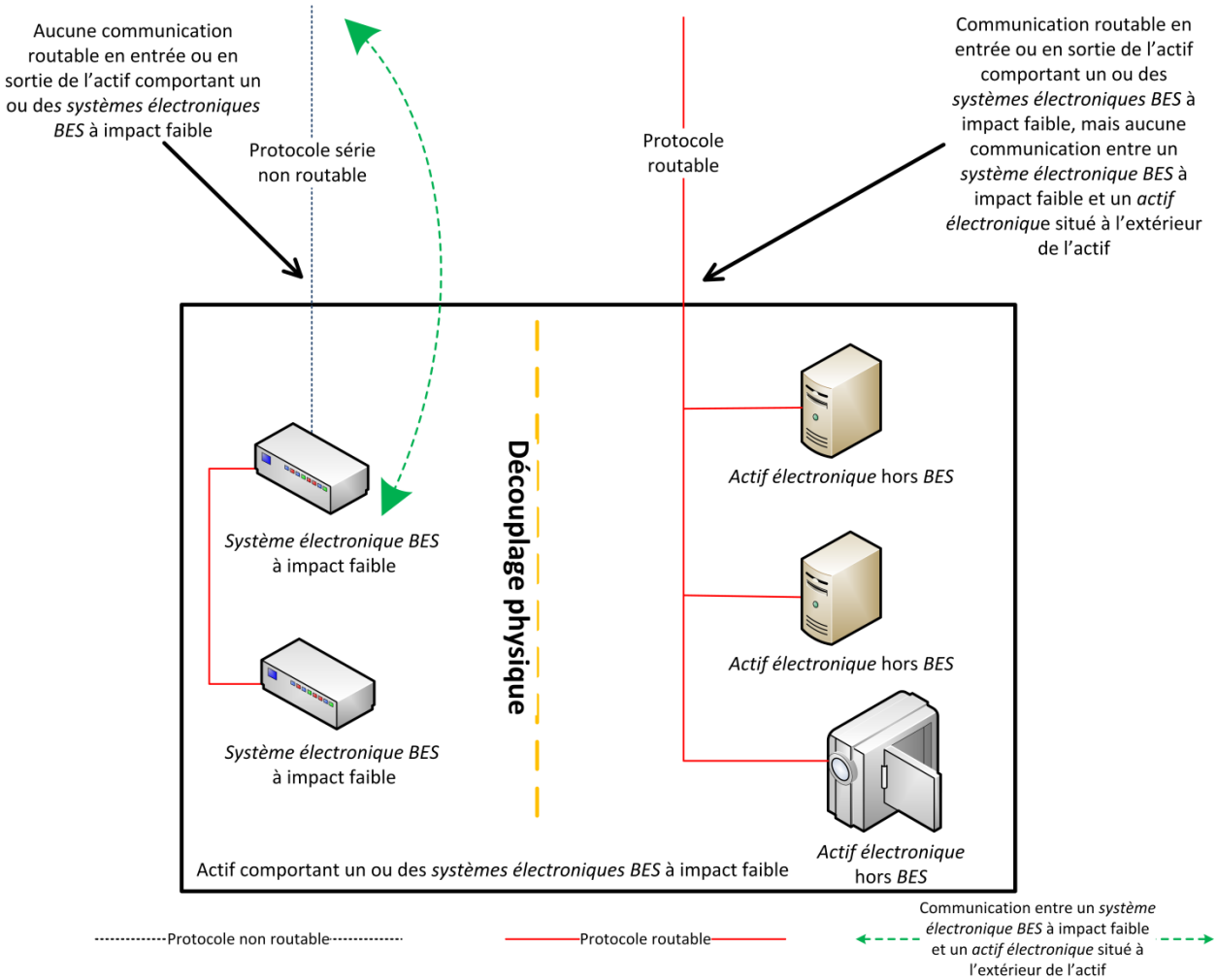


Modèle de référence 7

Modèle de référence 8 – Découplage physique et communication série non routable – Contrôle des accès électroniques non exigé

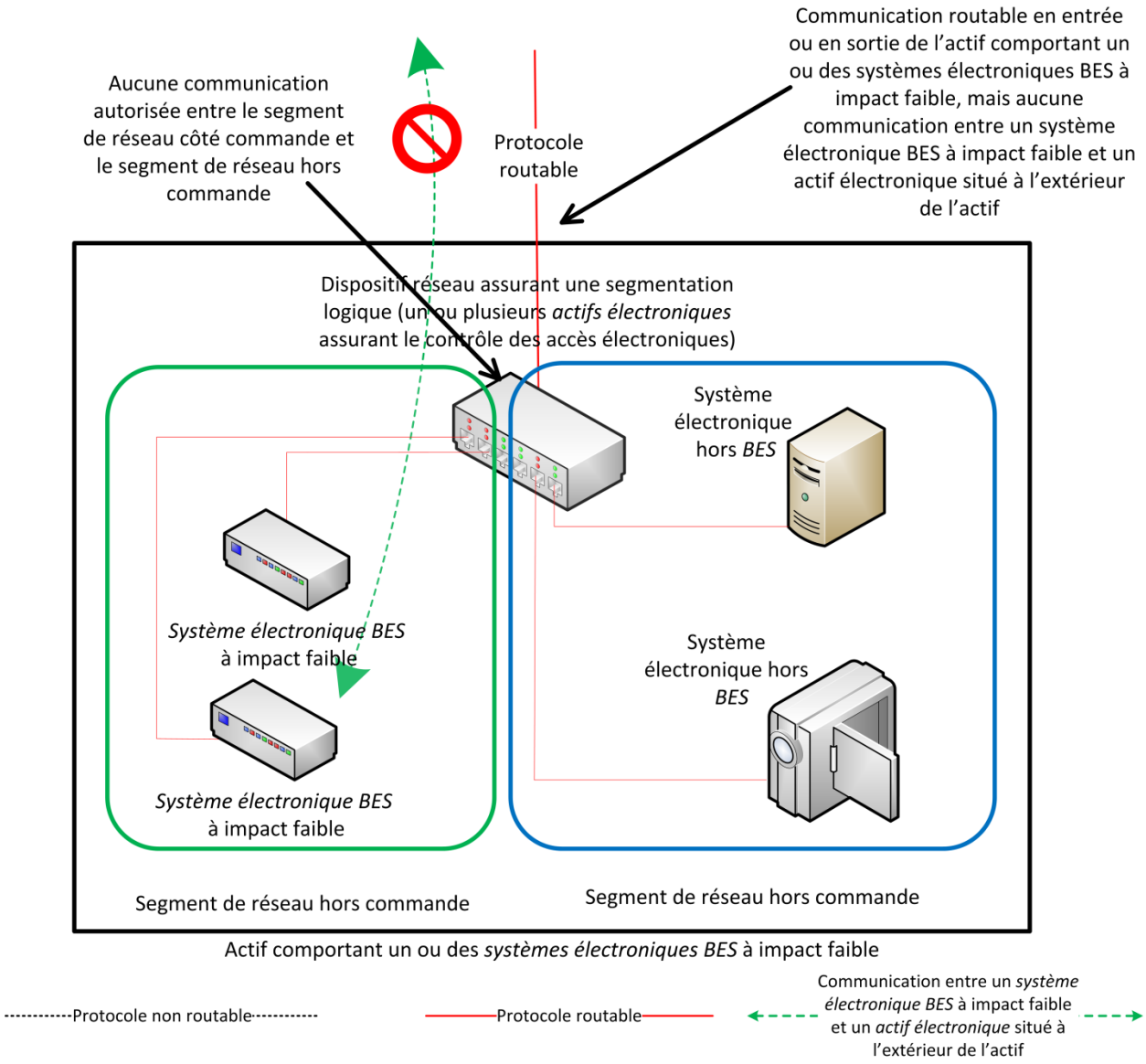
Dans ce modèle de référence, les critères de la section 3.1 de l'annexe 1 concernant l'obligation de contrôler les accès électroniques ne sont pas remplis. Ce modèle de référence illustre trois concepts :

1) Étant donné le découplage physique (communément appelé « *air gap* » en anglais) du ou des *systèmes électroniques BES* à impact faible par rapport aux communications entrantes ou sortantes par protocole routable de l'actif comportant le ou les *systèmes électroniques BES* à impact faible, le contrôle des accès électroniques n'est pas exigé.
2) Étant donné que la communication avec les *systèmes électroniques BES* à impact faible à partir d'un *actif électronique* situé à l'extérieur de l'actif comportant ces *systèmes électroniques BES* à impact faible utilise uniquement un protocole série non routable au point d'entrée ou de sortie de cette communication, le contrôle des accès électroniques n'est pas exigé.
3) Une communication par protocole routable entre les *systèmes électroniques BES* à impact faible et d'autres *actifs électroniques*, par exemple entre les premier et deuxième *systèmes électroniques BES* à impact faible de la figure, ne nécessite pas de contrôle des accès électroniques pourvu que les communications par protocole routable ne sortent jamais de l'actif comportant les *systèmes électroniques BES* à impact faible.



Modèle de référence 8

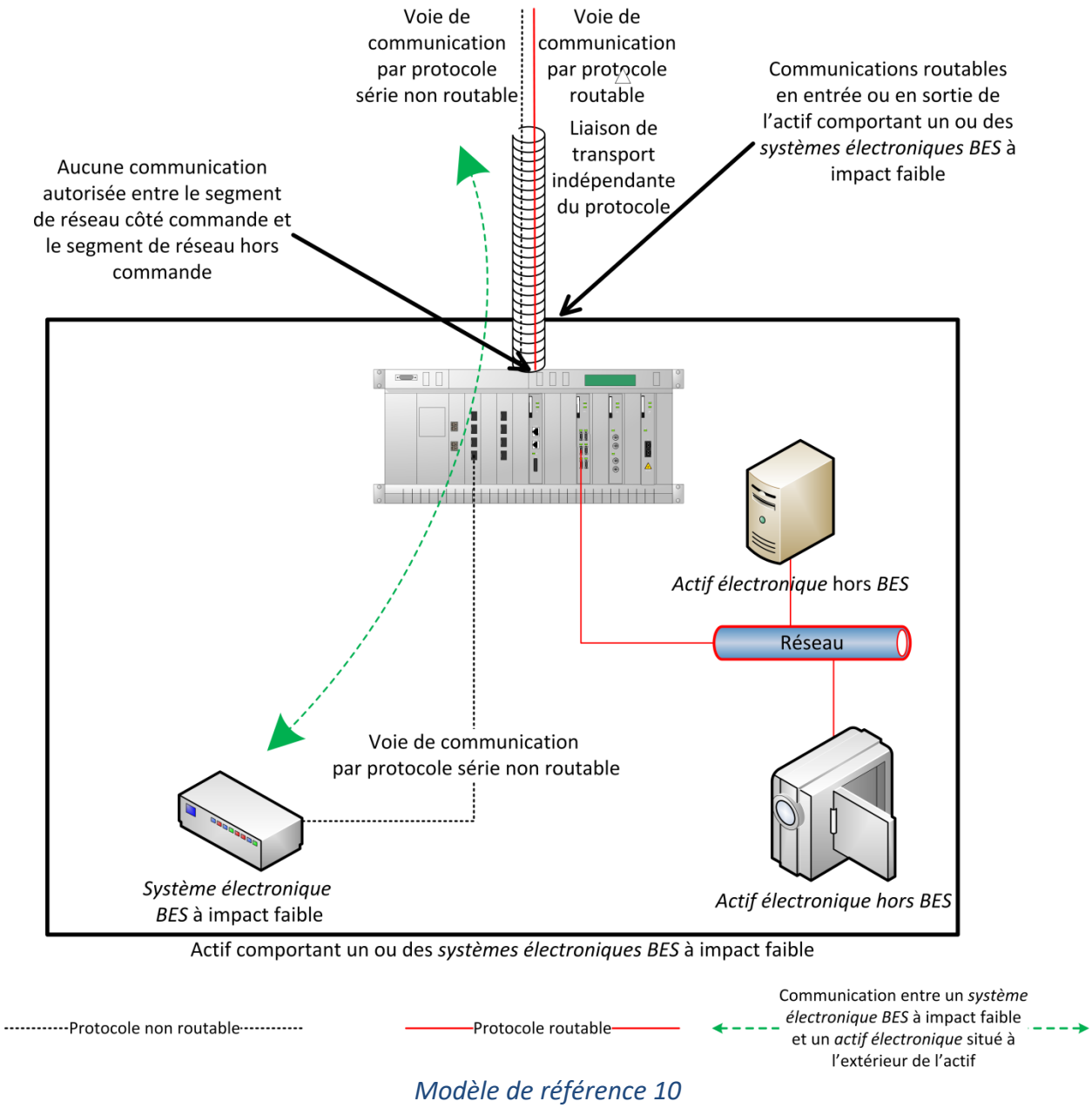
Modèle de référence 9 – Isolement logique – Contrôle des accès électroniques non exigé
Dans ce modèle de référence, les critères de la section 3.1 de l'annexe 1 concernant l'obligation de contrôler les accès électroniques ne sont pas remplis. L'entité responsable a isolé logiquement le ou les *systèmes électroniques BES* à impact faible par rapport aux communications entrantes ou sortantes par protocole routable de l'actif comportant le ou les *systèmes électroniques BES* à impact faible. La segmentation logique du réseau dans ce modèle de référence n'autorise aucune communication entre un *système électronique BES* à impact faible et un *actif électronique* situé à l'extérieur de l'actif. En outre, il n'existe aucun accès indirect parce que les *actifs électroniques* hors *BES* capables de communiquer avec l'extérieur de l'actif sont strictement empêchés de communiquer vers le ou les *systèmes électroniques BES* à impact faible. Le ou les *systèmes électroniques BES* à impact faible sont confinés dans un segment de réseau isolé par des contrôles électroniques qui empêchent toute communication entrante ou sortante par protocole routable avec l'extérieur de ce segment de réseau ; ainsi, les communications des *systèmes électroniques BES* à impact faible ne sortent jamais de l'actif au moyen d'un protocole routable.



Modèle de référence 9

Modèle de référence 10 – Communication série non routable empruntant une voie isolée dans un réseau de transport non routable – Contrôle des accès électroniques non exigé

Dans ce modèle de référence, les critères de la section 3.1 de l'annexe 1 concernant l'obligation de contrôler les accès électroniques ne sont pas remplis. Ce modèle de référence décrit une communication entre un *système électronique BES* à impact faible et un *actif électronique* situé à l'extérieur de l'actif comportant ce *système électronique BES* à impact faible. Cette communication utilise un protocole série non routable qui se trouve transporté dans un réseau étendu au moyen d'un mécanisme indépendant du protocole et capable de véhiculer des communications routables et non routables, par exemple un réseau à multiplexage temporel (TDM), un réseau optique synchrone (SONET) ou un réseau de commutation multiprotocole par étiquette (MPLS). Bien qu'il y ait par ailleurs une communication par protocole routable en entrée ou en sortie de l'actif comportant le *système électronique BES* à impact faible en plus de la communication entre le *système électronique BES* à impact faible et un *actif électronique* situé à l'extérieur de l'actif, la communication entre le *système électronique BES* à impact faible et l'*actif électronique* extérieur n'utilise pas une communication par protocole routable. Ce modèle présente une analogie avec le modèle de référence 9, en ce qu'il dépend d'un isolement logique pour empêcher toute communication entre un *système électronique BES* à impact faible et un *actif électronique* situé à l'extérieur de l'actif au moyen d'un protocole routable.



Modèle de référence 10

Connectivité par lien commuté

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.

Contrôles d'accès insuffisants

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 *système électronique BES* à impact faible 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 cas de cartes d'interface à double résidence ou multiréseaux sans désactivation du réacheminement IP dans l'*actif électronique* hors *BES* à l'intérieur de la zone DMZ afin d'assurer une coupure entre le ou les *systèmes électroniques BES* à impact faible et le réseau externe, l'exigence de « contrôle » des accès électroniques entrants et sortants ne serait pas respectée en supposant l'absence d'un autre pare-feu hôte ou d'autres dispositifs de sécurité pour cet *actif électronique* hors *BES*.

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 un ou 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.

Le ou 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 d'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 E2, section 5 de l'annexe 1 – Atténuation des risques liés à l'introduction de programmes malveillants à partir d'*actifs électroniques temporaires* ou de *supports de stockage amovibles*

La plupart des *actifs électroniques BES* et des *systèmes électroniques BES* sont isolés des réseaux externes publics ou non fiables ; en conséquence, les *actifs électroniques temporaires* et les *supports de stockage amovibles* constituent souvent le seul moyen d'entrée et de sortie des fichiers pour des zones sécurisées dans le cadre d'opérations de maintenance, de surveillance ou de dépannage de systèmes

névralgiques. Les *actifs électroniques temporaires* et les *supports de stockage amovibles* se présentent assurément comme un vecteur de cyberattaque. Afin de protéger les *actifs électroniques BES* et les *systèmes électroniques BES*, la section 5 de l'annexe 1 de la norme CIP-003, liée à l'exigence E2 de cette norme, demande aux entités responsables de documenter et de mettre en œuvre un plan qui leur permettra d'atténuer le risque lié à l'introduction de programmes malveillants dans les *systèmes électroniques BES* à impact faible à partir d'*actifs électroniques temporaires* ou de *supports de stockage amovibles*. L'élaboration de ce plan amène l'entité responsable à documenter des processus que son organisation est capable de mettre en œuvre et qui cadrent avec ses processus de gestion des changements.

Les *actifs électroniques temporaires* sont très variés ; ils vont des dispositifs conçus spécialement pour la maintenance d'équipements liés au *BES* à des appareils courants (ordinateurs portatifs ou de bureau, tablettes, etc.) qui peuvent simplement se connecter à des *systèmes électroniques BES* ou exécuter des applications afférentes à ceux-ci et qui sont capables de transmettre du code exécutable aux *actifs électroniques BES* ou aux *systèmes électroniques BES*. Remarque : Les *actifs électroniques* connectés à un *système électronique BES* pendant moins de 30 jours en raison d'un retrait prématuré (par exemple à cause d'une panne) ne sont pas considérés comme des *actifs électroniques temporaires*. Les *supports de stockage amovibles* visés par cette exigence comprennent notamment les disquettes, les cédéroms, les clés USB, les disques durs externes et autres cartes ou lecteurs à mémoire flash (non volatile).

Exemples non limitatifs de ces dispositifs connectés temporairement :

- équipements de diagnostic ;
- équipements de maintenance de *systèmes électroniques BES* ; ou
- équipement de configuration de *systèmes électroniques BES*.

Afin de réaliser l'objectif d'atténuer les risques associés à l'introduction de programmes malveillants dans les *systèmes électroniques BES* à impact faible, la section 5 spécifie les ressources et les moyens de sécurité auxquels peuvent avoir recours les entités responsables d'après le type d'un actif et son propriétaire.

À partir de la liste d'options présentée à l'annexe 1, l'entité responsable est libre de choisir le ou les moyens qui lui conviennent le mieux, y compris pour documenter comment et quand elle entend examiner l'*actif électronique temporaire* sous son contrôle ou placé sous le contrôle d'une autre entité. L'entité doit éviter de mettre en place des fonctions de sécurité susceptibles d'affaiblir la fiabilité du réseau en agissant d'une manière qui nuirait au fonctionnement ou au soutien de l'*actif électronique temporaire* ou de l'*actif électronique BES*.

Atténuation des risques liés à l'introduction de programmes malveillants

Des expressions comme « atténuer le risque » ou « atténuation du risque » sont utilisées à la section 5 de l'annexe 1 à l'endroit des risques présentés par les programmes malveillants au moment de connecter des *actifs électroniques temporaires* et des *supports de stockage amovibles* à des *systèmes électroniques BES*. L'exigence d'atténuation consiste à réduire les risques pour la sécurité associés à la connexion de l'*actif électronique temporaire* ou du *support de stockage amovible*. Lorsqu'elles déterminent les moyens d'atténuer le risque lié à l'introduction de programmes malveillants, les entités n'ont pas à effectuer et à documenter une évaluation formelle des risques associés à l'introduction de programmes malveillants.

Prise en compte des capacités de l'*actif électronique temporaire*

Comme dans d'autres normes CIP, les moyens à utiliser par l'entité se limitent à ceux que le système est capable de mettre en œuvre. L'expression « selon les capacités de l'*actif électronique temporaire* » sert à éviter le recours à une exception pour raison technique (TFE) lorsqu'il est évident que certains moyens ne sont pas utilisables avec tel ou tel dispositif. Par exemple, dans le cas des programmes malveillants, bien des types de dispositifs n'ont pas la capacité de faire fonctionner un logiciel antivirus ; par conséquent, la mise en œuvre d'un logiciel antivirus ne serait pas exigée pour ces dispositifs.

Exigence E2, section 5.1 de l'annexe 1 – *Actifs électroniques temporaires* gérés par l'entité responsable

Dans le cas des *actifs électroniques temporaires* et des *supports de stockage amovibles* qui sont connectés à des *systèmes électroniques BES* à impact faible ainsi qu'à des *systèmes électroniques BES* à impact moyen ou élevé, les entités doivent comprendre que les niveaux d'exigences sont différents, et gérer ces actifs selon le programme qui correspond au niveau d'impact le plus élevé.

Section 5.1 : Les entités doivent documenter et mettre en œuvre leurs plans visant à atténuer les risques liés à l'introduction de programmes malveillants au moyen d'une ou de plusieurs des mesures de protection énumérées, selon les capacités de l'*actif électronique temporaire*.

Quant à la méthode choisie pour atténuer le risque lié à l'introduction de programmes malveillants, l'entité est libre d'appliquer cette méthode soit en permanence, soit à la demande. Exemple d'application permanente : gérer la solution antivirus pour le dispositif dans le cadre d'une solution de sécurité des points terminaux avec des mises à jour régulières des signatures ou des séquences de code, des balayages de système programmés, etc. Par contre, dans le cas de dispositifs utilisés assez rarement et dont les signatures ou les séquences de code ne sont pas tenues à jour, l'entité peut gérer ces dispositifs à la demande seulement, en demandant une mise à jour des signatures ou des séquences de code et un balayage du dispositif avant sa connexion afin de vérifier qu'il est exempt de programme malveillant.

Le choix d'une gestion permanente ou à la demande n'implique pas l'obligation de vérifier le dispositif avant chacune de ses connexions. Par exemple, si un dispositif géré à la demande est utilisé successivement pour la maintenance de plusieurs *actifs électroniques BES*, l'entité responsable peut choisir de documenter la mise à jour du dispositif avant sa connexion à titre d'*actif électronique temporaire* pour la première opération de maintenance. Pour l'équipe de rédaction, il est exclu d'exiger une écriture de registre pour chaque connexion d'un *actif électronique temporaire* à un *actif électronique BES*.

Voici d'autres indications sur les différentes méthodes utilisables pour atténuer le risque lié à l'introduction de programmes malveillants.

- Les logiciels antivirus, avec mises à jour manuelles ou systématiques des signatures ou des séquences de code, offrent une certaine souplesse pour gérer les *actifs électroniques temporaires* en déployant des logiciels antivirus ou des outils de sécurité des points terminaux qui assurent une mise à jour programmée des signatures ou des séquences de code. Par ailleurs, pour les dispositifs dont la connexion non régulière ne leur permet pas de recevoir des mises à jour programmées, l'entité peut choisir de mettre à jour les signatures ou les séquences de code et de balayer l'*actif électronique temporaire* avant sa connexion afin de confirmer l'absence de programme malveillant.
- La liste blanche d'applications consiste à autoriser seulement les applications et les processus nécessaires pour l'*actif électronique temporaire*. Ce procédé réduit la possibilité que des

programmes malveillants puissent s'exécuter sur l'*actif électronique temporaire* et attaquer l'*actif électronique BES* ou le *système électronique BES*.

- Si elles utilisent des méthodes autres que celles énumérées, les entités doivent documenter comment ces méthodes réalisent l'objectif d'atténuer le risque lié à l'introduction de programmes malveillants.

Si un programme malveillant est découvert dans l'*actif électronique temporaire*, il faut le neutraliser avant toute connexion à un *système électronique BES* afin d'empêcher que le programme malveillant ne s'y introduise. L'entité responsable peut également décider de ne pas connecter l'*actif électronique temporaire* à un *système électronique BES* afin de prévenir un tel risque. Par ailleurs, l'entité doit aussi déterminer si la détection du programme malveillant constitue un *incident de cybersécurité*.

Exigence E2, section 5.2 de l'annexe 1 – *Actifs électroniques temporaires* gérés par une tierce partie autre que l'entité responsable

La section 5 reconnaît également que l'entité responsable n'a aucun contrôle direct sur les *actifs électroniques temporaires* qui sont gérés par une tierce partie. Cependant, même dans ce cas, l'entité responsable est tenue de s'assurer que des moyens ont été déployés pour atténuer le risque lié à l'introduction de programmes malveillants dans des *systèmes électroniques BES* à impact faible à partir d'*actifs électroniques temporaires* qui ne relèvent pas de sa gestion. La section 5 demande aux entités d'examiner les pratiques de sécurité des tierces parties relativement aux *actifs électroniques temporaires* afin de réaliser l'objectif de l'exigence. La mention « avant de connecter l'*actif électronique temporaire* » vise à obliger l'entité responsable à effectuer l'examen avant la première connexion de l'*actif électronique temporaire* afin de réaliser l'objectif d'atténuer le risque lié à l'introduction de programmes malveillants. L'équipe de rédaction ne souhaite pas obliger l'entité responsable à effectuer un examen pour chaque connexion d'un *actif électronique temporaire* si l'entité responsable a déjà établi que cet *actif électronique temporaire* est conforme à l'objectif de sécurité. Il est exclu d'exiger une écriture de registre pour chaque connexion d'un *actif électronique temporaire* à un *actif électronique BES*.

Afin d'assurer un contrôle adéquat, les entités responsables peuvent conclure des ententes avec des tierces parties pour la prestation de services de soutien des *systèmes électroniques BES* et des *actifs électroniques BES* avec lesquels des *actifs électroniques temporaires* peuvent être utilisés. Les entités pourront juger avantageux d'adopter les clauses normalisées du département de l'Énergie des États-Unis pour les contrats de cybersécurité dans le domaine de la fourniture d'énergie (*Cybersecurity Procurement Language for Energy Delivery Systems*, avril 2014[1]). Ces clauses d'approvisionnement peuvent aider à harmoniser les actions de l'entité responsable et des tierces parties chargées du soutien des *systèmes électroniques BES* et des *actifs électroniques BES*. Les attributs du programme de protection des infrastructures essentielles (CIP), y compris les rôles et responsabilités, les contrôles d'accès, la surveillance, la journalisation, la gestion des vulnérabilités et celle des correctifs logiciels ainsi que les interventions en cas d'incident et la récupération des sauvegardes, peuvent faire partie des prestations confiées à une tierce partie. Les entités pourront s'inspirer des chapitres *General Cybersecurity Procurement Language* et *The Supplier's Life Cycle Security Program* du document précité pour la rédaction des ententes-cadres de services, des contrats et des processus et contrôles du programme CIP.

1. http://www.energy.gov/oe/downloads/cybersecurity-procurement-language-energy-delivery-april-2014

Section 5.2.1 : Les entités doivent documenter et mettre en œuvre leurs processus d'atténuation du risque lié à l'introduction des programmes malveillants, comportant une ou plusieurs des mesures d'atténuation indiquées ci-après.

- Procéder à un examen des niveaux de tenue à jour des logiciels antivirus ainsi que des signatures ou des séquences de code afin de s'assurer que ces niveaux permettent à l'entité responsable d'atténuer adéquatement le risque lié à l'introduction de programmes malveillants dans un système visé.
- Procéder à un examen des processus antivirus ou de sécurisation des points terminaux de la tierce partie afin de s'assurer que ces processus permettent à l'entité responsable d'atténuer adéquatement le risque lié à l'introduction de programmes malveillants dans un système visé.
- Procéder à un examen de l'utilisation par la tierce partie de listes blanches d'applications pour atténuer le risque lié à l'introduction de programmes malveillants dans un système visé.
- Procéder à un examen de l'utilisation de systèmes d'exploitation ou de logiciels exécutables uniquement à partir de supports non inscriptibles afin de s'assurer que les supports eux-mêmes sont exempts de tout programme malveillant. Les entités doivent examiner les processus de préparation des supports non inscriptibles ainsi que les supports eux-mêmes.
- Procéder à un examen des pratiques adoptées par la tierce partie pour le renforcement du système d'exploitation afin de s'assurer que les ports, services, applications et autres éléments inutiles ont été désactivés ou retirés. Cette mesure vise à réduire la surface d'attaque de l'*actif électronique temporaire* et à limiter les voies d'introduction de programmes malveillants.

Section 5.2.2 : Cette section vise à faire en sorte que si, lors de l'examen prescrit à la section 5.2.1, des lacunes sont constatées, les mesures d'atténuation des risques liés à des programmes malveillants pour les *systèmes électroniques BES* à impact faible soient effectivement mises en œuvre avant la connexion du ou des actifs à un système visé.

Exigence E2, section 5.3 de l'annexe 1 – *Supports de stockage amovibles*

Les entités ont un degré de contrôle élevé sur les *supports de stockage amovibles* destinés à être connectés à leurs *actifs électroniques BES*.

Section 5.3 : Les entités doivent documenter et mettre en œuvre leurs processus d'atténuation du risque lié à l'introduction de programmes malveillants, comportant un ou plusieurs moyens de détecter tout programme malveillant sur les *supports de stockage amovibles* avant leur connexion à un *actif électronique BES*. La détection de programmes malveillants doit normalement se faire à partir d'un système qui ne fait pas partie d'un *système électronique BES*, afin d'atténuer le risque lié à la propagation de programmes malveillants dans le réseau des *systèmes électroniques BES* ou dans un des *actifs électroniques BES*. Si un programme malveillant est détecté, il faut le supprimer ou le neutraliser afin qu'il ne puisse pas être introduit dans un *actif électronique BES* ou un *système électronique BES*. L'entité doit aussi déterminer si la détection du programme malveillant constitue un *incident de cybersécurité*. La fréquence et le choix du moment d'utilisation des moyens de détection des programmes malveillants ont été intentionnellement exclus de l'exigence, car il existe de multiples scénarios temporels possibles pour un plan d'atténuation du risque lié à l'introduction de programmes malveillants. L'équipe de rédaction ne souhaite pas obliger l'entité responsable à effectuer un examen pour chaque connexion d'un *actif électronique temporaire*, mais plutôt à mettre en œuvre son ou ses plans d'une façon qui protège tous les *systèmes électroniques BES* avec lesquels un *support de stockage*

amovible pourrait être utilisé. Il est exclu d'exiger une écriture de registre pour chaque connexion d'un *actif électronique temporaire* à un *actif électronique BES*.

Pour la détection des programmes malveillants, les entités peuvent choisir d'utiliser des *supports de stockage amovibles* auxquels sont intégrés des outils de détection de programmes malveillants. Dans ce cas, les outils de détection intégrés au *support de stockage amovible* doivent quand même être utilisés en combinaison avec un *actif électronique*. La section 5.3.1 précise que l'*actif électronique* utilisé pour la détection de programmes malveillants doit être situé à l'extérieur du *système électronique BES*.

Exigence E3

L'esprit de l'exigence E3 de la norme CIP-003-8 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 ainsi que la gouvernance générale du programme.

Exigence E4

Comme l'indique la justification de l'exigence E4 de la norme CIP-003-8, 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 un ou des *systèmes électroniques BES* à impact faible. Les plans de cybersécurité couvrent cinq thèmes : 1) la sensibilisation à la cybersécurité ; 2) les mesures de sécurité physique ; 3) le contrôle des accès électroniques ; 4) l'intervention en cas d'*incident de cybersécurité* ; et 5) l'atténuation des risques liés à l'introduction de programmes malveillants à partir d'*actifs électroniques temporaires* ou de *supports de stockage amovibles*. Ces plans, combinés aux politiques de cybersécurité spécifiées à l'alinéa 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 des modifications aux sections 2 et 3 de l'annexe 1 (exigence E2) :

L'exigence E2 demande aux entités d'élaborer et de mettre en œuvre un ou des plans de cybersécurité afin de réaliser des objectifs de sécurité précis pour leurs actifs comportant un ou des *systèmes électroniques BES* à impact faible. Au paragraphe 73 de son ordonnance 822, la FERC demande à la NERC de modifier « la définition du terme *connectivité externe routable à impact faible* en fonction du commentaire de la section Principes directeurs et fondements techniques de la norme CIP-003-6… afin

d'apporter un éclaircissement souhaitable à cette définition et d'éliminer l'ambiguïté du mot "direct" utilisé dans la définition proposée… dans les douze mois suivant l'entrée en vigueur de cette décision finale ».

Les révisions de la section 3 de l'annexe 1 reprennent des portions de la définition du terme *connectivité externe routable à impact faible* (*LERC*) et mettent l'accent sur l'exigence de contrôle des accès électroniques pour les actifs comportant un ou des *systèmes électroniques BES* à impact faible. Ce changement oblige l'entité responsable à autoriser uniquement les accès électroniques entrants et sortants jugés nécessaires s'il existe une communication par protocole routable, en entrée ou en sortie d'un actif, entre un ou des *systèmes électroniques BES* à impact faible de cet actif et un ou des *actifs électroniques* situés à l'extérieur de cet actif. Si une telle communication est présente, l'entité responsable doit mettre en place un contrôle des accès électroniques, sauf si la communication répond à l'exemption suivante du sous-alinéa iii), qui faisait partie de la définition du terme *LERC* : « ne servant pas à des fonctions de commande ou de protection à délai critique entre des dispositifs électroniques intelligents (par exemple, des communications utilisant le protocole R-GOOSE de la norme CEI TR-61850-90-5) ».

Les changements apportés à la section 2 de l'annexe 1 sont liés à ceux de la section 3 ; il est maintenant demandé à l'entité responsable de contrôler l'accès physique « à tout *actif électronique* qu'elle décide d'affecter, conformément à la section 3.1, au contrôle des accès électroniques ». L'accent mis sur le contrôle des accès électroniques plutôt que sur les points d'accès électronique de *système électronique BES* à impact faible élimine le besoin de ceux-ci.

En raison de ces changements aux sections 2 et 3, les termes connectivité externe routable à impact faible (LERC) et point d'accès électronique de *système électronique BES* à impact faible (LEAP) seront retirés du glossaire de la NERC.

Justification de la section 5 de l'annexe 1 (exigence E2) :

L'exigence E2 demande aux entités d'élaborer et de mettre en œuvre un ou des plans de cybersécurité afin de réaliser des objectifs de sécurité précis pour leurs actifs comportant un ou des *systèmes électroniques BES* à impact faible. Au paragraphe 32 de son ordonnance 822, la FERC demande à la NERC de « …rendre obligatoires des mesures de protection visant les actifs temporaires utilisés avec les *systèmes électroniques BES* à impact faible, d'après le risque pour la fiabilité du *système de production-transport d'électricité* ». Les actifs temporaires sont des vecteurs potentiels d'introduction de programmes malveillants dans les *systèmes électroniques BES* à impact faible. La section 5 de l'annexe 1 vise à combattre le risque de contamination du *BES* par des maliciels propagés par l'entremise de *systèmes électroniques BES* à impact faible, en demandant aux entités d'élaborer et de mettre en œuvre un ou des plans à cette fin. Ces plans de cybersécurité, combinés aux politiques de cybersécurité spécifiées à l'alinéa 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.

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 permanent 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 l'équipe de rédaction 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.

A. Introduction

1. **Titre :** Cybersécurité – Périmètres de sécurité électronique

2. **Numéro :** CIP-005-6

3. **Objet :** Gérer l'accès électronique aux *systèmes électroniques BES* en établissant un *périmètre de sécurité électronique* (*ESP*) contrôlé afin de protéger les *systèmes électroniques BES* contre les compromissions qui pourraient entraîner un fonctionnement incorrect ou une instabilité dans le *BES*.

4. **Applicabilité :**

   4.1. Entités fonctionnelles : Dans le contexte de la présente norme, les entités fonctionnelles indiquées ci-après sont appelées collectivement « entités responsables ». Si certaines exigences visent plus spécifiquement une entité fonctionnelle ou un sous-ensemble 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 systèmes, *installations* et équipements suivants pour la protection ou la remise en charge du *BES* :

   4.1.2.1. Système de délestage de *charge* en sous-fréquence (DSF) ou 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 des délestages automatiques de *charge* de 300 MW ou plus sous la commande d'un système commun détenu par l'entité responsable, sans intervention humaine.

   4.1.2.2. *Automatisme de réseau* (*RAS*) visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou de l'*entité régionale*.

   4.1.2.3. *Système de protection* de réseau de *transport* (à l'exclusion des systèmes de DSF et de DST) visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou de l'*entité régionale*.

   4.1.2.4. *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 de la présente norme, les systèmes, *installations* et équipements suivants détenus par une entité responsable indiquée à la section 4.1 sont visés par les exigences. Si certaines exigences visent plus spécifiquement un type ou un sous-ensemble de systèmes, d'*installations* ou d'équipements, ceux-ci sont précisés explicitement.

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

4.2.1.1. 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 des délestages de *charge* automatiques de 300 MW ou plus sous la commande d'un système commun détenu par l'entité responsable, sans intervention humaine.

4.2.1.2. *Automatisme de réseau* (*RAS*) visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou de l'*entité régionale*.

4.2.1.3. *Système de protection* de réseau de *transport* (à l'exclusion des systèmes de DSF et de DST) visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou de l'*entité régionale*.

4.2.1.4. *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-005-6 :

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 électronique* distincts.

4.2.3.3. Les systèmes, structures et composantes régis par la U.S. Nuclear Regulatory Commission en vertu d'un plan de cybersécurité conforme 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 ont déterminé n'avoir aucun *système électronique BES* classé dans les catégories « impact élevé » ou « impact moyen » selon le processus d'inventaire et de catégorisation prescrit dans la norme CIP-002-5.

5. Date d'entrée en vigueur :

Voir le plan de mise en œuvre du projet 2016-03.

6. Contexte :

La norme CIP-005 fait partie d'une série de normes CIP sur la cybersécurité qui exigent l'inventaire et la catégorisation initiales des *systèmes électroniques BES*, ainsi qu'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 le 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 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 de DSF et de DST. Ce seuil particulier de 300 MW pour les systèmes de DSF et de DST provient de la version 1 des normes CIP sur la cybersécurité. Le seuil demeure à 300 MW puisqu'il concerne spécifiquement les systèmes de DST et de DSF, qui constituent des efforts de dernier

recours pour sauver le *système de production-transport d'électricité*. Un examen des tolérances des systèmes de 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 de 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. L'équipe de rédaction (SDT) CSO706 a adapté ce concept à partir du cadre de gestion des risques du National Institute of Standards and Technology (NIST) en vue d'établir une méthode d'application des exigences qui tient compte plus adéquatement de l'impact et des caractéristiques de connectivité. La colonne « Systèmes visés » repose sur les conventions suivantes :

- ***Systèmes électroniques BES* à impact élevé** – Désigne les *systèmes électroniques BES* classés dans la catégorie « impact élevé », selon les processus d'inventaire et de catégorisation de la norme CIP-002.
- ***Systèmes électroniques BES* à impact élevé à *connectivité par lien commuté*** – Désigne uniquement les *systèmes électroniques BES* à impact élevé à *connectivité par lien commuté*.
- ***Systèmes électroniques BES* à impact élevé à *connectivité externe routable* –** Désigne uniquement les *systèmes électroniques BES* à impact élevé à *connectivité externe routable*. Exclut les *actifs électroniques* des systèmes électroniques BES auxquels on ne peut avoir accès directement par *connectivité externe routable*.
- ***Systèmes électroniques BES* à impact moyen** – Désigne les *systèmes électroniques BES* classés dans la catégorie « impact moyen », selon les processus d'inventaire et de catégorisation de la norme CIP-002.
- ***Systèmes électroniques BES* à impact moyen situés aux *centres de contrôle*** – Désigne uniquement les *systèmes électroniques BES* à impact moyen situés dans un *centre de contrôle*.
- ***Systèmes électroniques BES* à impact moyen à *connectivité par lien commuté*** – Désigne uniquement les *systèmes électroniques BES* à impact moyen à *connectivité par lien commuté*.
- ***Systèmes électroniques BES* à impact moyen à *connectivité externe routable*** – Désigne uniquement les *systèmes électroniques BES* à impact moyen à *connectivité externe routable*. Exclut les *actifs électroniques* des *systèmes électroniques BES* auxquels on ne peut avoir accès directement par *connectivité externe routable*.
- ***Actifs électroniques protégés* (*PCA*)** – Désigne tout *actif électronique protégé* associé à un *système électronique BES* à impact élevé ou moyen visé.
- ***Points d'accès électronique* (*EAP*)** – Désigne les *points d'accès électronique* associés à un *système électronique BES* à impact élevé ou moyen visé.

B. Exigences et mesures

E1. Chaque entité responsable doit mettre en œuvre un ou plusieurs processus documentés qui, collectivement, couvrent tous les alinéas applicables du tableau E1 (CIP-005-6) – *Périmètre de sécurité électronique*. *[Facteur de risque de non-conformité : moyen] [Horizon : planification de l'exploitation et exploitation le même jour]*

M1. Les pièces justificatives doivent comprendre chacun des processus documentés applicables qui, collectivement, couvrent tous les alinéas applicables du tableau E1 (CIP-005-6) – *Périmètre de sécurité électronique*, ainsi que des pièces justificatives additionnelles attestant la mise en œuvre, selon la colonne Mesures du tableau.

Tableau E1 (CIP-005-6) – Périmètre de sécurité électronique			
Alinéa	**Systèmes visés**	**Exigences**	**Mesures**
1.1	*Systèmes électroniques BES* à impact élevé et : • les *PCA* associés. *Systèmes électroniques BES* à impact moyen et : • les *PCA* associés.	Tous les *actifs électroniques* visés qui sont reliés à un réseau au moyen d'un protocole routable doivent être situés à l'intérieur d'un *ESP* défini.	Exemple non limitatif de pièce justificative : liste de tous les *ESP* avec tous les *actifs électroniques* visés à identifiant unique qui sont reliés au moyen d'un protocole routable dans chaque *ESP*.
1.2	*Systèmes électroniques BES* à impact élevé à *connectivité externe routable* et : • les *PCA* associés. *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et : • les *PCA* associés.	Toute *connectivité externe routable* doit s'effectuer par l'intermédiaire d'un *point d'accès électronique* (*EAP*) identifié.	Exemples non limitatifs de pièces justificatives : schémas de réseau montrant tous les chemins de communication routables externes et les *EAP* identifiés.

Tableau E1 (CIP-005-6) – Périmètre de sécurité électronique			
Alinéa	**Systèmes visés**	**Exigences**	**Mesures**
1.3	*Points d'accès électronique* associés à des *systèmes électroniques BES* à impact élevé. *Points d'accès électronique* associés à des *systèmes électroniques BES* à impact moyen.	Exiger des autorisations pour les accès entrants et sortants, y compris la raison pour donner l'accès, et refuser tout autre accès par défaut.	Exemple non limitatif de pièce justificative : liste de règles (coupe-feu, liste des droits d'accès, etc.) démontrant que seuls les accès autorisés sont permis et que chaque règle d'accès est justifiée, documentation à l'appui.
1.4	*Systèmes électroniques BES* à impact élevé à *connectivité par lien commuté* et : • les *PCA* associés. *Systèmes électroniques BES* à impact moyen à *connectivité par lien commuté* et : • les *PCA* associés.	Lorsque techniquement faisable, effectuer l'authentification lors de l'établissement de la *connectivité par lien commuté* avec les *actifs électroniques* visés.	Exemple non limitatif de pièce justificative : processus documenté décrivant la méthode utilisée par l'entité responsable afin d'assurer l'authentification des accès effectués pour chaque connexion par lien commuté.
1.5	*Points d'accès électronique* associés à des *systèmes électroniques BES* à impact élevé. *Points d'accès électronique* associés à des *systèmes électroniques BES* à impact moyen situés dans des *centres de contrôle*.	Avoir un ou plusieurs moyens de détection des communications entrantes et sortantes malveillantes avérées ou présumées.	Exemple non limitatif de pièce justificative : documentation attestant la mise en œuvre de moyens de détection des communications malveillantes (système de détection des intrusions, pare-feu au niveau de la couche application, etc.).

E2. Chaque entité responsable qui autorise un *accès distant interactif* à des *systèmes électroniques BES* doit mettre en œuvre un ou plusieurs processus documentés qui, collectivement, et lorsque c'est techniquement faisable, couvrent tous les alinéas applicables du tableau E2 (CIP-005-6) – Gestion des *accès distants interactifs*. *[Facteur de risque de non-conformité : moyen] [Horizon : planification de l'exploitation et exploitation le même jour]*

M2. Les pièces justificatives doivent comprendre les processus documentés qui, collectivement, traitent de chacun des alinéas applicables du tableau E2 (CIP-005-6) – Gestion des *accès distants interactifs*, ainsi que des pièces justificatives additionnelles attestant la mise en œuvre, selon la colonne Mesures du tableau.

Tableau E2 (CIP-005-6) – Gestion des *accès distants interactifs*			
Alinéa	**Systèmes visés**	**Exigences**	**Mesures**
2.1	*Systèmes électroniques BES* à impact élevé et : • les *PCA* associés. *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et : • les *PCA* associés.	Pour tous les *accès distant interactifs*, utiliser un *système intermédiaire* de façon que l'*actif électronique* qui commande l'*accès distant interactif* n'ait pas directement accès à l'*actif électronique* visé.	Exemples non limitatifs de pièces justificatives : schémas de réseau ou documents sur l'architecture.
2.2	*Systèmes électroniques BES* à impact élevé et : • les *PCA* associés. *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et : • les *PCA* associés.	Pour toutes les sessions d'*accès distant interactif*, utiliser un cryptage se terminant à un *système intermédiaire*.	Exemple non limitatif de pièce justificative : documents sur l'architecture qui indiquent les points où commence et où se termine le cryptage.

Tableau E2 (CIP-005-6) – Gestion des *accès distants interactifs*			
Alinéa	**Systèmes visés**	**Exigences**	**Mesures**
2.3	*Systèmes électroniques BES* à impact élevé et : • les *PCA* associés. *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et leurs : • les *PCA* associés.	Exiger l'authentification multifactorielle pour toutes les sessions d'*accès distant interactif*.	Exemple non limitatif de pièce justificative : documents sur l'architecture décrivant les facteurs d'authentification utilisés. Exemples non limitatifs de facteurs d'authentification : • ce que l'utilisateur sait, comme un mot de passe ou un NIP. Ceci n'inclut pas les identifiants d'utilisateur ; • ce que l'utilisateur possède, comme un jeton, un certificat numérique ou une carte intelligente ; ou • une caractéristique biométrique de l'utilisateur, comme ses empreintes digitales ou le motif de son iris.
2.4	*Systèmes électroniques BES* à impact élevé et : • les *PCA* associés. *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et : • les *PCA* associés.	Disposer d'une ou de plusieurs méthodes permettant de déterminer les sessions actives d'accès distant par des fournisseurs (y compris les *accès distants interactifs* et les accès distants de système à système).	Exemples non limitatifs de pièces justificatives : documentation des méthodes utilisées pour déterminer les sessions actives d'accès distant par des fournisseurs (y compris les *accès distants interactifs* et les accès distants de système à système), par exemple : • méthodes d'accès aux informations journalisées ou de surveillance pour déterminer les

Tableau E2 (CIP-005-6) – Gestion des *accès distants interactifs*			
Alinéa	**Systèmes visés**	**Exigences**	**Mesures**
			sessions actives d'accès distant par des fournisseurs ; • méthodes de surveillance de l'activité (par exemple, tableaux des connexions ou compteurs de règles dans un pare-feu, ou surveillance de l'activité des utilisateurs) ou des ports ouverts (par exemple, commandes netstat ou connexes pour afficher les ports en activité) permettant de déterminer les sessions actives d'accès distant de système à système ; ou • méthodes de contrôle des accès distants commandés par les fournisseurs, par exemple l'exigence que ceux-ci téléphonent pour demander un deuxième facteur d'identification afin d'établir un accès distant.

Tableau E2 (CIP-005-6) – Gestion des *accès distants interactifs*			
Alinéa	**Systèmes visés**	**Exigences**	**Mesures**
2.5	*Systèmes électroniques BES* à impact élevé et : • les *PCA* associés. *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et leurs : • les *PCA* associés.	Disposer d'une ou de plusieurs méthodes permettant de désactiver les accès distants actifs des fournisseurs (y compris les *accès distants interactifs* et les accès distants de système à système).	Exemples non limitatifs de pièces justificatives : documentation des méthodes utilisées pour désactiver les accès distants actifs des fournisseurs (y compris les *accès distants interactifs* et les accès distants de système à système), par exemple : • méthodes permettant de désactiver l'accès distant des fournisseurs au *point d'accès électronique* applicable dans le cas d'un accès distant de système à système ; ou • méthodes permettant de désactiver l'*accès distant interactif* des fournisseurs au *système intermédiaire* applicable l'*accès distant interactif* par des fournisseurs.

C. Conformité

1. Processus de surveillance de la conformité

1.1. Responsable des mesures pour assurer la conformité

Le terme « *responsable des mesures pour assurer la conformité* » (*CEA*) désigne la NERC ou l'*entité régionale*, ou toute entité désignée par un organisme gouvernemental pertinent, dans leurs rôles respectifs visant à surveiller et à assurer la conformité avec les normes de fiabilité obligatoires et exécutoires 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 pour montrer qu'elle était conforme pendant la période complète écoulée depuis le dernier audit.

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

- Chaque entité visée doit conserver des pièces justificatives pour chaque exigence de la présente norme pendant trois années civiles.
- Si une entité visée 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. Programme de surveillance de la conformité et d'application des normes

Selon la définition des règles de procédure de la NERC, l'expression « programme de surveillance de la conformité et d'application des normes » désigne la liste des processus qui serviront à évaluer les données ou l'information afin de déterminer les résultats de conformité avec la norme de fiabilité.

Niveau de gravité de la non-conformité (VSL)

Ex.	Niveau de gravité de la non-conformité			
	VSL faible	VSL modéré	VSL élevé	VSL critique
E1.			L'entité responsable n'avait pas un moyen de détection des communications entrantes et sortantes malveillantes. (1.5)	L'entité responsable n'avait pas documenté un ou plusieurs processus pour le tableau E1 (CIP-005-6) – *Périmètre de sécurité électronique*. (R1) OU L'entité responsable n'avait pas tous les *actifs électroniques* visés qui sont reliés à un réseau au moyen d'un protocole routable à l'intérieur d'un *périmètre de sécurité électronique* (*ESP*) défini. (1.1) OU La *connectivité externe routable* à travers l'*ESP* n'était pas effectuée par l'intermédiaire d'un *EAP* identifié. (1.2) OU L'entité responsable n'a pas exigé d'autorisations pour les accès entrants et sortants et refusé tout autre accès par défaut. (1.3) OU L'entité responsable n'a pas effectué l'authentification lors de l'établissement de la connectivité par lien commuté avec les *actifs électroniques* visés, lorsque techniquement faisable. (1.4)
E2.	L'entité responsable n'a pas de processus documentés pour un ou plusieurs des éléments visés des alinéas 2.1 à 2.3.	L'entité responsable n'a pas mis en œuvre de processus pour un des éléments visés des alinéas 2.1 à 2.3.	L'entité responsable n'a pas mis en œuvre de processus pour deux des éléments visés des alinéas 2.1 à 2.3. OU	L'entité responsable n'a pas mis en œuvre de processus pour trois des éléments visés des alinéas 2.1 à 2.3. OU

Ex.	Niveau de gravité de la non-conformité			
	VSL faible	VSL modéré	VSL élevé	VSL critique
			L'entité responsable ne disposait pas : soit d'une ou de plusieurs méthodes permettant de déterminer les sessions actives d'accès distant par des fournisseurs (y compris les *accès distants interactifs* et les accès distants de système à système) (2.4) ; soit d'une ou de plusieurs méthodes permettant de désactiver les accès distants actifs des fournisseurs (y compris les *accès distants interactifs* et les accès distants de système à système (2.5).	L'entité responsable ne disposait : ni d'une ou de plusieurs méthodes permettant de déterminer les sessions actives d'accès distant par des fournisseurs (y compris les *accès distants interactifs* et les accès distants de système à système) (2.4) ; ni d'une ou de plusieurs méthodes permettant de désactiver les accès distants actifs des fournisseurs (y compris les *accès distants interactifs* et les accès distants de système à système) (2.5).

D. Différences régionales

Aucune.

E. 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	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. Suppression de la mention sur la prise en compte des considérations d'affaires. Remplacement de l'organisation régionale de fiabilité par l'entité régionale comme entité responsable. Reformulation de la date d'entrée en vigueur. Remplacement de « Responsabilité de la surveillance de la conformité » par « Responsable des mesures pour assurer la conformité».	
3	16 décembre 2009	Changement du numéro de version de -2 à -3. Approbation par le Conseil d'administration de la NERC.	
3	31 mars 2010	Approbation par la FERC.	
4	30 décembre 2010	Ajout de critères précis pour l'identification des actifs critiques.	Mise à jour
4	24 janvier 2011	Approbation par le Conseil d'administration de la NERC.	Mise à jour
5	26 novembre 2012	Adoption par le Conseil d'administration de la NERC.	Modifiée en coordination avec les autres normes CIP et révision du format selon le gabarit RBS.
5	22 novembre 2013	Ordonnance de la FERC approuvant la norme CIP-005-5.	
6	20 juillet 2017	Modifications visant à répondre à certaines directives de l'Ordonnance 829 de la FERC.	Révision
6	10 août 2017	Adoption par le Conseil d'administration de la NERC.	

6	18 octobre 2018	Ordonnance de la FERC approuvant la norme CIP-005-6. Dossier RM17-13-000.	

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

La section 4.2. *Installations* définit la portée des *installations,* systèmes et équipements détenus par l'entité responsable désignée à la section 4.1, qui 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. 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 l'appartenance au *BES*, l'utilisation additionnelle du terme « *BES* » vise ici à renforcer la portée d'applicabilité pour ces *installations*, en particulier dans cette section sur l'applicabilité. Cela établit quels sont les *installations*, systèmes et équipements visés par les normes.

Exigence E1

L'exigence E1 de la norme CIP-005-6 exige l'isolation des *systèmes électroniques BES* des autres systèmes de degrés de confiance différents en exigeant des *points d'accès électroniques* contrôlés entre les différentes zones de confiance. Les *périmètres de sécurité électronique* sont également utilisés comme première couche de défense pour certains *systèmes électroniques BES* qui ne disposent pas intrinsèquement d'une protection électronique suffisante, notamment les dispositifs qui n'ont pas de fonction d'authentification.

Tous les *systèmes électroniques BES* visés qui sont reliés à un réseau au moyen d'un protocole routable doivent avoir un *périmètre de sécurité électronique* (*ESP*) défini. Même les réseaux autonomes qui n'ont pas de connectivité externe avec d'autres réseaux doivent avoir un *ESP* défini. L'*ESP* établit une zone de protection autour d'un *système électronique BES* en plus de définir clairement, du point de vue des entités, quels sont les systèmes ou les *actifs électroniques* visés et quelles sont les exigences auxquelles elles doivent se conformer. L'*ESP* permet de définir :

- l'étendue des « *actifs électroniques protégés* (*PCA*) associés » qui doivent également répondre à certaines exigences CIP, et
- la frontière à l'intérieur de laquelle tous les *actifs électroniques* doivent répondre aux exigences qui s'appliquent au *système électronique BES* ayant l'impact le plus élevé à l'intérieur de la zone (seuil de protection).

Les normes sur la cybersécurité (CIP) n'exigent pas une segmentation par réseaux des *systèmes électroniques BES* en fonction de leur catégorie d'impact. Un *ESP* peut comprendre des systèmes ayant des degrés d'impact différents. Cependant, tous les *actifs électroniques* et les *systèmes électroniques BES* qui se trouvent à l'intérieur de l'*ESP* doivent avoir un niveau de protection équivalent à celui du *système électronique BES* inclus dans l'*ESP* dont l'impact est le plus élevé (ce que l'on appelle le « seuil de protection ») lorsque l'expression « *actifs électroniques protégés* » est utilisée. Dans les

normes sur la cybersécurité (CIP), on obtient le « seuil de protection » en définissant tous les *actifs électroniques* situés à l'intérieur d'un *ESP* comme « *actifs électroniques protégés* » ayant le même impact que le système à l'intérieur de l'*ESP* dont l'impact est le plus élevé, et ce, peu importe qu'ils aient un impact moindre.

Par exemple, si un ESP comprend à la fois un *système électronique BES* à impact élevé et un *système électronique BES* à impact faible, chaque *actif électronique* du *système électronique BES* à impact faible est considéré comme un « *actif électronique protégé* (*PCA*) associé » du *système électronique BES* à impact élevé, et il doit donc se conformer à toutes les exigences afférentes figurant dans les tableaux.

Lorsqu'un *actif électronique* est accessible par connectivité routable à travers l'*ESP*, les données qui entrent dans l'*ESP* ou en sortent doivent être contrôlées par un *point d'accès électronique* (*EAP*). Les entités responsables doivent savoir quelles données ont besoin de traverser l'*EAP*, et en justifier les raisons dans un document, afin de s'assurer que l'*EAP* limite les échanges aux communications nécessaires uniquement. Ces communications comprennent, sans s'y limiter, celles qui sont requises dans le cadre de l'exploitation normale, des interventions d'urgence, du soutien, de la maintenance et du dépannage.

L'*EAP* doit contrôler les échanges tant entrants que sortants. La norme exige dorénavant le contrôle des échanges sortants puisqu'elles constituent un premier indicateur de compromission et un mécanisme de défense de premier niveau contre les attaques de vulnérabilité du jour zéro. Si des *actifs électroniques* à l'intérieur de l'*ESP* sont compromis et tentent de communiquer avec des hôtes inconnus à l'extérieur de l'*ESP* (il s'agit habituellement d'hôtes de « commande et contrôle », sur Internet, ou d'hôtes de rebond compromis au sein d'autres réseaux de l'entité responsable et qui agissent comme intermédiaires), l'*EAP* doit agir comme mécanisme de défense de premier niveau pour rompre la communication. Cela n'empêche pas l'entité responsable de contrôler les échanges sortants au niveau de granularité qu'elle considère comme approprié et d'autoriser de grandes plages d'adresses internes. L'intention de l'équipe de rédaction de la norme (SDT) est de faire en sorte que l'entité responsable connaisse les autres *actifs électroniques* ou plages d'adresses avec lesquels le *système électronique BES* a besoin de communiquer et qu'elle limite les communications à ces actifs et adresses connus. Par exemple, la plupart des *systèmes électroniques BES* au sein du réseau de l'entité responsable ne devraient pas pouvoir communiquer via un EAP avec n'importe quelle adresse dans le monde ; à tout le moins, ils devraient probablement être limités à l'espace d'adressage de l'entité responsable et, idéalement, à des plages de sous-réseaux distincts ou à des hôtes particuliers à l'intérieur de l'espace d'adressage de l'entité responsable. L'objectif de la SDT n'est pas de faire en sorte que l'entité responsable documente les activités internes des pare-feu dynamiques, où les connexions amorcées dans un sens sont autorisées dans l'autre sens. L'objectif est plutôt que l'entité responsable connaisse et documente les systèmes ou groupes de systèmes qui peuvent communiquer entre eux de part et d'autre de l'*EAP* afin que les connexions indésirables puissent être détectées et bloquées.

Cette exigence vise uniquement les communications auxquelles peuvent s'appliquer de manière universelle des listes d'accès ou des exigences de type « refus par défaut », soit celles qui utilisent aujourd'hui des protocoles routables. Elle ne s'applique pas aux connexions directes série non routables, car il n'existe aucun périmètre ou pare-feu de sécurité qui devrait être rendu obligatoire pour l'ensemble des entités et des communications série. Il est impossible de mettre en place un pare-feu ou un périmètre de sécurité pour un câble RS-232 reliant deux *actifs électroniques*. Sans mécanisme de sécurité faisant appel à un périmètre et pouvant être appliqué à pratiquement tous les cas, une telle exigence aurait pour effet d'engendrer de nombreuses exceptions liées à la faisabilité technique (TFE) plutôt que d'améliorer la sécurité.

Dans le cas de la connectivité par lien commuté, l'intention de la SDT est de prévenir les situations où il serait possible d'établir une liaison directe avec un *actif électronique BES* au moyen d'un numéro de téléphone uniquement. Si un modem est configuré de manière à simplement répondre au téléphone et à établir la liaison avec l'*actif électronique BES* demandé sans authentifier le demandeur, il rend vulnérable le *système électronique BES*. En vertu de cette exigence, le modem doit authentifier le demandeur avant d'établir la communication avec le *système électronique BES*. Il peut s'agir par exemple de modems à fonction de rappel, de modems activés ou mis sous tension à distance et de modems mis sous tension au besoin par le personnel sur place et mis hors tension après utilisation en vertu d'une politique bien établie. L'exigence E2 s'applique également dans le cas d'une connectivité par lien commuté utilisée pour un *accès distant interactif*.

La norme ajoute une exigence pour les *centres de contrôle* concernant la détection des communications malveillantes. Ceci est en réponse à l'ordonnance 706 de la FERC, alinéas 496-503, stipulant qu'il faut prévoir deux dispositifs de sécurité distincts pour les *ESP* afin de préserver le périmètre de protection des *systèmes électroniques BES* advenant une défaillance ou un défaut de configuration de l'un ou l'autre de ces dispositifs. L'ordonnance indique clairement qu'il ne s'agit pas simplement d'assurer une redondance des pare-feu ; la SDT a donc décidé d'ajouter l'exigence liée à la mise en œuvre de moyens de détection des communications malveillantes pour les *ESP*. Les technologies qui répondent à cette exigence comprennent notamment les systèmes de détection ou de prévention des intrusions (IDS/IPS) et d'autres formes d'inspection en profondeur des paquets. Ces technologies vont plus loin que les ensembles de règles associant ports, sources et destinations, et constituent par le fait même un autre mécanisme de sécurité distinct mis en œuvre par l'*ESP*.

Exigence E2

Voir le document de référence sur l'accès distant protégé (voir alerte d'accès distant).

Justifications

Justifications pour E1

Le *périmètre de sécurité électronique* (*ESP*) sert à contrôler les échanges de données à la frontière électronique externe du *système électronique BES*. Il constitue une première couche de défense contre les attaques provenant du réseau puisqu'il limite la reconnaissance des cibles, restreint et interdit les échanges en fonction d'un ensemble de règles définies et contribue à circonscrire les effets d'attaques réussies.

Sommaire des modifications apportées : L'exigence E1 de la norme CIP-005 insiste davantage sur les *points d'accès électroniques* distincts que sur le « périmètre » logique.

L'exigence à l'alinéa 1.2 de la norme CIP-005 (versions 1 à 4) a été supprimée de la version 5. Cette exigence avait un caractère définitoire et servait à inclure les modems commutés utilisant des protocoles non routables dans le domaine d'application de la norme CIP-005. L'exclusion liée aux protocoles non routables n'existant plus en tant que critère spécifique d'applicabilité (norme CIP-002) dans la version 5, cette exigence est dorénavant inutile.

Les exigences aux alinéas 1.1 et 1.3 de la norme CIP-005 (versions 1 à 4) avaient également un caractère définitoire et ont été supprimées de la version 5 ; cependant, les concepts sous-jacents à ces deux exigences ont été intégrés aux définitions des termes *périmètre de sécurité électronique* (*ESP*) et *point d'accès électronique* (*EAP*).

Référence à une version précédente : (alinéa 1.1) CIP-005-4, E1

Justification des modifications : (alinéa 1.1)

Affirmation claire du fait que les *actifs électroniques BES* reliés au moyen d'un protocole routable doivent se situer à l'intérieur d'un *périmètre de sécurité électronique*.

Référence à une version précédente : (alinéa 1.2) CIP-005-4, E1

Justification des modifications : (alinéa 1.2)

Utilisation des termes définis *point d'accès électronique* et *système électronique BES*.

Référence à une version précédente : (alinéa 1.3) CIP-005-4, E2.1

Justification des modifications : (alinéa 1.3)

Utilisation du terme défini *point d'accès électronique* et insistance sur le fait que l'entité doit connaître les accès entrants et sortants via l'*EAP* qu'elle autorise et que les raisons pour lesquelles elle autorise ces accès sont justifiées.

Référence à une version précédente : (alinéa 1.4) CIP-005-4, E2.3

Justification des modifications apportées : (alinéa 1.4)

Explication plus claire du fait que la connectivité par lien commuté doit assurer l'authentification afin de rendre impossible l'accès direct au *système électronique BES* à l'aide d'un simple numéro de téléphone.

Référence à une version précédente : (alinéa 1.5) CIP-005-4, E1

Justification des modifications : (alinéa 1.5)

Conformité avec l'Ordonnance 706 de la FERC, alinéas 496-503, en vertu de laquelle il faut prévoir deux dispositifs de sécurité distincts pour les *ESP* afin de préserver le périmètre de protection des *actifs électroniques* advenant une défaillance ou un défaut de configuration de l'un ou l'autre de ces

dispositifs. L'Ordonnance indique clairement qu'il ne s'agit pas simplement d'assurer une redondance des pare-feu ; la SDT a donc décidé d'ajouter l'exigence liée à la mise en œuvre de moyens de détection des communications malveillantes pour les *ESP*.

Justifications pour E2

Les entités inscrites utilisent l'*accès distant interactif* pour accéder aux *actifs électroniques* en vue d'assurer le soutien et la maintenance des réseaux de systèmes de commande. La détection et le signalement des vulnérabilités dans les technologies et les méthodes d'accès distant, que l'on croyait sécurisées et qui étaient utilisées par des entités du secteur électrique, nécessitent que l'on apporte des modifications aux normes de contrôle de la sécurité au sein de l'industrie. Actuellement, aucune exigence n'oblige les gestionnaires d'un accès distant sécurisé à des *actifs électroniques* à se doter des mesures de protection mentionnées dans les normes CIP de la NERC. Des dispositifs de protection inadéquats peuvent permettre un accès non autorisé au réseau de l'organisation, ce qui pourrait entraîner des conséquences graves. Le document ***Guidance for Secure Interactive Remote Access***, publié par la NERC en juillet 2011, renferme davantage de renseignements à cet égard.

Les procédures de contrôle de l'accès distant doivent prévoir des mesures de protection adéquates, notamment l'utilisation de techniques d'identification, d'authentification et de cryptage efficaces. L'accès distant au réseau et aux ressources de l'organisation ne doit être permis que si les conditions suivantes sont remplies : les utilisateurs autorisés sont authentifiés, les données sont cryptées dans tout le réseau et les privilèges sont restreints.

Le *système intermédiaire* sert de mandataire pour l'utilisateur distant. Au lieu de faire en sorte que tous les protocoles dont l'utilisateur pourrait avoir besoin pour accéder aux *actifs électroniques* à l'intérieur du *périmètre de sécurité électronique* puissent traverser ce *périmètre de sécurité électronique* pour atteindre l'ordinateur distant, on ne laisse passer que le protocole nécessaire pour commander à distance l'hôte de rebond. Ainsi, on peut établir des règles de pare-feu beaucoup plus contraignantes que s'il fallait autoriser l'ordinateur distant à se connecter directement aux *actifs électroniques* se trouvant dans le *périmètre de sécurité électronique*. Un *système intermédiaire* permet aussi de protéger les *actifs électroniques* des vulnérabilités de l'ordinateur distant.

L'application d'une méthode d'authentification multifactorielle offre une couche de protection supplémentaire. En effet, les mots de passe peuvent être devinés, volés, piratés, trouvés ou divulgués. Pour découvrir un mot de passe, on peut lancer des attaques automatisées, notamment des attaques par force brute – essai de tous les mots de passe possibles – ou des attaques par dictionnaire – essai de mots ou de combinaisons de mots. Toutefois, un mot de passe ou un NIP n'a aucune valeur si l'on n'acquiert pas en même temps les autres facteurs requis pour l'authentification, comme un jeton ou une empreinte digitale.

Le cryptage protège les données transmises entre l'ordinateur distant et le *système intermédiaire*. Il faut crypter les données pour pouvoir les transférer de manière sécuritaire, notamment lorsqu'il existe un risque d'interception non autorisée sur les voies de communication utilisées, particulièrement sur Internet.

Les alinéas 2.4 et 2.5 de l'exigence E2 répondent aux prescriptions de l'Ordonnance 829 de la FERC qui spécifient des contrôles pour les accès distants par les fournisseurs aux *systèmes électroniques BES* – tant les accès qui sont commandés par l'utilisateur que ceux qui se font de système à système (alinéa 51). L'objectif est d'atténuer les risques potentiels qu'une compromission chez un fournisseur pendant une session active d'accès distant avec une entité responsable puisse avoir un impact sur le *BES*.

L'objectif de l'alinéa 2.4 de l'exigence E2 est de faire en sorte que les entités aient une bonne visibilité sur les sessions d'accès distant des fournisseurs (tant les *accès distants interactifs* que les accès distants de système à système) qui sont actives dans leur système. Cette prescription s'étend à toutes les sessions d'accès distant avec des fournisseurs. L'alinéa 2.4 stipule que les entités doivent disposer d'une méthode permettant de déterminer les sessions actives d'accès distant avec des fournisseurs. Bien que non nécessaire, une solution qui couvrirait toutes les sessions actives d'accès distant, établies ou non par des fournisseurs, répondrait à cette exigence. L'objectif de l'alinéa 2.5 de l'exigence E2 est de faire en sorte que les entités aient la capacité de désactiver les sessions actives d'accès distant en cas de brèche de sécurité, comme le spécifie l'alinéa 52 de l'Ordonnance 829.

La portée de l'exigence E2 de la norme CIP-005-6 est élargie par rapport à la norme CIP-005-5 approuvée afin de couvrir non seulement les *accès distant interactifs*, mais bien l'ensemble des accès distants. Si une entité responsable ne permet pas les accès distants (*accès distants interactifs* et accès distants de système à système), cette entité n'est pas tenue d'élaborer un processus pour chacun des alinéas de l'exigence E2 ; elle pourrait simplement documenter qu'elle ne permet pas les accès distants afin de réaliser l'objectif de fiabilité.

Le terme « fournisseur » utilisé dans cette norme désigne uniquement les personnes, entreprises ou autres organisations avec lesquelles l'entité responsable, ou une société affiliée, est en relation contractuelle en vue de la fourniture de *systèmes électroniques BES* et de services connexes. Ce terme exclut les autres entités inscrites auprès de la NERC qui fournissent des services de fiabilité (par exemple, des services de *responsable de l'équilibrage* ou de *coordonnateur de la fiabilité* dans le cadre des normes de fiabilité de la NERC). Un fournisseur, selon l'emploi de ce terme dans la norme, peut comprendre : i) des créateurs de logiciels ou de systèmes d'information, des fabricants de composants de système ou des prestataires de services informatiques ; ii) des revendeurs de produits ; ou iii) des intégrateurs de systèmes.

Sommaire des modifications apportées : Il s'agit d'une nouvelle exigence pour appuyer la poursuite des efforts de l'équipe d'intervention rapide dans le cadre du projet 2010-15 (révision accélérée de la norme CIP-005-3).

Référence à une version précédente : (alinéa 2.1) Nouveau

Justification des modifications apportées : (alinéa 2.1)

Nouvelle exigence visant à poursuivre les efforts de l'équipe d'intervention rapide affectée au projet 2010-15 (révision accélérée de la norme CIP-005-3).

Référence à une version précédente : (alinéa 2.2) CIP-007-5, E3.1

Justification des modifications apportées : (alinéa 2.2)

Nouvelle exigence visant à poursuivre les efforts de l'équipe d'intervention rapide affectée au projet 2010-15 (révision accélérée de la norme CIP-005-3). Cette exigence vise à protéger la confidentialité et l'intégrité de chaque session d'*accès distant interactif*.

Référence à une version précédente : (alinéa 2.3) CIP-007-5, E3.2

Justification des modifications apportées : (alinéa 2.3)

Nouvelle exigence visant à poursuivre les efforts de l'équipe d'intervention rapide affectée au projet 2010-15 (révision accélérée de la norme CIP-005-3). Les méthodes d'authentification

multifactorielle sont décrites dans la Homeland Security Presidential Directive 12 (HSPD-12) du 12 août 2007.

A. Introduction

1. **Titre :** Cybersécurité — Déclaration des incidents et planification des mesures d'intervention

2. **Numéro :** CIP-008-6

3. **Objet :** Réduire les risques posés au fonctionnement fiable du *BES* par un *incident de cybersécurité* en définissant des exigences d'intervention en cas d'incident.

4. **Applicabilité :**

   4.1. Entités fonctionnelles : Dans le contexte de la présente norme, les entités fonctionnelles indiquées ci-après sont appelées collectivement « entités responsables ». Si certaines exigences visent plus spécifiquement une entité fonctionnelle ou un sous-ensemble 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 systèmes, *installations* et équipements suivants pour la protection ou la remise en charge du *BES* :

   4.1.2.1. Système de délestage de charge en sous-fréquence (DSF) ou 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 ;*

   4.1.2.1.2. effectue des délestages automatiques de *charge* de 300 MW ou plus sous la commande d'un système commun détenu par l'entité responsable, sans intervention humaine.

   4.1.2.2. *Automatisme de réseau (RAS)* visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou de l'*entité régionale*.

   4.1.2.3. *Système de protection* de réseau de *transport* (à l'exclusion des systèmes de DSF et de DST) visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou de l'*entité régionale*.

   4.1.2.4. *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 de la fiabilité***

   4.1.6. ***Exploitant de réseau de transport***

   4.1.7. ***Propriétaire d'installation de transport***

4.2. ***Installations*** **:** Dans le contexte de la présente norme, les systèmes, *installations* et équipements suivants détenus par une entité responsable indiquée à la section 4.1 sont visés par les exigences. Si certaines exigences visent plus spécifiquement un type ou un sous-ensemble de systèmes, d'*installations* ou d'équipements, ceux-ci sont précisés explicitement.

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

4.2.1.1. 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 des délestages de *charge* automatiques de 300 MW ou plus sous la commande d'un système commun détenu par l'entité responsable, sans intervention humaine.

4.2.1.2. *Automatisme de réseau* (*RAS*) visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou de l'*entité régionale*.

4.2.1.3. *Système de protection* de réseau de *transport* (à l'exclusion des systèmes de DSF et de DST) visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou de l'entité régionale.

4.2.1.4. *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-008-6 :

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 électronique* distincts.

4.2.3.3. Les systèmes, structures et composantes régis par la U.S. Nuclear Regulatory Commission en vertu d'un plan de cybersécurité conforme 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 ont déterminé qu'elles n'ont aucun *système électronique BES* classé dans les catégories « impact élevé » ou « impact moyen » selon le processus d'inventaire et de catégorisation de la norme CIP-002.

5. Dates d'entrée en vigueur :

Voir le plan de mise en œuvre de la norme CIP-008-6.

6. Contexte :

La norme CIP-008 fait partie d'une série de normes CIP sur la cybersécurité. La norme CIP-002 exige l'inventaire et la catégorisation initiale des *systèmes électroniques BES*. Les normes CIP-003, CIP-004, CIP-005, CIP-006, CIP-007, CIP-008, CIP-009, CIP-010 et CIP-011 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 le 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 cela correspond à la compréhension générale. 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 particulier. 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 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 de DSF et de DST. Ce seuil particulier de 300 MW pour les systèmes de DSF et de DST provient de la version 1 des normes CIP sur la cybersécurité. Le seuil demeure à 300 MW puisqu'il

concerne spécifiquement les systèmes de DST et de DSF, qui constituent des efforts de dernier recours pour sauver le *système de production-transport d'électricité*. Un examen des tolérances des systèmes de 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 de 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. L'équipe de rédaction (SDT) CSO706 a adapté ce concept à partir du cadre de gestion des risques du National Institute of Standards and Technology (NIST) en vue d'établir une méthode d'application des exigences qui tient compte plus adéquatement de l'impact et des caractéristiques de connectivité. La colonne « Systèmes visés » repose sur les conventions suivantes :

- ***Systèmes électroniques BES* à impact élevé** – Désigne les *systèmes électroniques BES* classés dans la catégorie « impact élevé », selon les processus d'inventaire et de catégorisation de la norme CIP-002.
- ***Systèmes électroniques BES* à impact moyen** – Désigne les *systèmes électroniques BES* classés dans la catégorie « impact moyen », selon les processus d'inventaire et de catégorisation de la norme CIP-002.

B. Exigences et mesures

E1. Chaque entité responsable doit mettre en œuvre un ou plusieurs plans d'intervention en cas d'*incident de cybersécurité* documentés qui, collectivement, couvrent tous les alinéas applicables du tableau E1 (CIP-008-6) – Caractéristiques du plan d'intervention en cas d'*incident de cybersécurité*.
[Facteur de risque de non-conformité : faible] [Horizon : planification à long terme]

M1. Les pièces justificatives doivent comprendre chacun des plans documentés qui, collectivement, couvrent tous les alinéas applicables du tableau E1 (CIP-008-6) – Caractéristiques du plan d'intervention en cas d'*incident de cybersécurité*.

Tableau E1 (CIP-008-6) – Caractéristiques du plan d'intervention en cas d'*incident de cybersécurité*

Alinéa	Systèmes visés	Exigences	Mesures
1.1	*Systèmes électroniques BES* à impact élevé et : • les *EACMS* associés. *Systèmes électroniques BES* à impact moyen et : • les *EACMS* associés	Un ou plusieurs processus visant à détecter les *incidents de cybersécurité*, à les classer et à y répondre.	Exemple non limitatif de pièce justificative : plan ou plans d'intervention en cas d'*incident de cybersécurité* documentés et datés qui prévoient un ou des processus pour détecter les *incidents de cybersécurité*, les classer et y répondre.

Tableau E1 (CIP-008-6) – Caractéristiques du plan d'intervention en cas d'*incident de cybersécurité*			
Alinéa	**Systèmes visés**	**Exigences**	**Mesures**
1.2	*Systèmes électroniques BES* à impact élevé et : • les *EACMS* associés. *Systèmes électroniques BES* à impact moyen et : • les *EACMS* associés.	Un ou plusieurs processus : 1.2.1 qui comprennent des critères d'évaluation servant à reconnaître les tentatives de compromission ; 1.2.2 qui visent à déterminer si un *incident de cybersécurité* constaté est : • un *incident de cybersécurité à signaler* ; ou • une tentative de compromettre, selon les critères prescrits à l'alinéa 1.2.1, un ou plusieurs systèmes indiqués à la colonne « Systèmes visés » du présent alinéa ; et 1.2.3 qui spécifient une notification selon l'exigence E4.	Exemples non limitatifs de pièces justificatives : plan ou plans d'intervention pour *incident de cybersécurité* documentés et datés qui fournissent des indications ou des seuils pour déterminer quels *incidents de cybersécurité* sont aussi un *incident de cybersécurité à signaler* ou un *incident de cybersécurité* dont on détermine qu'il constitue une tentative de compromettre un système indiqué à la colonne « Systèmes visés », y compris la justification des critères d'évaluation, ainsi que des processus documentés de notification.
1.3	*Systèmes électroniques BES* à impact élevé et : • les *EACMS* associés. *Systèmes électroniques BES* à impact moyen et : • les *EACMS* associés.	Rôles et responsabilités des groupes ou des personnes chargés de l'intervention en cas d'*incident de cybersécurité*.	Exemple non limitatif de pièce justificative : processus ou procédures d'intervention en cas d'*incident de cybersécurité* datés qui définissent les rôles et les responsabilités (p. ex., surveillance, déclaration, déclenchement, documentation, etc.) des groupes ou des personnes chargés de l'intervention en cas d'*incident de cybersécurité*.

Tableau E1 (CIP-008-6) – Caractéristiques du plan d'intervention en cas d'*incident de cybersécurité*			
Alinéa	**Systèmes visés**	**Exigences**	**Mesures**
1.4	*Systèmes électroniques BES* à impact élevé et : • les *EACMS* associés. *Systèmes électroniques BES* à impact moyen et : • les *EACMS* associés.	Procédures de gestion des *incidents de cybersécurité*.	Exemples non limitatifs de pièces justificatives : processus ou procédures d'intervention en cas d'*incident de cybersécurité* datés qui traitent de la gestion des incidents (p. ex., confinement, élimination, reprise après incident ou résolution de l'incident).

E2. Chaque entité responsable doit mettre en œuvre chacun de ses plans d'intervention en cas d'*incident de cybersécurité* documentés qui, collectivement, couvrent tous les alinéas applicables du tableau E2 (CIP-008-6) – Mise en œuvre et vérification du plan d'intervention en cas d'*incident de cybersécurité*.
[Facteur de risque de non-conformité : faible] [Horizon : planification de l'exploitation et exploitation en temps réel].

M2. Les pièces justificatives doivent comprendre, sans toutefois s'y limiter, des documents qui, collectivement, démontrent la mise en œuvre de tous les alinéas applicables du tableau E2 (CIP-008-6) – Mise en œuvre et vérification du plan d'intervention en cas d'*incident de cybersécurité*.

Tableau E2 (CIP-008-6) – Mise en œuvre et vérification du plan d'intervention en cas d'*incident de cybersécurité*			
Alinéa	**Systèmes visés**	**Exigences**	**Mesures**
2.1	*Systèmes électroniques BES* à impact élevé et : • les *EACMS* associés. *Systèmes électroniques BES* à impact moyen et : • les *EACMS* associés.	Tester chaque plan d'intervention en cas d'*incident de cybersécurité* au moins une fois tous les 15 mois civils : • en répondant à un *incident de cybersécurité à déclarer* réel ; • en effectuant un exercice de réponse à un *incident de cybersécurité à déclarer*, sur papier ou en salle ; ou • en effectuant un exercice opérationnel de réponse à un *incident de cybersécurité à déclarer*.	Exemple non limitatif de pièce justificative : preuve datée de l'existence d'un rapport sur les leçons apprises qui contient un résumé de l'épreuve ou une compilation des notes, des journaux et des communications qui résultent du test. Les types d'exercices peuvent inclure des exercices axés sur les discussions ou sur les opérations.

Tableau E2 (CIP-008-6) – Mise en œuvre et vérification du plan d'intervention en cas d'*incident de cybersécurité*			
Alinéa	**Systèmes visés**	**Exigences**	**Mesures**
2.2	*Systèmes électroniques BES* à impact élevé et : • les *EACMS* associés. *Systèmes électroniques BES* à impact moyen et : • les *EACMS* associés.	Utiliser le ou les plans d'intervention en cas d'*incident de cybersécurité* cités à l'exigence E1 au moment de répondre à un *incident de cybersécurité à déclarer*, de répondre à un *incident de cybersécurité* consistant en une tentative de compromettre un système indiqué à la colonne « Systèmes visés » du présent alinéa ou d'effectuer un exercice de réponse à un *incident de cybersécurité à déclarer*. Documenter les écarts entre le ou les plans et les mesures prises pendant l'intervention à la suite de l'incident ou lors de l'exercice.	Exemples non limitatifs de pièces justificatives : rapports d'incident, journaux et notes prises durant l'intervention à la suite de l'incident, et documents de suivi décrivant les écarts entre le ou les plans et les mesures prises durant l'intervention à la suite de l'incident ou lors de l'exercice.
2.3	*Systèmes électroniques BES* à impact élevé et : • les *EACMS* associés. *Systèmes électroniques BES* à impact moyen et : • les *EACMS* associés.	Conserver les dossiers relatifs aux *incidents de cybersécurité à déclarer* et aux *incidents de cybersécurité* consistant en une tentative de compromettre un système indiqué à la colonne « Systèmes visés » du présent alinéa conformément aux plans d'intervention en cas d'*incident de cybersécurité* spécifiés à l'exigence E1.	Exemples non limitatifs de pièces justificatives : documents datés, tels que journaux de sécurité, rapports de police, courriels, formulaires d'intervention ou listes de contrôle, résultats d'analyses judiciaires, dossiers de remise en charge et notes d'analyse après incident relativement à *des incidents de cybersécurité à déclarer* et à des *incidents de cybersécurité* consistant en une tentative de compromettre un système indiqué à la colonne « Systèmes visés ».

E3. Chaque entité responsable doit tenir à jour chacun de ses plans d'intervention en cas d'*incident de cybersécurité* conformément à chacun des alinéas applicables du tableau E3 (CIP-008-6) – Examen, mise à jour et communication du plan d'intervention en cas d'*incident de cybersécurité*.
[Facteur de risque de non-conformité : faible] [Horizon : évaluation des activités d'exploitation]

M3. Les pièces justificatives doivent comprendre, sans toutefois s'y limiter, des documents qui, collectivement, démontrent que tous les plans d'intervention en cas d'*incident de cybersécurité* sont tenus à jour conformément aux alinéas applicables du tableau E3 (CIP-008-6) – Examen, mise à jour et communication du plan d'intervention en cas d'*incident de cybersécurité*.

Tableau E3 (CIP-008-6) – Examen, mise à jour et communication du plan d'intervention en cas d'*incident de cybersécurité*			
Alinéa	**Systèmes visés**	**Exigences**	**Mesures**
3.1	*Systèmes électroniques BES* à impact élevé et : • les *EACMS* associés. *Systèmes électroniques BES* à impact moyen et : • les *EACMS* associés.	Au plus tard 90 jours civils après la réalisation d'un test des plans d'intervention en cas d'*incident de cybersécurité* ou après une intervention réelle en cas d'*incident de cybersécurité à déclarer* : 3.1.1. documenter les leçons apprises, ou encore l'absence de leçons apprises ; 3.1.2. mettre à jour le plan d'intervention en cas d'*incident de cybersécurité* en tenant compte des leçons apprises documentées qui se rapportent à ce plan ; et 3.1.3 aviser chaque personne ou groupe qui joue un rôle défini dans le plan d'intervention en cas d'*incident de cybersécurité* des mises à jour à ce plan qui tiennent compte des leçons apprises documentées.	Exemples non limitatifs de pièces justificatives : 1. documents datés, tels que notes de réunion après incident ou rapports de suivi indiquant les leçons apprises associées à la mise à l'épreuve du ou des plans d'intervention en cas d'*incident de cybersécurité* ou à une intervention réelle en cas d'*incident de cybersécurité à déclarer*, ou encore documents datés confirmant l'absence de leçons apprises ; 2. plan d'intervention en cas d'*incident de cybersécurité* daté et révisé indiquant toutes les modifications apportées en tenant compte des leçons apprises ; et 3. preuve de distribution du plan révisé, par exemple : • courriels ; • service postal (US Postal Service ou autre) ; • système de distribution électronique ; ou • feuilles de présence aux formations.

Tableau E3 (CIP-008-6) – Examen, mise à jour et communication du plan d'intervention en cas d'*incident de cybersécurité*			
Alinéa	**Systèmes visés**	**Exigences**	**Mesures**
3.2	*Systèmes électroniques BES* à impact élevé et : • les *EACMS* associés. *Systèmes électroniques BES* à impact moyen et : • les *EACMS* associés.	Au plus tard 60 jours civils après qu'un changement jugé par l'entité responsable comme ayant un impact sur la capacité d'exécuter le plan a été apporté aux rôles ou responsabilités, aux groupes ou personnes chargés de l'intervention en cas d'*incident de cybersécurité* ou à une technologie : 3.2.1. mettre à jour le ou les plans d'intervention en cas d'*incident de cybersécurité* ; et 3.2.2. aviser des mises à jour chaque personne ou groupe jouant un rôle défini dans le plan d'intervention en cas d'*incident de cybersécurité*.	Exemples non limitatifs de pièces justificatives : 1. plan d'intervention en cas d'*incident de cybersécurité* révisé et daté comprenant les changements apportés aux rôles ou responsabilités, aux intervenants ou à une technologie ; et 2. preuve de distribution du plan révisé, par exemple : • courriels ; • service postal (US Postal Service ou autre) ; • système de distribution électronique ; ou • feuilles de présence aux formations.

E4. Chaque entité responsable doit aviser l'Electricity Information Sharing and Analysis Center (E-ISAC) et aussi, si elle est soumise à la réglementation des États-Unis, le National Cybersecurity and Communications Integration Center (NCCIC)[1] des États-Unis, ou leurs remplaçants éventuels, de tout *incident de cybersécurité à déclarer* et de tout *incident de cybersécurité* qui constitue une tentative de compromettre, selon les critères prescrits à l'alinéa 1.2.1 de l'exigence E1, un système indiqué à la colonne « Systèmes visés », à moins que la loi ne l'interdise, conformément à chacun des alinéas applicables du tableau E4 (CIP-008-6) – Notification et déclaration des *incidents de cybersécurité*.
[Facteur de risque de non-conformité : faible] [Horizon : évaluation des activités d'exploitation].

M4. Les pièces justificatives doivent comprendre, sans toutefois s'y limiter, des documents qui, collectivement, démontrent la notification de chaque *incident de cybersécurité à déclarer* et *incident de cybersécurité* qui constitue une tentative de compromettre un système indiqué à la colonne « Systèmes visés », conformément aux alinéas applicables du tableau E4 (CIP-008-6) – Notification et déclaration des *incidents de cybersécurité.*

Tableau E4 (CIP-008-6) – Notification et déclaration des *incidents de cybersécurité*

Alinéa	Systèmes visés	Exigences	Mesures
4.1	*Systèmes électroniques BES* à impact élevé et : • les *EACMS* associés. *Systèmes électroniques BES* à impact moyen et : • les *EACMS* associés.	Les notifications initiales et leurs mises à jour doivent au minimum préciser les éléments suivants, dans la mesure où ils sont connus : 4.1.1 l'impact fonctionnel ; 4.1.2 le vecteur d'attaque utilisé ; et 4.1.3 le degré d'intrusion atteint ou visé.	Exemples non limitatifs de pièces justificatives : documents datés de notification initiale et de mise à jour transmis à l'E-ISAC et au NCCIC.

1. Le National Cybersecurity and Communications Integration Center (NCCIC) est l'organisme qui remplace l'Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). En 2017, le NCCIC a réorganisé ses structures en y intégrant des fonctions antérieurement remplies de façon indépendante par l'ICS-CERT et par la United States Computer Emergency Readiness Team (US-CERT).

Tableau E4 (CIP-008-6) – Notification et déclaration des *incidents de cybersécurité*			
Alinéa	**Systèmes visés**	**Exigences**	**Mesures**
4.2	*Systèmes électroniques BES* à impact élevé et : • les *EACMS* associés. *Systèmes électroniques BES* à impact moyen et : • les *EACMS* associés.	Après la détermination par l'entité responsable selon le ou les processus documentés prescrits à l'alinéa 1.2 de l'exigence E1, transmettre une notification initiale dans les délais suivants : • une heure après avoir déterminé qu'il s'est produit un *incident de cybersécurité à signaler* ; • au plus tard à la fin du jour civil suivant la détermination qu'un *incident de cybersécurité* constitue une tentative de compromettre un système indiqué à la colonne « Systèmes visés » du présent alinéa.	Exemples non limitatifs de pièces justificatives : documents datés de notification transmis à l'E-ISAC et au NCCIC.
4.3	*Systèmes électroniques BES* à impact élevé et : • les *EACMS* associés *Systèmes électroniques BES* à impact moyen et : • les *EACMS* associés	Transmettre toute mise à jour pertinente, dans un délai de 7 jours civils après avoir déterminé des ajouts ou des changements aux éléments d'information exigés à l'alinéa 4.1.	Exemples non limitatifs de pièces justificatives : documents pertinents datés transmis à l'E-ISAC et au NCCIC.

C. Conformité

1. Processus de surveillance de la conformité

1.1. Responsable des mesures pour assurer la conformité

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

1.2. Conservation des pièces justificatives

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

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

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

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

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

1.4. Autres informations sur la conformité

- Aucune

2. Tableau des éléments de conformité

Ex.	Horizon	VRF	Niveau de gravité de la non-conformité (VSL) (CIP-008-6)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
E1.	**Planification à long terme**	**Faible**	Sans objet	Sans objet	L'entité responsable a élaboré un ou des plans d'intervention en cas d'*incident de cybersécurité*, mais ces plans ne comprennent pas les rôles et responsabilités des groupes ou des personnes chargés de l'intervention en cas d'*incident de cybersécurité*. (1.3) OU L'entité responsable a élaboré un ou des plans d'intervention en cas d'*incident de cybersécurité*, mais ces plans ne comprennent pas les procédures de gestion des *incidents de cybersécurité*. (1.4) OU L'entité responsable a élaboré un plan d'intervention en cas d'*incident de cybersécurité*, mais ce plan ne comprend pas de processus qui spécifie	L'entité responsable n'a pas élaboré un plan d'intervention en cas d'*incident de cybersécurité* comprenant un ou plusieurs processus visant à détecter les *incidents de cybersécurité*, à les classer et à y répondre. (1.1) OU L'entité responsable a élaboré un plan d'intervention en cas d'*incident de cybersécurité,* mais ce plan ne comprend pas un ou plusieurs processus permettant de reconnaître les *incidents de cybersécurité à déclarer* ou tout *incident de cybersécurité* qui constitue une tentative de compromettre, selon les critères prescrits à l'alinéa 1.2.1, un système indiqué à la colonne « Systèmes visés » de l'alinéa 1.2. (1.2)

Ex.	Horizon	VRF	Niveau de gravité de la non-conformité (VSL) (CIP-008-6)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
					une notification selon l'exigence E4. (1.4) OU L'entité responsable a élaboré un plan d'intervention en cas d'*incident de cybersécurité*, mais ce plan ne comprend pas de processus qui spécifie des critères d'évaluation servant à reconnaître les tentatives de compromission. (1.2)	
E2.	**Planification de l'exploitation** **Exploitation en temps réel**	**Faible**	L'entité responsable n'a pas testé le ou les plans d'intervention en cas d'*incident de cybersécurité* dans un intervalle de 15 mois civils, sans excéder 16 mois civils, entre les tests du ou des plans. (2.1)	L'entité responsable n'a pas testé le ou les plans d'intervention en cas d'*incident de cybersécurité* dans un intervalle de 16 mois civils, sans excéder 17 mois civils, entre les tests du ou des plans. (2.1)	L'entité responsable n'a pas testé le ou les plans d'intervention en cas d'*incident de cybersécurité* dans un intervalle de 17 mois civils, sans excéder 18 mois civils, entre les tests du ou des plans. (2.1) OU L'entité responsable n'a pas documenté les écarts, s'il y en a, par rapport au plan pendant un exercice ou lorsque se produit un *incident de cybersécurité à déclarer* ou un *incident de cybersécurité* qui constitue une tentative de	L'entité responsable n'a pas testé le ou les plans d'intervention en cas d'*incident de cybersécurité* dans un intervalle de 18 mois civils entre les tests du ou des plans. (2.1) OU L'entité responsable n'a pas conservé les dossiers pertinents relatifs aux *incidents de cybersécurité à déclarer* ou aux *incidents de cybersécurité* qui constituent une tentative de compromettre un système indiqué à la colonne

Ex.	Horizon	VRF	Niveau de gravité de la non-conformité (VSL) (CIP-008-6)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
					compromettre un système indiqué à la colonne « Systèmes visés » de l'alinéa 2.2. (2.2)	« Systèmes visés » de l'alinéa 2.3. (2.3)
E3.	**Évaluation de l'exploitation**	**Faible**	L'entité responsable n'a pas avisé chaque personne ou groupe qui joue un rôle défini dans le plan d'intervention en cas d'*incident de cybersécurité* des mises à jour à ce plan dans un délai de 90 jours civils suivant un test ou une intervention réelle à un *incident de cybersécurité à déclarer*, mais l'a fait dans un délai de moins de 120 jours civils. (3.1.3)	L'entité responsable n'a pas mis à jour le plan d'intervention en cas d'*incident de cybersécurité* en tenant compte des leçons apprises documentées dans un délai de 90 jours civils suivant un test ou une intervention réelle à un *incident de cybersécurité à déclarer*, mais l'a fait dans un délai de moins de 120 jours civils. (3.1.2) OU L'entité responsable n'a pas avisé chaque personne ou groupe qui joue un rôle défini dans le plan d'intervention en cas d'*incident de cybersécurité* des mises à jour à ce plan dans un délai de 120 jours civils suivant un test ou une intervention réelle à un *incident de cybersécurité à déclarer*. (3.1.3) OU	L'entité responsable n'a ni documenté les leçons apprises ni documenté l'absence de leçons apprises dans un délai de 90 jours civils suivant un test ou une intervention réelle à un *incident de cybersécurité à déclarer*, mais l'a fait dans un délai de moins de 120 jours civils. (3.1.1) OU L'entité responsable n'a pas mis à jour le plan d'intervention en cas d'*incident de cybersécurité* en tenant compte des leçons apprises documentées dans un délai de 120 jours civils suivant un test ou une intervention réelle à un *incident de cybersécurité à déclarer*. (3.1.2) OU L'entité responsable n'a pas mis à jour le ou les plans d'intervention en cas	L'entité responsable n'a ni documenté les leçons apprises ni documenté l'absence de leçons apprises dans un délai de 120 jours civils suivant un test ou une intervention réelle à un *incident de cybersécurité à déclarer*. (3.1.1)

Ex.	Horizon	VRF	Niveau de gravité de la non-conformité (VSL) (CIP-008-6)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
				L'entité responsable n'a pas mis à jour le ou les plans d'intervention en cas d'*incident de cybersécurité* ou avisé chaque personne ou groupe qui joue un rôle défini dans le plan d'intervention dans un délai de 60 jours civils suivant un des changements ci-après que l'entité responsable juge comme ayant un impact sur la capacité à exécuter le plan, mais l'a fait dans un délai de moins de 90 jours civils : (3.2) • changements aux rôles et responsabilités ou • changements aux personnes ou groupes intervenant en cas d'*incident de cybersécurité* ou • changements technologiques.	d'*incident de cybersécurité* ou avisé chaque personne ou groupe qui joue un rôle défini dans le plan d'intervention dans un délai de 90 jours civils suivant un des changements ci-après que l'entité responsable juge comme ayant un impact sur la capacité à exécuter le plan : (3.2) • changements aux rôles et responsabilités ou • changements aux personnes ou groupes intervenant en cas d'*incident de cybersécurité* ou • changements technologiques.	
E4.	**Évaluation des activités d'exploitation**	**Faible**	L'entité responsable a avisé l'E-ISAC et le NCCIC, ou leurs remplaçants éventuels, d'un *incident de cybersécurité* qui constitue une tentative de compromettre un système indiqué à la colonne	L'entité responsable n'a pas avisé l'E-ISAC ou le NCCIC, ou leurs remplaçants éventuels, d'un *incident de cybersécurité* qui constitue, selon les critères prescrits à l'alinéa 1.2.1 de	L'entité responsable a avisé l'E-ISAC et le NCCIC, ou leurs remplaçants éventuels, d'un *incident de cybersécurité à déclarer*, mais ne les a pas avisés dans les délais prescrits à l'alinéa 4.2. (4.2)	L'entité responsable n'a avisé ni l'E-ISAC, ni le NCCIC, ou leurs remplaçants éventuels, d'un *incident de cybersécurité à déclarer*. (R4)

Ex.	Horizon	VRF	Niveau de gravité de la non-conformité (VSL) (CIP-008-6)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
			« Systèmes visés » de l'alinéa 4.2, mais sans respecter les délais prescrits à l'alinéa 4.2. (4.2) OU L'entité responsable a avisé l'E-ISAC et le NCCIC, ou leurs remplaçants éventuels, d'un *incident de cybersécurité à déclarer* ou d'un *incident de cybersécurité* qui constitue une tentative de compromettre un système indiqué à la colonne « Systèmes visés » de l'alinéa 4.3, mais n'a pas transmis, dans un délai de 7 jours civils après les avoir déterminés, un ou plusieurs des éléments exigés à l'alinéa 4.1, mais non encore déclarés. (4.3) OU L'entité responsable a avisé l'E-ISAC et le NCCIC, ou leurs remplaçants éventuels, d'un *incident de cybersécurité à déclarer* ou d'un *incident de cybersécurité* qui constitue une tentative de compromettre un système indiqué à la colonne	l'exigence E1, une tentative de compromettre un système indiqué à la colonne « Systèmes visés ». (E4)	OU L'entité responsable n'a pas avisé l'E-ISAC ou le NCCIC, ou leurs remplaçants éventuels, d'un *incident de cybersécurité à déclarer*. (E4)	

Ex.	Horizon	VRF	Niveau de gravité de la non-conformité (VSL) (CIP-008-6)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
			« Systèmes visés » de l'alinéa 4.1, mais n'a pas déclaré un ou plusieurs des éléments exigés à l'alinéa 4.1 après les avoir déterminés. (4.1)			

D. Différences régionales

Aucune.

E. Interprétations

Aucune.

F. Documents connexes

Aucun.

Historique des versions

Version	Date	Modification apportée	Suivi des modifications
1	16 janvier 2006	E3.2 — Remplacement de « Control Center » par « control center ».	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. Suppression de la mention sur la prise en compte des considérations d'affaires raisonnables. Remplacement de l'organisation régionale de fiabilité par l'entité régionale comme entité responsable. Reformulation de la date d'entrée en vigueur. Remplacement de « Responsabilité de la surveillance de la conformité » par « Responsable de la surveillance de l'application des normes ».	
3		Changement du numéro de version de -2 à -3. 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.	
3	16 décembre 2009	Approbation par le Conseil d'administration de la NERC.	Mise à jour
3	31 mars 2010	Approbation par la FERC.	
4	30 décembre 2010	Ajout de critères précis pour l'identification des *actifs critiques*.	Mise à jour
4	24 janvier 2011	Approbation par le Conseil d'administration de la NERC.	Mise à jour

Version	Date	Modification apportée	Suivi des modifications
5	26 novembre 2012	Adoption par le Conseil d'administration de la NERC.	Modifiée en coordination avec les autres normes CIP et révision du format selon le gabarit RBS.
5	22 novembre 2013	Ordonnance de la FERC approuvant la norme CIP-008-5.	
5	9 juillet 2014	Ordonnance de la FERC approuvant les révisions aux VRF et aux VSL de certaines normes CIP.	Exigence E2 de la norme CIP-008-5, tableau des VSL sous Critique, changé de 19 à 18 mois civils.
6	6 février 2019	Adoption par le Conseil d'administration de la NERC.	Changements en réponse aux prescriptions de l'Ordonnance 848 de la FERC.

A. Introduction

1. **Titre :** Cybersécurité — Gestion des changements de configuration et analyses de vulnérabilité

2. **Numéro :** CIP-010-3

3. **Objet :** Prévenir et détecter les changements non autorisés aux *systèmes électroniques BES* au moyen d'exigences relatives à la gestion des changements de configuration et aux analyses de vulnérabilité, afin de protéger les *systèmes électroniques BES* contre les compromissions qui pourraient entraîner un fonctionnement incorrect ou des instabilités dans le *système de production-transport d'électricité* (*BES*).

4. **Applicabilité :**

   4.1. Entités fonctionnelles : Dans le contexte de la présente norme, les entités fonctionnelles indiquées ci-après sont appelées collectivement « entités responsables ». Si certaines exigences visent plus spécifiquement une entité fonctionnelle ou un sous-ensemble 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 systèmes, *installations* et équipements suivants pour la protection ou la remise en charge du *BES* :

   4.1.2.1. Système de délestage de *charge* en sous-fréquence (DSF) ou 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 des délestages automatiques de *charge* de 300 MW ou plus sous la commande d'un système commun détenu par l'entité responsable, sans intervention humaine.

   4.1.2.2. *Automatisme de réseau* (*RAS*) visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou de l'*entité régionale*.

   4.1.2.3. *Système de protection* de réseau de *transport* (à l'exclusion des systèmes de DSF et de DST) visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou de l'*entité régionale*.

   4.1.2.4. *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 de la présente norme, les systèmes, *installations* et équipements suivants détenus par une entité responsable indiquée à la section 4.1 sont visés par les exigences. Si certaines exigences visent plus spécifiquement un type ou un sous-ensemble de systèmes, d'*installations* ou d'équipements, ceux-ci sont précisés explicitement.

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

4.2.1.1. 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 des délestages de *charge* automatiques de 300 MW ou plus sous la commande d'un système commun détenu par l'entité responsable, sans intervention humaine.

4.2.1.2. *Automatisme de réseau* (*RAS*) visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou de l'*entité régionale*.

4.2.1.3. *Système de protection* de réseau de transport (à l'exclusion des systèmes de DSF et de DST) visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou de l'*entité régionale*.

4.2.1.4. *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* :

4.2.2.1. Toutes les *installations* du *BES*.

4.2.3. Exemptions : Sont exemptés de la norme CIP-010-3 :

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 électronique* 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 ont déterminent n'avoir aucun *système électroniques BES* classé dans les catégories « impact élevé » ou « impact moyen » selon le processus d'inventaire et de catégorisation de la norme CIP-002-5.

5. Dates d'entrée en vigueur :

Voir le plan de mise en œuvre du projet 2016-03.

6. Contexte :

La norme CIP-010 fait partie d'une série de normes CIP sur la cybersécurité qui exigent l'inventaire et la catégorisation initiales des *systèmes électroniques BES* ainsi qu'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 de DSF et de DST. Ce seuil particulier de 300 MW pour les systèmes de DSF et de DST provient de la version 1 des normes CIP sur la cybersécurité. Le seuil demeure à 300 MW puisqu'il concerne spécifiquement les systèmes de DST et de DSF, qui constituent des efforts de dernier recours pour sauver le *BES*. Un examen des tolérances des systèmes de 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 de 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. L'équipe de rédaction (SDT) CSO706 a adapté ce concept à partir du cadre de gestion des risques du National Institute of Standards and Technology (NIST) en vue d'établir une méthode d'application des exigences qui tient compte plus adéquatement de l'impact et des caractéristiques de connectivité. La colonne « Systèmes visés » repose sur les conventions suivantes :

- ***Systèmes électroniques BES* à impact élevé –** Désigne les *systèmes électroniques BES* classés dans la catégorie « impact élevé », selon les processus d'inventaire 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 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 physiques* associés à un *système électronique BES* à impact élevé ou moyen visé à *connectivité externe routable*.
- ***Actifs électroniques protégés* (*PCA*) –** Désigne tout *actif électronique protégé* associé à un *système électronique BES* à impact élevé ou moyen visé.

B. Exigences et mesures

E1. Chaque entité responsable doit mettre en œuvre un ou plusieurs processus documentés qui, collectivement, couvrent tous les alinéas applicables du tableau E1 (CIP-010-3) – Gestion des changements de configuration.
[Facteur de risque de non-conformité : moyen] [Horizon : planification de l'exploitation].

M1. Les pièces justificatives doivent comprendre chacun des processus documentés applicables qui, collectivement, couvrent tous les alinéas applicables du tableau E1 (CIP-010-3) – Gestion des changements de configuration ; d'autres pièces justificatives doivent attester la mise en œuvre, selon la colonne Mesures du tableau.

Tableau E1 (CIP-010-3) – Gestion des changements de configuration			
Alinéa	**Systèmes visés**	**Exigences**	**Mesures**
1.1	*Systèmes électroniques BES* à impact élevé et : 1. les *EACMS* associés ; 2. les *PACS* associés ; et 3. les *PCA* associés. *Systèmes électroniques BES* à impact moyen et : 1. les *EACMS* associés ; 2. les *PACS* associés ; et 3. les *PCA* associés.	Établir une configuration de référence, individuellement ou par groupe, qui doit comprendre les éléments suivants : 1.1.1. le ou les systèmes d'exploitation (y compris la version), ou tout système embarqué en l'absence de système d'exploitation indépendant ; 1.1.2. tout logiciel commercial ou logiciel libre (y compris la version) installé intentionnellement ; 1.1.3. tout logiciel personnalisé installé ; 1.1.4. tout port logique accessible par le réseau ; et 1.1.5. tout correctif de sécurité appliqué.	Exemples non limitatifs de pièces justificatives : • feuille de calcul indiquant les éléments de configuration de référence requis pour chaque *actif électronique*, individuellement ou par groupe ; ou • enregistrement dans un système de gestion d'actifs indiquant les éléments de configuration de référence requis pour chaque *actif électronique*, individuellement ou par groupe.

Tableau E1 (CIP-010-3) – Gestion des changements de configuration			
Alinéa	**Systèmes visés**	**Exigences**	**Mesures**
1.2	*Systèmes électroniques BES* à impact élevé et : 1. les *EACMS* associés ; 2. les *PACS* associés ; et 3. les *PCA* associés. *Systèmes électroniques BES* à impact moyen et : 1. les *EACMS* associés ; 2. les *PACS* associés ; et 3. les *PCA* associés.	Autoriser et documenter tout changement par rapport à la configuration de référence existante.	Exemples non limitatifs de pièces justificatives : • pour chaque changement, l'enregistrement dans un système de gestion des changements de la demande de changement et de l'autorisation électronique correspondante (accordée par une personne ou un groupe dûment habilité) ; ou • documentation attestant que le changement a été effectué conformément à l'exigence.
1.3	*Systèmes électroniques BES* à impact élevé et : 1. les *EACMS* associés ; 2. les *PACS* associés ; et 3. les *PCA* associés. *Systèmes électroniques BES* à impact moyen et : 1. les *EACMS* associés ; 2. les *PACS* associés ; et 3. les *PCA* associés.	Pour tout changement par rapport à la configuration de référence existante, mettre à jour la configuration de référence dans les 30 jours civils suivant l'exécution du changement.	Exemple non limitatif de pièce justificative : documentation de la configuration de référence avec mise à jour datée d'au plus 30 jours civils après la date d'exécution du changement.

Tableau E1 (CIP-010-3) – Gestion des changements de configuration			
Alinéa	**Systèmes visés**	**Exigences**	**Mesures**
1.4	*Systèmes électroniques BES* à impact élevé et : 1. les *EACMS* associés ; 2. les *PACS* associés ; et 3. les *PCA* associés. *Systèmes électroniques BES* à impact moyen et : 1. les *EACMS* associés ; 2. les *PACS* associés ; et 3. les *PCA* associés.	Pour tout changement par rapport à la configuration de référence existante : 1.4.1. avant le changement, déterminer les mécanismes de cybersécurité des normes CIP-005 et CIP-007 qui pourraient être touchés par le changement ; 1.4.2. après le changement, vérifier que les mécanismes de cybersécurité déterminés en 1.4.1 ne sont pas dégradés ; et 1.4.3. documenter les résultats de la vérification.	Exemple non limitatif de pièce justificative : liste de mécanismes de cybersécurité vérifiés ou mis à l'essai, avec résultats d'essai datés.

Tableau E1 (CIP-010-3) – Gestion des changements de configuration			
Alinéa	**Systèmes visés**	**Exigences**	**Mesures**
1.5	*Systèmes électroniques BES* à impact élevé.	Pour chaque changement par rapport à la configuration de référence existante, dans la mesure où c'est techniquement faisable : 1.5.1. avant de mettre en œuvre un changement dans l'environnement de production, mettre à l'essai le changement dans un environnement d'essai ou mettre à l'essai le changement dans un environnement de production où l'essai est effectué d'une manière qui réduit au minimum les effets adverses, en simulant la configuration de référence de manière à s'assurer que les mécanismes de cybersécurité des normes CIP-005 et CIP-007 ne sont pas dégradés ; et 1.5.2. documenter les résultats des essais et, si un environnement d'essai a été utilisé, les différences entre celui-ci et l'environnement de production, y compris la description des mesures visant à tenir compte des différences de fonctionnement entre les environnements d'essai et de production.	Exemples non limitatifs de pièces justificatives : liste des mécanismes de cybersécurité mis à l'essai avec résultats d'essai concluants, liste de différences entre les environnements d'essai et de production et description des mesures visant à tenir compte des différences de fonctionnement, y compris la date de l'essai.

Tableau E1 (CIP-010-3) – Gestion des changements de configuration			
Alinéa	**Systèmes visés**	**Exigences**	**Mesures**
1.6	*Systèmes électroniques BES* à impact élevé *Systèmes électroniques BES* à impact moyen Remarque : La mise en œuvre d'un plan n'oblige pas l'entité responsable à renégocier ou à résilier des contrats existants (y compris les modifications aux ententes-cadres ou les bons de commande). En outre, la partie 1.6 ne s'étend pas : 1) aux modalités mêmes d'un contrat d'approvisionnement ; et 2) à l'exécution et au respect du contrat par le fournisseur.	Avant tout changement touchant les éléments de la configuration de référence spécifiés aux alinéas 1.1.1, 1.1.2 et 1.1.5 par rapport à la configuration existante, dans la mesure où la source d'un logiciel met les méthodes appropriées à la disposition de l'entité responsable : 1.6.1. vérifier l'identité de la source du logiciel ; et 1.6.2. vérifier l'intégrité du logiciel obtenu de la source du logiciel.	Exemples non limitatifs de pièces justificatives : enregistrement d'une demande de changement qui atteste que l'identité de la source du logiciel et l'intégrité du logiciel ont été vérifiées avant le changement à la configuration de référence ; ou processus qui documente les mécanismes en place pour assurer la vérification automatique de l'identité de la source du logiciel et de l'intégrité du logiciel.

E2. Chaque entité responsable doit mettre en œuvre un ou plusieurs processus documentés qui, collectivement, couvrent tous les alinéas applicables du tableau E2 (CIP-010-3) – Surveillance de la configuration.
[Facteur de risque de non-conformité : moyen] [Horizon : planification de l'exploitation].

M2. Les pièces justificatives doivent comprendre chacun des processus documentés applicables qui, collectivement, couvrent tous les alinéas applicables du tableau E2 (CIP-010-3) – Surveillance de la configuration ; d'autres pièces justificatives doivent attester la mise en œuvre, selon la colonne Mesures du tableau.

Tableau E2 (CIP-010-3) – Surveillance de la configuration			
Alinéa	**Systèmes visés**	**Exigences**	**Mesures**
2.1	*Systèmes électroniques BES* à impact élevé et : 1. les *EACMS* associés ; et 2. les *PCA* associés.	Au moins une fois tous les 35 jours civils, vérifier s'il y a eu des changements à la configuration de référence (décrite à l'alinéa 1.1 de l'exigence E1). Documenter tout changement non autorisé détecté et faire enquête.	Exemples non limitatifs de pièces justificatives : registres d'un système de surveillance de configuration et dossiers d'enquête pour tout changement non autorisé détecté.

E3. Chaque entité responsable doit mettre en œuvre un ou plusieurs processus documentés qui, collectivement, couvrent tous les alinéas applicables du tableau E3 (CIP-010-3) – Analyses de vulnérabilité.
[Facteur de risque de non-conformité : moyen] [Horizon : planification à long terme et planification de l'exploitation]

M3. Les pièces justificatives doivent comprendre chacun des processus documentés applicables qui, collectivement, couvrent tous les alinéas applicables du tableau E3 (CIP-010-3) – Analyses de vulnérabilité ; d'autres pièces justificatives doivent attester la mise en œuvre, selon la colonne Mesures du tableau.

Tableau E3 (CIP-010-3) – Analyses de vulnérabilité			
Alinéa	**Systèmes visés**	**Exigences**	**Mesures**
3.1	*Systèmes électroniques BES* à impact élevé et : 1. les *EACMS* associés ; 2. les *PACS* associés ; et 3. les *PCA* associés. *Systèmes électroniques BES* à impact moyen et : 1. les *EACMS* associés ; 2. les *PACS* associés ; et 3. les *PCA* associés.	Au moins tous les 15 mois civils, effectuer une analyse de vulnérabilité sur papier ou active.	Exemples non limitatifs de pièces justificatives : • document indiquant la date de l'analyse (effectuée au moins une fois tous les 15 mois civils), les mécanismes évalués pour chaque *système électronique BES* et la méthode d'analyse ; ou • document indiquant la date de l'analyse et le résultat produit par tout outil utilisé pour l'analyse.

Tableau E3 (CIP-010-3) – Analyses de vulnérabilité			
Alinéa	**Systèmes visés**	**Exigences**	**Mesures**
3.2	*Systèmes électroniques BES* à impact élevé.	Au moins une fois tous les 36 mois civils, dans la mesure où c'est techniquement faisable : 3.2.1 effectuer une analyse de vulnérabilité active dans un environnement d'essai, ou effectuer une analyse de vulnérabilité active dans un environnement de production où l'essai est réalisé d'une manière qui réduit au minimum les effets adverses, en simulant la configuration de référence du *système électronique BES* dans un environnement de production ; et 3.2.2 documenter les résultats des essais et, si un environnement d'essai a été utilisé, les différences entre celui-ci et l'environnement de production, y compris la description des mesures visant à tenir compte des différences de fonctionnement entre les environnements d'essai et de production.	Exemples non limitatifs de pièces justificatives : document indiquant la date de l'analyse (effectuée au moins une fois tous les 36 mois civils), résultat produit par les outils utilisés pour effectuer l'analyse et liste des différences entre les environnements de production et d'essai, avec explications sur la prise en compte des différences dans l'analyse.

Tableau E3 (CIP-010-3) – Analyses de vulnérabilité			
Alinéa	**Systèmes visés**	**Exigences**	**Mesures**
3.3	*Systèmes électroniques BES* à impact élevé et : 1. les *EACMS* associés ; 2. les *PCA* associés.	Avant d'ajouter un nouvel *actif électronique* visé à un environnement de production, effectuer une analyse de vulnérabilité active du nouvel *actif électronique*, sauf dans des *circonstances CIP exceptionnelles* ou pour un remplacement d'un *actif électronique* existant par un équivalent dont la configuration de référence simule celle de l'*actif électronique* remplacé ou d'un autre *actif électronique* existant.	Exemples non limitatifs de pièces justificatives : document indiquant la date de l'analyse (effectuée avant la mise en service du nouvel *actif électronique*) et le résultat produit par les outils utilisés pour l'analyse.
3.4	*Systèmes électroniques BES* à impact élevé et : 1. les *EACMS* associés ; 2. les *PACS* associés ; et 3. les *PCA* associés. *Systèmes électroniques BES* à impact moyen et : 1. les *EACMS* associés ; 2. les *PACS* associés ; et 3. les *PCA* associés.	Documenter les résultats des analyses effectuées conformément aux alinéas 3.1, 3.2 et 3.3 ainsi que le plan d'action visant à corriger ou à atténuer les vulnérabilités constatées lors des analyses, en précisant la date prévue d'achèvement du plan d'action et l'état d'exécution de toute mesure de correction ou d'atténuation.	Exemples non limitatifs de pièces justificatives : document donnant les résultats de l'examen ou de l'analyse, liste des mesures à prendre, dates proposées d'achèvement du plan d'action et dossier de l'état d'exécution des mesures à prendre (procès-verbaux de réunion d'étape, mises à jour dans un système d'ordres de travail, suivi des mesures au moyen d'une feuille de calcul, etc.).

E4. Chaque entité responsable, pour ses *systèmes électroniques BES* à impact moyen et élevé ainsi que les *actifs électroniques protégés* connexes, doit mettre en œuvre (sauf dans des *circonstances CIP exceptionnelles*) un ou plusieurs plans documentés concernant les *actifs électroniques temporaires* et les *supports de stockage amovibles* ; ces plans doivent être conformes aux sections de l'annexe 1.
[Facteur de risque de non-conformité : moyen] [Horizon : planification à long terme et planification de l'exploitation]

M4. Les pièces justificatives doivent comprendre chacun des plans documentés qui concernent les *actifs électroniques temporaires* et les *supports de stockage amovibles* et qui, collectivement, couvrent toutes les sections applicables de l'annexe 1 ; d'autres pièces justificatives doivent attester la mise en œuvre de ces plans. D'autres exemples de pièces justificatives pour les différentes sections sont présentés à l'annexe 2. Si une entité responsable n'utilise pas d'*actifs électroniques temporaires* ni de *supports de stockage amovibles*, les pièces justificatives appropriées peuvent comprendre, sans limitation, une déclaration, une politique ou tout autre document affirmant que l'entité responsable n'utilise pas d'*actifs électroniques temporaires* ou de *supports de stockage amovibles.*

C. Conformité

1. Processus de surveillance de la conformité

1.1. Responsable des mesures pour assurer la conformité

Le terme « *responsable des mesures pour assurer la conformité* » (*CEA*) désigne la NERC ou l'*entité régionale*, ou toute entité désignée par un organisme gouvernemental pertinent, dans leurs rôles respectifs visant à surveiller et à assurer la conformité avec les normes de fiabilité obligatoires et exécutoires 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 visée 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 visée doit conserver des pièces justificatives pour chaque exigence de la présente norme pendant trois années civiles.
- Si une entité visée 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. Programme de surveillance et de mise en application des normes

Selon la définition des règles de procédure de la NERC, l'expression « programme de surveillance de la conformité » désigne la liste des processus qui serviront à évaluer les données ou l'information afin de déterminer les résultats de conformité avec la norme de fiabilité.

Niveau de gravité de la non-conformité (VSL)

Ex.	Niveau de gravité de la non-conformité (CIP-010-3)			
	VSL faible	VSL modéré	VSL élevé	VSL critique
E1.	L'entité responsable a documenté et mis en œuvre un ou des processus de gestion des changements de configuration qui comprennent seulement quatre des éléments de référence exigés en 1.1.1 à 1.1.5. (1.1)	L'entité responsable a documenté et mis en œuvre un ou des processus de gestion des changements de configuration qui comprennent seulement trois des éléments de référence exigés en 1.1.1 à 1.1.5. (1.1)	L'entité responsable a documenté et mis en œuvre un ou des processus de gestion des changements de configuration qui comprennent seulement deux des éléments de référence exigés en 1.1.1 à 1.1.5. (1.1) OU L'entité responsable a un processus conforme à l'alinéa 1.6 pour vérifier l'identité de la source du logiciel (1.6.1), mais n'a pas de processus conforme à l'alinéa 1.6 pour vérifier l'intégrité du logiciel obtenu de la source du logiciel alors que la méthode appropriée est mise à la disposition de l'entité responsable par la source du logiciel (1.6.2).	L'entité responsable n'a documenté ou mis en œuvre aucun processus de gestion des changements de configuration. (E1) OU L'entité responsable a documenté et mis en œuvre un ou des processus de gestion des changements de configuration qui comprennent seulement un des éléments de référence exigés en 1.1.1 à 1.1.5. (1.1) OU L'entité responsable n'a pas de processus qui exige l'autorisation et la documentation des changements par rapport à la configuration de référence existante. (1.2) OU L'entité responsable n'a pas de processus pour mettre à jour la configuration de référence dans les 30 jours civils suivant l'exécution de changements par rapport à la configuration de référence existante. (1.3) OU

Ex.	Niveau de gravité de la non-conformité (CIP-010-3)			
	VSL faible	VSL modéré	VSL élevé	VSL critique
				L’entité responsable n’a pas de processus pour déterminer les mécanismes de sécurité exigés par les normes CIP-005 et CIP-007 qui pourraient être touchés par des changements par rapport à la configuration de référence existante. (1.4.1) OU L’entité responsable a un ou des processus pour déterminer les mécanismes de sécurité exigés par les normes CIP-005 et CIP-007 qui pourraient être touchés par des changements par rapport à la configuration de référence existante, mais elle n’a pas vérifié et documenté que les mécanismes exigés n’étaient pas dégradés par suite du changement. (1.4.2 et 1.4.3) OU L’entité responsable n’a pas de processus pour mettre à l’essai les changements dans un environnement qui simule la configuration de référence avant de mettre en œuvre un changement par rapport à la configuration de référence. (1.5.1) OU

Ex.	Niveau de gravité de la non-conformité (CIP-010-3)			
	VSL faible	VSL modéré	VSL élevé	VSL critique
				L'entité responsable n'a pas de processus pour documenter les résultats de l'essai et, si un environnement d'essai a été utilisé, pour documenter les différences entre les environnements d'essai et de production. (1.5.2) OU L'entité responsable n'a pas de processus conforme à l'alinéa 1.6 ni pour vérifier l'identité de la source du logiciel, ni pour vérifier l'intégrité du logiciel obtenu de la source du logiciel, alors que les méthodes appropriées sont mises à la disposition de l'entité responsable par la source du logiciel. (1.6)
E2.	Sans objet	Sans objet	Sans objet	L'entité responsable n'a pas documenté ou mis en œuvre de processus pour vérifier, au moins une fois tous les 35 jours civils, s'il y a eu des changements non autorisés à la configuration de référence, pour documenter ceux-ci et pour faire enquête. (2.1)
E3.	L'entité responsable a mis en œuvre un ou plusieurs processus documentés d'analyse de vulnérabilité pour chacun de ses *systèmes électroniques BES*	L'entité responsable a mis en œuvre un ou plusieurs processus documentés d'analyse de vulnérabilité pour chacun de ses *systèmes électroniques BES*	L'entité responsable a mis en œuvre un ou plusieurs processus documentés d'analyse de vulnérabilité pour chacun de ses *systèmes électroniques BES*	L'entité responsable n'a mis en œuvre aucun processus d'analyse de vulnérabilité pour un de

Ex.	Niveau de gravité de la non-conformité (CIP-010-3)			
	VSL faible	VSL modéré	VSL élevé	VSL critique
	visés, mais elle a effectué une analyse de vulnérabilité dans un délai de plus de 15 mois et de moins de 18 mois suivant la dernière analyse de l'un de ses *systèmes électroniques BES* visés. (3.1) OU L'entité responsable a mis en œuvre un ou plusieurs processus documentés d'analyse de vulnérabilité active pour les systèmes visés, mais elle a effectué une analyse de vulnérabilité active dans un délai de plus de 36 mois et de moins de 39 mois suivant la dernière analyse active de l'un de ses *systèmes électroniques BES* visés. (3.2)	visés, mais elle a effectué une analyse de vulnérabilité dans un délai de plus de 18 mois et de moins de 21 mois suivant la dernière analyse de l'un de ses *systèmes électroniques BES* visés. (3.1) OU L'entité responsable a mis en œuvre un ou plusieurs processus documentés d'analyse de vulnérabilité active pour les systèmes visés, mais elle a effectué une analyse de vulnérabilité active dans un délai de plus de 39 mois et de moins de 42 mois suivant la dernière analyse active de l'un de ses *systèmes électroniques BES* visés. (3.2)	visés, mais elle a effectué une analyse de vulnérabilité dans un délai de plus de 21 mois et de moins de 24 mois suivant la dernière analyse de l'un de ses *systèmes électroniques BES* visés. (3.1) OU L'entité responsable a mis en œuvre un ou plusieurs processus documentés d'analyse de vulnérabilité active pour les systèmes visés, mais elle a effectué une analyse de vulnérabilité active dans un délai de plus de 42 mois et de moins de 45 mois suivant la dernière analyse active de l'un de ses *systèmes électroniques BES* visés. (3.2)	ses *systèmes électroniques BES* visés. (E3) OU L'entité responsable a mis en œuvre un ou plusieurs processus documentés d'analyse de vulnérabilité pour chacun de ses *systèmes électroniques BES* visés, mais elle a effectué une analyse de vulnérabilité plus de 24 mois suivant la dernière analyse de l'un de ses *systèmes électroniques BES* visés. (3.1) OU L'entité responsable a mis en œuvre un ou plusieurs processus documentés d'analyse de vulnérabilité active pour les systèmes visés, mais elle a effectué une analyse de vulnérabilité active dans un délai de plus de 45 mois suivant la dernière analyse active de l'un de ses *systèmes électroniques BES* visés. (3.2) OU L'entité responsable a mis en œuvre et documenté un ou plusieurs processus d'analyse de vulnérabilité pour chacun de ses *systèmes électroniques BES* visés, mais elle n'a pas effectué

Ex.	Niveau de gravité de la non-conformité (CIP-010-3)			
	VSL faible	**VSL modéré**	**VSL élevé**	**VSL critique**
				l'analyse de vulnérabilité active d'une manière qui simule une configuration de référence existante de ses *systèmes électroniques BES* visés. (3.3) OU L'entité responsable a mis en œuvre un ou plusieurs processus documentés d'analyse de vulnérabilité pour chacun de ses *systèmes électroniques BES* visés, mais elle n'a pas documenté les résultats des analyses de vulnérabilité, les plans d'action pour corriger ou atténuer les vulnérabilités constatées dans les analyses, la date planifiée d'achèvement du plan d'action et l'état d'exécution des plans d'atténuation. (3.4)
E4.	L'entité responsable a documenté son ou ses plans concernant les *actifs électroniques temporaires* et les *supports de stockage amovibles*, mais n'a pas géré ses *actifs électroniques temporaires* conformément à la section 1.1 de l'annexe 1 complémentaire à l'exigence E4 de la norme CIP-010-3. (E4) OU	L'entité responsable a documenté son ou ses plans concernant les *actifs électroniques temporaires* et les *supports de stockage amovibles*, mais n'a pas mis en œuvre les mesures applicables aux *supports de stockage amovibles* conformément à la section 3 de l'annexe 1 complémentaire à l'exigence E4 de la norme CIP-010-3. (E4)	L'entité responsable a documenté son ou ses plans concernant les *actifs électroniques temporaires* et les *supports de stockage amovibles*, mais n'a pas établi les autorisations relatives aux *actifs électroniques temporaires* conformément à la section 1.2 de l'annexe 1 complémentaire à l'exigence E4 de la norme CIP-010-3. (E4)	L'entité responsable n'a pas documenté ou mis en œuvre un ou plusieurs plans concernant les *actifs électroniques temporaires* et les *supports de stockage amovibles* conformément à l'exigence E4 de la norme CIP-010-3. (E4)

Ex.	Niveau de gravité de la non-conformité (CIP-010-3)			
	VSL faible	**VSL modéré**	**VSL élevé**	**VSL critique**
	L'entité responsable a documenté son ou ses plans concernant les *actifs électroniques temporaires* et les *supports de stockage amovibles*, mais n'a pas documenté les mesures applicables aux *supports de stockage amovibles* conformément à la section 3 de l'annexe 1 complémentaire à l'exigence E4 de la norme CIP-010-3. (E4) OU L'entité responsable a documenté son ou ses plans concernant les *actifs électroniques temporaires* et les *supports de stockage amovibles*, mais n'a pas documenté les autorisations relatives aux *actifs électroniques temporaires* qu'elle gère elle-même conformément à la section 1.2 de l'annexe 1 complémentaire à l'exigence E4 de la norme CIP-010-3. (E4)	OU L'entité responsable a documenté son ou ses plans concernant les *actifs électroniques temporaires* et les *supports de stockage amovibles*, mais n'a pas documenté les mesures d'atténuation du risque lié aux vulnérabilités logicielles, à l'introduction de programmes malveillants ou aux utilisations non autorisées pour des *actifs électroniques temporaires* gérés par l'entité responsable conformément aux sections 1.3, 1.4 et 1.5 de l'annexe 1 complémentaire à l'exigence E4 de la norme CIP-010-3. (E4) OU L'entité responsable a documenté son ou ses plans concernant les *actifs électroniques temporaires* et les *supports de stockage amovibles*, mais n'a pas documenté les mesures d'atténuation du risque lié aux vulnérabilités logicielles ou à l'introduction de programmes malveillants pour des *actifs électroniques temporaires* gérés par une tierce partie conformément aux sections 2.1, 2.2 et 2.3 de l'annexe 1	OU L'entité responsable a documenté son ou ses plans concernant les *actifs électroniques temporaires* et les *supports de stockage amovibles*, mais n'a pas mis en œuvre les mesures d'atténuation du risque lié aux vulnérabilités logicielles, à l'introduction de programmes malveillants ou aux utilisations non autorisées pour des *actifs électroniques temporaires* gérés par l'entité responsable conformément aux sections 1.3, 1.4 et 1.5 de l'annexe 1 complémentaire à l'exigence E4 de la norme CIP-010-3. (E4) OU L'entité responsable a documenté son ou ses plans concernant les *actifs électroniques temporaires* et les *supports de stockage amovibles*, mais n'a pas mis en œuvre les mesures d'atténuation du risque lié aux vulnérabilités logicielles ou à l'introduction de programmes malveillants pour des *actifs électroniques temporaires* gérés par une tierce partie conformément aux sections 2.1, 2.2 et 2.3 de l'annexe 1	

Ex.	Niveau de gravité de la non-conformité (CIP-010-3)			
	VSL faible	VSL modéré	VSL élevé	VSL critique
		complémentaire à l'exigence E4 de la norme CIP-010-3. (E4)	complémentaire à l'exigence E4 de la norme CIP-010-3. (E4)	

D. Différences régionales

Aucune.

E. Documents connexes

Aucun.

Historique des versions

Version	Date	Intervention	Suivi des modifications
1	26 novembre 2012	Adoption par le Conseil d'administration de la NERC.	Cette norme encadre la gestion des changements de configuration et des analyses de vulnérabilité en coordination avec d'autres normes CIP et met en œuvre certaines dispositions de l'ordonnance 706 de la FERC.
1	22 novembre 2013	Ordonnance de la FERC approuvant la norme CIP-010-1. (L'ordonnance entre en vigueur le 3 février 2014.)	
2	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.
2	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 *systèmes électroniques BES* à impact faible.
2	21 janvier 2016	Ordonnance de la FERC approuvant la norme CIP-010-3. Dossier RM15-14-000	
3	20 juillet 2017	Modifications visant à répondre à certaines directives de l'Ordonnance 829 de la FERC.	Révision
3	10 août 2017	Adoption par le Conseil d'administration de la NERC.	
3	18 octobre 2018	Ordonnance de la FERC approuvant la norme CIP-010-3. Dossier RM17-13-000.	

CIP-010-3 – Annexe 1

Exigences détaillées des plans concernant les *actifs électroniques temporaires* et les *supports de stockage amovibles*

Les entités responsables doivent intégrer chacune des sections suivantes à leurs plans, prescrits à l'exigence E4, concernant les *actifs électroniques temporaires* et les *supports de stockage amovibles*.

Section 1. *Actifs électroniques temporaires* gérés par l'entité responsable.

1.1. Gestion des *actifs électroniques temporaires* : Les entités responsables doivent gérer leurs *actifs électroniques temporaires*, individuellement ou par groupe : 1) en permanence, afin d'assurer la conformité avec les exigences pertinentes en tout temps ; 2) à la demande, en appliquant les exigences pertinentes avant d'établir la connexion à un système électronique BES ; ou 3) selon une combinaison des moyens 1) et 2) ci-dessus.

1.2. Autorisations relatives aux *actifs électroniques temporaires* : Pour chaque *actif électronique temporaire* ou groupe d'*actifs électroniques temporaires*, chaque entité responsable doit autoriser :

1.1.1. les utilisateurs (individuellement, par groupe ou par rôle) ;

1.1.2. les emplacements (individuellement ou par groupe) ; et

1.1.3. les utilisations, qui doivent être limitées aux actions nécessaires pour assurer les fonctions opérationnelles.

1.3. Atténuation du risque lié aux vulnérabilités logicielles : Utiliser un ou plusieurs des moyens suivants pour réaliser l'objectif d'atténuer le risque lié aux vulnérabilités présentées par des logiciels sans correctifs dans l'*actif électronique temporaire* (selon les capacités de ce dernier) :

- application de correctifs, manuellement ou par mises à jour systématiques ;
- systèmes d'exploitation et logiciels exécutables uniquement à partir de supports non inscriptibles ;
- renforcement du système d'exploitation ; ou
- autres moyens d'atténuer le risque lié aux vulnérabilités logicielles.

1.4. Atténuation du risque lié à l'introduction de programmes malveillants : Utiliser un ou plusieurs des moyens suivants pour réaliser l'objectif d'atténuer le risque lié à l'introduction de programmes malveillants (selon les capacités de l'*actif électronique temporaire*) :

- logiciel antivirus, avec mises à jour manuelles ou systématiques des signatures ou des séquences de code ;
- liste blanche d'applications ; ou
- autres moyens d'atténuer le risque lié à l'introduction de programmes malveillants.

1.5. Atténuation du risque lié aux utilisations non autorisées : Utiliser un ou plusieurs des moyens suivants pour réaliser l'objectif d'atténuer le risque lié aux utilisations non autorisées d'*actifs électroniques temporaires* :

- restriction de l'accès physique ;

- cryptage de disque intégral avec authentification ;
- authentification multifactorielle ; ou
- autres moyens d'atténuer le risque lié aux utilisations non autorisées.

Section 2. *Actifs électroniques temporaires* gérés par une tierce partie autre que l'entité responsable.

2.1. Atténuation du risque lié aux vulnérabilités logicielles : Utiliser un ou plusieurs des moyens suivants pour réaliser l'objectif d'atténuer le risque lié aux vulnérabilités présentées par les logiciels sans correctifs dans l'*actif électronique temporaire* (selon les capacités de ce dernier) :

- examen des correctifs de sécurité installés ;
- examen de la procédure d'application des correctifs par la tierce partie ;
- examen d'autres mesures d'atténuation du risque lié aux vulnérabilités logicielles adoptées par la tierce partie ; ou
- autres moyens d'atténuer le risque lié aux vulnérabilités logicielles.

2.2. Atténuation du risque lié à l'introduction de programmes malveillants : Utiliser un ou plusieurs des moyens suivants pour réaliser l'objectif d'atténuer le risque lié à l'introduction programmes malveillants (selon les capacités de l'*actif électronique temporaire*) :

- examen du degré de maintien à jour de l'antivirus ;
- examen de la procédure de mise à jour de l'antivirus adoptée par la tierce partie ;
- examen de l'utilisation par la tierce partie de listes blanches d'applications ;
- examen de l'utilisation de systèmes d'exploitation et de logiciels exécutables uniquement à partir de supports non inscriptibles ;
- examen des mesures de renforcement du système d'exploitation adoptées par la tierce partie ; ou
- autres moyens d'atténuation du risque lié aux programmes malveillants.

2.3. Pour tout moyen d'atténuation du risque lié aux vulnérabilités logicielles ou à l'introduction de programmes malveillants mis en œuvre conformément aux alinéas 2.1 et 2.2, l'entité responsable doit déterminer si d'autres mesures d'atténuation sont nécessaires et appliquer ces mesures avant de connecter l'*actif électronique temporaire*.

Section 3. *Supports de stockage amovibles*

3.1. Autorisations relatives aux *supports de stockage amovibles* : Pour chaque *support de stockage amovible* ou groupe de *supports de stockage amovibles*, chaque entité responsable doit autoriser :

3.1.1. les utilisateurs (individuellement, par groupe ou par rôle) ; et

3.1.2. les emplacements (individuellement ou par groupe).

3.2. Atténuation du risque lié aux programmes malveillants : Afin de réaliser l'objectif d'atténuer le risque lié à l'introduction de programmes malveillants dans des *systèmes électroniques BES* à impact élevé ou moyen et dans les *actifs électroniques protégés* connexes, chaque entité responsable doit :

3.2.1. prendre des mesures pour détecter les programmes malveillants sur les *supports de stockage amovibles* au moyen d'un *actif électronique* autre qu'un *système électronique BES* ou que des *actifs électroniques protégés* ; et

3.2.2. neutraliser la menace de programmes malveillants détectés sur des *supports de stockage amovibles* avant de connecter ces supports à un *système électronique BES* à impact moyen ou élevé ou à des *actifs électroniques protégés* connexes.

CIP-010-3 – Annexe 2

Exemples de pièces justificatives pour les plans concernant les *actifs électroniques temporaires* et les *supports de stockage amovibles*

Section 1.1 : Exemples non limitatifs de pièces justificatives pour la section 1.1 : méthodes de gestion des *actifs électroniques temporaires*. Cette information peut faire partie des plans concernant les *actifs électroniques temporaires*, de la documentation concernant les autorisations relatives aux *actifs électroniques temporaires* gérés par l'entité responsable, ou encore d'une politique de sécurité.

Section 1.2 : Exemples non limitatifs de pièces justificatives pour la section 1.2 : documentation de systèmes de gestion des actifs ou de gestion des ressources humaines, ou formulaires ou feuilles de chiffrier indiquant les autorisations relatives aux *actifs électroniques temporaires* gérés par l'entité responsable. Cette information peut aussi être documentée dans le document principal du plan.

Section 1.3 : Exemples non limitatifs de pièces justificatives pour la section 1.3 : documentation des moyens utilisés pour atténuer le risque lié aux vulnérabilités présentées par les logiciels sans correctifs, comme la gestion des correctifs de sécurité, l'utilisation de systèmes d'exploitation sur support non inscriptible, le renforcement du système d'exploitation ou d'autres moyens d'atténuation appropriés. Les pièces justificatives peuvent provenir de systèmes de gestion des changements, de solutions de gestion systématique des correctifs, de procédures ou processus concernant l'utilisation de systèmes d'exploitation sur support amovible, ou de procédures ou processus associés aux pratiques de renforcement du système d'exploitation. Si un *actif électronique temporaire* n'a pas la capacité de mettre en œuvre certains moyens d'atténuation du risque lié aux vulnérabilités présentées par les logiciels sans correctifs, les pièces justificatives peuvent comprendre une documentation du fournisseur ou de l'entité responsable indiquant que l'*actif électronique temporaire* n'a pas cette capacité.

Section 1.4 : Exemples non limitatifs de pièces justificatives pour la section 1.4 : documentation des moyens utilisés pour atténuer le risque lié à l'introduction de programmes malveillants, comme des logiciels antivirus et des processus de gestion des mises à jour des signatures ou des séquences de code, des pratiques de liste blanche d'applications, des processus de restriction des communications ou d'autres moyens d'atténuation appropriés. Si un *actif électronique temporaire* n'a pas la capacité de mettre en œuvre certains moyens d'atténuation du risque lié à l'introduction de programmes malveillants, les pièces justificatives peuvent comprendre une documentation du fournisseur ou de l'entité responsable indiquant que l'*actif électronique temporaire* n'a pas cette capacité.

Section 1.5 : Exemples non limitatifs de pièces justificatives pour la section 1.5 : documentation (politiques ou procédures) des moyens de restriction des accès physiques ; description de la solution de cryptage de disque intégral et du protocole d'authentification ; description de la solution d'authentification multifactorielle ; ou documentation d'autres moyens d'atténuer le risque lié aux utilisations non autorisées.

Section 2.1 : Exemples non limitatifs de pièces justificatives pour la section 2.1 : documentation de systèmes de gestion des changements, courriels ou procédures qui documentent un examen des correctifs de sécurité installées ; notes de service, courriels, politiques ou contrats d'une tierce partie autre que l'entité responsable qui décrivent le processus

d'application de correctifs ou d'atténuation du risque lié aux vulnérabilités exécuté par la tierce partie ; pièces justificatives de systèmes de gestion des changements, courriels, documentation de système ou contrats indiquant que l'entité responsable juge acceptables les pratiques de la tierce partie ; ou documentation d'autres moyens d'atténuation du risque lié aux vulnérabilités logicielles d'*actifs électroniques temporaires* gérés par la tierce partie. Si un *actif électronique temporaire* n'a pas la capacité de mettre en œuvre certains moyens d'atténuation du risque lié aux vulnérabilités présentées par les logiciels sans correctifs, les pièces justificatives peuvent comprendre une documentation de l'entité responsable ou de la tierce partie indiquant que l'*actif électronique temporaire* n'a pas cette capacité.

Section 2.2 : Exemples non limitatifs de pièces justificatives pour la section 2.2 : documentation de systèmes de gestion des changements, courriels ou procédures qui documentent un examen du degré de maintien à jour des antivirus installés ; notes de service, courriels, documentation de système, politiques ou contrats d'une tierce partie autre que l'entité responsable qui décrivent le processus de mise à jour des antivirus, l'utilisation d'une liste blanche d'applications, l'utilisation de systèmes d'exploitation sur support externe ou le renforcement du système d'exploitation par la tierce partie ; pièces justificatives de systèmes de gestion des changements, courriels ou contrats indiquant que l'entité responsable juge acceptables les pratiques de la tierce partie ; ou documentation d'autres moyens d'atténuation du risque lié à l'introduction de programmes malveillants pour les *actifs électroniques temporaires* gérés par la tierce partie. Si un *actif électronique temporaire* n'a pas la capacité de mettre en œuvre certains moyens d'atténuation du risque lié à l'introduction de programmes malveillants, les pièces justificatives peuvent comprendre une documentation de l'entité responsable ou de la tierce partie indiquant que l'*actif électronique temporaire* n'a pas cette capacité.

Section 2.3 : Exemples non limitatifs de pièces justificatives pour la section 2.3 : documentation de systèmes de gestion des changements, courriels ou contrats attestant qu'un examen a été effectué pour déterminer le besoin de mesures d'atténuation supplémentaires, et que ces mesures ont été mises en œuvre avant la connexion de l'*actif électronique temporaire* géré par une tierce partie autre que l'entité responsable.

Section 3.1 : Exemples non limitatifs de pièces justificatives pour la section 3.1 : documentation de systèmes de gestion des actifs ou de gestion des ressources humaines, formulaires ou feuilles de chiffrier indiquant les autorisations relatives aux *supports de stockage amovibles*. La documentation doit désigner les *supports de stockage amovibles* (individuellement ou par groupe), les utilisateurs autorisés (individuellement, par groupe ou par rôle) et les emplacements autorisés (individuellement ou par groupe).

Section 3.2 : Exemples non limitatifs de pièces justificatives pour la section 3.2 : processus documentés des moyens d'atténuation du risque lié aux programmes malveillants, comme les résultats de balayage paramétré pour les *supports de stockage amovibles* ou la mise en œuvre du balayage à la demande ; processus documentés des moyens d'atténuation du risque lié aux programmes malveillants détectés sur les *supports de stockage amovibles*, comme les journaux créés par les mécanismes de détection qui montrent les résultats du balayage et indiquent la neutralisation des programmes malveillants détectés sur les *supports de stockage amovibles*, ou une confirmation documentée par l'entité que les *supports de stockage amovibles* sont considérés comme exempts de tout programme malveillant.

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.

Exigence E1 :

Configuration de référence

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

Les configurations de référence dans la norme CIP-010 comportent cinq éléments : le système d'exploitation ou le système embarqué ; les logiciels commerciaux ou les logiciels libres ; les logiciels personnalisés ; les ports logiques accessibles par le réseau ; et les correctifs de sécurité. L'information sur le système d'exploitation précise le nom et la version du logiciel en cours d'utilisation dans l'*actif électronique*. En l'absence de système d'exploitation indépendant (par exemple pour un relais de protection), l'information sur le système embarqué devrait être précisée. Les logiciels commerciaux ou les logiciels libres sont ceux qui ont été installés intentionnellement dans l'actif électronique. L'utilisation du mot « intentionnellement » vise à préciser que seuls les logiciels jugés nécessaires pour les *actifs électroniques* doivent être inclus dans la configuration de référence. La SDT ne souhaite pas que soient inclus dans cette configuration les calepins, calculettes, les DLL, les pilotes de périphérique ou d'autres applications compris dans un système d'exploitation commercial ou distribués à titre de logiciel libre. Les logiciels personnalisés installés peuvent comprendre des scripts programmés pour des fonctions locales de l'entité ou d'autres programmes créés en vue d'une tâche ou fonction spécifique à l'entité. Dans le cas d'un logiciel supplémentaire qui a été installé intentionnellement et qui n'est ni un logiciel commercial ni un logiciel libre, ce logiciel pourrait être considéré comme un logiciel personnalisé. Si un dispositif a besoin de communiquer avec un autre dispositif à l'extérieur du réseau, les communications doivent être limitées aux seuls dispositifs qui doivent communiquer, conformément à la norme CIP-007-6. Les ports accessibles doivent être indiqués dans la configuration de référence. Les correctifs de sécurité appliqués doivent comprendre tous les correctifs antérieurs et courants appliqués

sur l'actif électronique. Alors que l'alinéa 2.1 de l'exigence E2 de la norme CIP-007-6 stipule que les entités doivent se tenir informées des correctifs de sécurité, les évaluer et les appliquer, l'alinéa 1.1.5 de l'exigence E1 de la norme CIP-010 stipule que les entités doivent consigner tous les correctifs appliqués, antérieurs et courants.

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

Actif n^{o} 051028 au poste électrique Alpha

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

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

Mécanismes de cybersécurité

Les mécanismes de cybersécurité dont il est question dans cette exigence renvoient spécifiquement aux mécanismes des normes CIP-005 et CIP-007. Les alinéas pertinents de l'exigence E1 de la norme CIP-010 stipulent que l'entité doit déterminer et analyser les mécanismes des normes CIP-005 et CIP-007 qui pourraient être touchés par un changement par rapport à la configuration de référence existante. La SDT ne souhaite pas obliger l'entité responsable à passer en revue tous les mécanismes de cybersécurité des normes CIP-005 et CIP-007 pour chaque changement, mais seulement le ou les mécanismes susceptibles d'être touchés par le changement en question. Par exemple, les changements relatifs aux ports logiques concernent seulement l'exigence E1 de la norme CIP-007 (ports et services), tandis que les changements relatifs aux correctifs de sécurité concernent seulement l'exigence E2 de la norme CIP-007 (gestion des correctifs de sécurité). La SDT a choisi de ne pas préciser les exigences des normes CIP-005 et CIP-007 dans le texte de la norme CIP-010, étant donné que n'importe quel des mécanismes de cybersécurité de ces normes peut être touché par suite d'un changement dans la configuration de référence. La SDT considère qu'il est possible que toutes les exigences des normes CIP-005 et CIP-007 soient touchées par un changement important dans la configuration de référence, et c'est pourquoi les normes CIP-005 et CIP-007 sont citées dans leur globalité plutôt qu'à l'échelon de leurs exigences individuelles.

Environnement d'essai

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

En outre, l'entité responsable doit prendre note que, lorsqu'il est question d'un environnement d'essai (ou d'un environnement de production dans lequel l'essai est effectué d'une manière qui réduit au

minimum les effets dommageables), il s'agit bien de « simuler » la configuration de référence, et non de la reproduire à l'identique. Cette formulation a été choisie expressément pour les cas où il serait impossible de dupliquer certains éléments de *système électronique BES* d'un *centre de contrôle* ; par exemple, un modèle ancien de pilote de tableau de visualisation, ou encore les nombreuses liaisons d'échange de données à partir des installations sur le terrain ou vers d'autres *centres de contrôle* (comme les liaisons ICCP).

Vérification des logiciels

Le concept de vérification des logiciels (validation de l'identité de la source d'un logiciel et de l'intégrité du logiciel obtenu de cette source) est une mesure de contrôle essentielle pour prévenir l'introduction de maliciels ou de logiciels contrefaits. Cet objectif vise à réduire la probabilité qu'un assaillant puisse exploiter les processus de gestion des correctifs de fournisseurs légitimes pour infiltrer dans un *système électronique BES* des mises à jour ou des correctifs de logiciel compromis. L'équipe de rédaction entend amener les entités responsables à établir des mesures pour vérifier les éléments de configuration de référence qui sont mis à jour par les fournisseurs. Soulignons que cette exigence n'est pas limitée aux correctifs de sécurité.

La publication spéciale (SP) 800-161 du NIST décrit différents mécanismes de sécurité qui, combinés, réduisent la probabilité de succès d'attaques de type « point d'eau » ou d'autres cyberattaques semblables dans un environnement de systèmes de commande industrielle, et pourraient donc aider à satisfaire à l'objectif précité. Par exemple, dans la famille des mesures portant sur l'intégrité des systèmes et de l'information (*System and Information Integrity – SI*), la mesure SI-7 suggère aux utilisateurs de se procurer les logiciels directement auprès de l'éditeur et de vérifier l'intégrité des logiciels au moyen de mesures comme la signature numérique. Dans la famille des mesures portant sur la gestion des configurations (*Configuration Management – CM*), la mesure CM-5(3) consiste à faire bloquer par le système d'information l'installation de logiciels ou de micrologiciels si leur signature numérique n'a pas d'abord été vérifiée, afin de faire en sorte que les éléments matériels et logiciels soient bien authentiques et valides. La publication spéciale 800-161 du NIST, même si elle ne prétend pas apporter des réponses définitives, donne des exemples de mesures permettant de satisfaire à cet objectif. D'autres mesures pourraient également être adéquates à cet égard.

Pour la mise en œuvre de l'alinéa 1.6 de l'exigence E1, l'entité responsable devrait examiner ses politiques et mesures de cybersécurité CIP existantes, et envisager aussi les mesures suivantes :

- les processus de livraison des logiciels et les mesures permettant de vérifier l'identité de la source des logiciels et l'intégrité des logiciels livrés au moyen de ces processus. Dans la mesure où l'entité responsable utilise des systèmes automatisés – par exemple un service par abonnement – pour télécharger et diffuser les logiciels ainsi que leurs mises à jour, envisager d'intégrer à ces processus un mécanisme de vérification des logiciels ;
- la coordination des mesures de vérification des logiciels de l'entité responsable avec d'autres politiques et mesures de cybersécurité, notamment les processus de gestion des changements et des correctifs ainsi que les contrôles d'approvisionnement ;
- le stockage des logiciels dans un dépôt central, après validation de l'identité de la source et de l'intégrité des logiciels, afin d'évider de devoir répéter ces vérifications avant chaque installation ;
- des mesures supplémentaires comme les exemples décrits à la section SI-7 sur l'intégrité des logiciels, des micrologiciels et de l'information (*Software, Firmware, and Information Integrity*) de la publication spéciale 800-53 révision 4 du NIST, ou dans d'autres documents d'encadrement semblables ;

- des mesures supplémentaires comme celles décrites dans les normes FIPS 140-2 et FIPS 180-4 ou d'autres documents d'encadrement semblables, visant à ce que les méthodes cryptographiques utilisées soient acceptables par l'entité responsable.

Les entités responsables peuvent utiliser diverses méthodes pour vérifier l'intégrité des logiciels obtenus d'une source. Quelques exemples non limitatifs :

- Vérifier que le logiciel porte une signature numérique, et valider cette signature pour s'assurer que l'intégrité du logiciel n'a pas été compromise.
- Utiliser une infrastructure de clés publiques (PKI) avec chiffrement, de façon que seuls les destinataires désignés puissent déchiffrer les logiciels, afin que ceux-ci ne puissent pas être modifiés en cours de transit.
- Demander aux sources de logiciels de fournir des empreintes électroniques ou des codes de hachage pour tous les logiciels, et vérifier ces valeurs avant l'installation dans un *système électronique BES* afin de confirmer l'intégrité du logiciel. Il est souhaitable de recevoir les valeurs de vérification au moyen d'une méthode différente de celle utilisée pour recevoir le logiciel à partir de la source de logiciels.
- Utiliser des mécanismes de sécurisation pour la livraison et la diffusion afin de réduire les risques dans la chaîne d'approvisionnement (par exemple, exiger un emballage inviolable pour les logiciels pendant le transport.)

Exigence E2

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

Exigence E3

L'entité responsable doit prendre note que l'exigence d'analyse de vulnérabilité fait une distinction entre analyse sur papier et analyse active. Cette distinction s'appuie sur l'ordonnance 706 de la FERC et la proposition réglementaire (*Notice of Proposed Rulemaking*) connexe. Dans l'élaboration de ses processus d'analyse de vulnérabilité, l'entité responsable est fortement encouragée à inclure à tout le moins les éléments suivants, dont plusieurs sont mentionnés dans les normes CIP-005 et CIP-007 :

Analyse de vulnérabilité sur papier :

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

Analyse de vulnérabilité active :

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

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

Exigence E4

Comme la plupart des *actifs électroniques BES* et des *systèmes électroniques BES* sont isolés des réseaux externes publics ou non fiables, les *actifs électroniques temporaires* et les *supports de stockage amovibles* se présentent assurément comme un vecteur de cyberattaques. Ceux-ci constituent souvent le seul moyen d'entrée et de sortie des fichiers pour des zones sécurisées dans le cadre d'opérations de maintenance, de surveillance ou de dépannage de systèmes névralgiques. Afin de protéger les *actifs électroniques BES* et les *systèmes électroniques BES*, les entités sont tenues de documenter et de mettre en œuvre un plan de gestion de l'utilisation des *actifs électroniques temporaires* et des *supports de stockage amovibles*. L'élaboration de ce plan amène l'entité responsable à documenter des processus que son organisation est capable de mettre en œuvre et qui cadrent avec ses processus de gestion des changements.

Les *actifs électroniques temporaires* et les *supports de stockage amovibles* sont des dispositifs connectés temporairement : 1) à un *actif électronique BES*, 2) à un réseau à l'intérieur d'un *périmètre de sécurité électronique* (*ESP*) ou 3) à un *actif électronique protégé*. Les *actifs électroniques temporaires* et les *supports de stockage amovibles* n'assurent pas de services liés à la fiabilité du *BES* et ne font pas partie de l'*actif électronique BES* auquel ils sont connectés. Exemples non limitatifs de ces dispositifs connectés temporairement :

- équipements de diagnostic ;
- renifleurs de paquets ;
- équipements de maintenance de *systèmes électroniques BES* ;
- équipements de configuration de *systèmes électroniques BES*; ou
- équipements d'analyse de vulnérabilité.

Les *actifs électroniques temporaires* sont très variés ; ils vont des dispositifs conçus spécialement pour la maintenance d'équipements liés au *BES* à des appareils courants (ordinateurs portatifs ou de bureau, tablettes, etc.) qui peuvent simplement se connecter à des *systèmes électroniques BES* ou exécuter des applications afférentes à ceux-ci et qui sont capables de transmettre du code exécutable. Les *supports de stockage amovibles* visés par cette exigence peuvent être des disquettes, des cédéroms, des clés USB, des disques durs externes et des cartes ou lecteurs à mémoire flash (non volatile).

Bien que les définitions d'*actif électronique temporaire* et de *support de stockage amovible* comprennent une condition qui limite à 30 jours leur durée de connexion, la section 1.1 de l'annexe 1 permet à l'entité responsable d'incorporer à son plan des traitements appliqués en permanence ou à la demande ainsi que des mesures indépendantes de l'état de connexion ou de déconnexion. Il est à noter

qu'un traitement à la demande n'est à appliquer que lorsqu'on s'apprête à connecter l'*actif électronique temporaire* ou le *support de stockage amovible* à un *système électronique BES* ou à un *actif électronique protégé* ; une fois l'*actif électronique temporaire* ou le *support de stockage amovible* déconnecté, les exigences présentées ici cessent de s'appliquer tant qu'on ne s'apprête pas de nouveau à le connecter à l'*actif électronique BES* ou à l'*actif électronique protégé*.

L'annexe vise à spécifier les ressources et les moyens de sécurité auxquels peuvent avoir recours les entités responsables d'après le type d'un actif, son propriétaire et l'entité ou la partie qui le gère.

À partir de la liste d'options présentée à l'annexe 1 pour chacun des thèmes de cybersécurité, l'entité responsable est libre de choisir le ou les moyens qui lui conviennent le mieux. L'entité responsable est invitée à documenter comment et quand elle entend gérer les *actifs électroniques temporaires* sous son contrôle ou examiner ceux placés sous le contrôle d'autres entités. L'entité responsable doit éviter de mettre en place des fonctions de sécurité susceptibles d'affaiblir la fiabilité du réseau en agissant d'une manière qui nuirait au fonctionnement ou au soutien d'*actifs électroniques temporaires*, d'*actifs électroniques BES* ou d'*actifs électroniques protégés*.

Atténuation du risque lié aux vulnérabilités

Des expressions comme « atténuer le risque » ou « atténuation du risque » sont utilisées dans les sections de l'annexe 1 à l'endroit des risques présentés par les programmes malveillants, les vulnérabilités logicielles et les utilisations non autorisées lorsqu'il s'agit de connecter des *actifs électroniques temporaires* et des *supports de stockage amovibles*. Le choix du mot « atténuer » ou « atténuation » laisse entendre qu'il n'est pas exigé de parer à chacune des vulnérabilités possibles, car beaucoup d'entre elles peuvent être inconnues ou ne pas avoir d'effet sur le système auquel l'*actif électronique temporaire* ou *le support de stockage amovible* est connecté. L'exigence d'atténuation consiste à réduire les risques pour la sécurité associés à la connexion de l'*actif électronique temporaire*.

Prise en compte des capacités de l'*actif électronique temporaire*

Comme dans d'autres normes CIP, les moyens à utiliser par l'entité se limitent à ceux que le système est capable de mettre en œuvre. L'expression « selon les capacités de l'*actif électronique temporaire* » sert à éviter le recours à une exception pour raison technique (TFE) lorsqu'il est évident que certains moyens ne sont pas utilisables avec tel ou tel dispositif. Par exemple, dans le cas des programmes malveillants, bien des types de dispositifs n'ont pas la capacité de faire fonctionner un logiciel antivirus ; par conséquent, la mise en œuvre d'un logiciel antivirus ne serait pas exigée pour ces dispositifs.

Exigence E4, section 1 de l'annexe 1 – *Actifs électroniques temporaires* gérés par l'entité responsable

Section 1.1 – Les entités exercent un degré de contrôle élevé sur les actifs qu'elles gèrent elles-mêmes. Les exigences présentées ici donnent aux entités la souplesse de préautoriser un ensemble de dispositifs, d'autoriser les dispositifs au moment de leur connexion, ou encore de combiner ces deux méthodes. Les dispositifs peuvent être gérés individuellement ou par groupe.

Section 1.2 – Les entités doivent documenter et mettre en œuvre leurs processus d'autorisation pour l'utilisation des *actifs électroniques temporaires* qu'ils gèrent directement. Les *actifs électroniques temporaires* peuvent être désignés individuellement ou par type d'actifs. Afin de respecter cet élément de l'exigence, l'entité doit documenter les éléments suivants :

1.2.1 Les utilisateurs (individuellement, par groupe ou par rôle) autorisés à utiliser les *actifs électroniques temporaires*. On peut inscrire à cette fin le nom de la personne, le nom d'un service ou le titre d'un poste. Attention : il faut déterminer si ces utilisateurs doivent aussi

avoir un accès électronique autorisé au système pertinent conformément à la norme CIP-004.

1.2.2 Les emplacements où les *actifs électroniques temporaires* sont autorisés. On peut inscrire à cette fin un emplacement particulier ou un groupe d'emplacements.

1.2.3 L'utilisation prévue ou approuvée des *actifs électroniques temporaires* (individuellement, par groupe ou par rôle). Il faut aussi indiquer les logiciels ou progiciels qui sont autorisés pour des fonctions ou des tâches opérationnelles bien définies (transfert de données, analyse de vulnérabilité, maintenance, dépannage, etc.) ainsi que les interfaces réseau approuvées (par exemple les liaisons sans fil, y compris la communication en champ proche ou par Bluetooth, et les liaisons filaires). Les utilisations et les logiciels ou progiciels non spécifiquement inscrits comme acceptables doivent être considérés comme interdits. Les programmes de sensibilisation à la sécurité et de formation en cybersécurité de la norme CIP-004 peuvent servir à informer le personnel quant aux activités ou aux utilisations autorisées ou interdites (par exemple l'utilisation d'un dispositif pour naviguer sur Internet ou lire des courriels, ou encore pour accéder à des réseaux sans fil dans des hôtels ou d'autres commerces).

Les entités doivent se montrer prudentes dans l'utilisation d'*actifs électroniques temporaires* et s'assurer que ceux-ci n'ont pas de fonctions activées (par exemple la connectivité sans fil ou Bluetooth) qui permettraient au dispositif de servir de relais entre un réseau extérieur et un système visé. Dans un tel cas, l'*actif électronique temporaire* deviendrait un *point d'accès électronique* non autorisé, en contravention avec l'exigence E1 de la norme CIP-005.

Il faut prêter attention aux *actifs électroniques temporaires* qui peuvent être utilisés avec des actifs situés dans des zones ayant des degrés d'impact différents (impacts élevé, moyen et faible). Ces zones d'impact ont différents niveaux de protection en vertu des normes CIP, et il faut prendre des mesures pour atténuer le risque lié à l'introduction de programmes malveillants à partir d'une zone d'impact moindre. Une entité pourrait juger préférable d'avoir des *actifs électroniques temporaires* distincts pour chaque degré d'impact.

Section 1.3 – Les entités doivent documenter et mettre en œuvre leurs processus visant à atténuer le risque lié aux vulnérabilités présentées par les logiciels sans correctifs, en adoptant une ou plusieurs des mesures de protection indiquées. Ces mesures doivent tenir compte des capacités de chaque dispositif. Étant donné la très grande diversité des types de dispositifs qui peuvent servir d'*actifs électroniques temporaires* ainsi que les progrès dans les solutions de gestion des vulnérabilités logicielles, les options présentées laissent la porte ouverte à des solutions de rechange (technologies ou processus) qui atténueraient adéquatement le risque lié à ces vulnérabilités.

- L'application de correctifs, avec mises à jour manuelles ou systématiques, offre à l'entité responsable une certaine latitude quant à l'utilisation de ses *actifs électroniques temporaires*. L'entité peut décider de mettre en place pour ses *actifs électroniques temporaires* un processus normalisé d'application de correctifs de sécurité selon un calendrier régulier, ou plutôt d'appliquer les correctifs de sécurité nécessaires à un *actif électronique temporaire* avant de le connecter à un *actif électronique* visé. Contrairement à l'exigence E2 de la norme CIP-007, l'entité n'a pas à élaborer de plans d'atténuation datés ou d'autres documents au-delà de ce qui est nécessaire pour déterminer que l'*actif électronique temporaire* reçoit les correctifs de sécurité appropriées.
- L'utilisation de systèmes d'exploitation et de logiciels exécutables uniquement à partir de supports non inscriptibles permet d'avoir un système d'exploitation protégé qui ne peut être

modifié de manière à transmettre des programmes malveillants. Lorsqu'une entité crée un système d'exploitation personnalisé sur support externe, elle doit vérifier l'image pendant sa création afin de s'assurer que l'image ne contient aucun programme malveillant.

- Le renforcement du système d'exploitation consiste à éliminer tous les logiciels et utilitaires non essentiels et à n'installer que le minimum indispensable au fonctionnement de l'ordinateur, ce qui aide à réduire les vulnérabilités. Les programmes supplémentaires peuvent offrir des fonctionnalités utiles, mais ils peuvent aussi receler des « portes dérobées » d'accès au système ; leur élimination a pour effet de renforcer le système.
- Si elle opte pour des moyens autres que ceux qui sont suggérés pour atténuer le risque lié aux vulnérabilités logicielles, l'entité doit établir une documentation qui indique comment ces moyens réalisent l'objectif d'atténuer le risque en question.

Section 1.4 – Les entités doivent documenter et mettre en œuvre leurs processus d'atténuation du risque lié à l'introduction de programmes malveillants, en adoptant une ou plusieurs des mesures de protection indiquées. Ces mesures doivent tenir compte des capacités de chaque dispositif. Comme pour la gestion des vulnérabilités logicielles, il convient de reconnaître la grande diversité des types de dispositifs qui peuvent servir d'*actifs électroniques temporaires* ainsi que les progrès réalisés dans la protection contre les programmes malveillants. L'entité responsable doit adopter des mesures pour bloquer, détecter ou prévenir les programmes malveillants. Si un programme malveillant est détecté, il faut le supprimer ou le neutraliser afin qu'il ne puisse pas être introduit dans un *actif électronique BES* ou un *système électronique BES*. L'entité doit aussi déterminer si la détection du programme malveillant constitue un *incident de cybersécurité*.

- Un logiciel antivirus, avec mises à jour manuelles ou systématiques des signatures ou des séquences de code, offre la même souplesse que l'application de correctifs. On peut ainsi gérer les *actifs électroniques temporaires* en déployant des logiciels antivirus ou des outils de sécurité des points terminaux qui assurent une mise à jour programmée des signatures ou des séquences de code. Par ailleurs, pour les dispositifs dont la connexion non régulière ne leur permet pas de recevoir des mises à jour programmées, l'entité peut choisir de balayer l'*actif électronique temporaire* avant son raccordement afin de confirmer l'absence de programme malveillant.
- La liste blanche d'applications consiste à autoriser seulement les applications et les processus nécessaires pour l'*actif électronique temporaire*. Cela réduit d'autant la possibilité pour un programme malveillant de devenir résident, et encore moins de se propager à partir de l'*actif électronique temporaire* vers l'*actif électronique BES* ou le *système électronique BES*.
- On peut limiter les communications aux seuls échanges de données entre un *actif électronique temporaire* géré et les *actifs électroniques* auxquels il est connecté, en restreignant ou en désactivant les communications série ou réseau (y compris sans fil) de l'*actif électronique temporaire*, afin de réduire au minimum les occasions d'introduire un programme malveillant dans celui-ci pendant qu'il n'est pas connecté à un *système électronique BES*. Le dispositif est alors incapable de communiquer avec des dispositifs autres que celui auquel il doit être connecté.
- Si elle opte pour des moyens autres que ceux qui sont suggérés pour l'atténuation du risque lié à l'introduction de programmes malveillants, l'entité doit établir une documentation qui indique comment ces moyens réalisent l'objectif d'atténuer le risque en question.

Section 1.5 : Les entités doivent documenter et mettre en œuvre leurs processus de protection et d'évaluation des *actifs électroniques temporaires* visant à atténuer le risque qu'une utilisation non autorisée de ceux-ci peut présenter pour les *systèmes électroniques BES*. La préoccupation à laquelle

répond cette section est la possibilité qu'un *actif électronique temporaire* puisse être manipulé de façon inappropriée ou être exposé à des logiciels malveillants pendant qu'il n'est pas utilisé aux fins prévues par une personne autorisée. La sécurité physique de l'*actif électronique temporaire* est assurément une mesure qui atténue ce risque, mais d'autres outils et techniques sont aussi envisageables. La liste d'exemples ci-après présente différentes possibilités suggérées.

- Les restrictions d'accès physique consistent à maintenir l'*actif électronique temporaire* à l'intérieur d'un *périmètre de sécurité physique* ou d'un autre lieu ou enceinte physique dont les accès physiques sont contrôlés afin de protéger l'*actif électronique temporaire*.
- Le cryptage de disque intégral avec authentification est une option qui permet de protéger un *actif électronique temporaire* contre toute utilisation non autorisée ; il est toutefois important qu'une authentification soit exigée avant le décryptage. Par exemple, l'authentification avant le démarrage ou à la mise sous tension sécurise le système d'exploitation en constituant autour de lui une couche d'authentification externe. Les données du disque dur ne peuvent pas être lues tant que l'utilisateur n'a pas confirmé son identité au moyen d'un mot de passe ou d'autres éléments d'authentification. En imposant une authentification avant le décryptage du système et le démarrage, on réduit le risque qu'une personne non autorisée puisse manipuler l'*actif électronique temporaire*.
- L'authentification multifactorielle sert à confirmer l'identité de la personne qui accède au dispositif. L'authentification multifactorielle atténue aussi le risque qu'une personne non autorisée puisse manipuler l'*actif électronique temporaire*.
- Outre les mécanismes d'authentification et de sécurité physique pure, d'autres possibilités existent. Certaines solutions de sécurisation en cas de vol permettent de géolocaliser l'*actif électronique temporaire*, de détecter tout accès, d'effacer le contenu à distance et de verrouiller le système, limitant ainsi la menace potentielle liée à une utilisation non autorisée si l'*actif électronique temporaire* était par la suite connecté à un *actif électronique BES*. D'autres solutions plus rudimentaires peuvent aussi être efficaces pour atténuer le risque lié à l'utilisation d'un *actif électronique temporaire* falsifié, par exemple des étiquettes ou des sceaux d'inviolabilité dont l'intégrité est vérifiée au moyen d'une procédure spéciale avant l'utilisation du dispositif.
- Si elle opte pour des moyens autres que ceux qui sont suggérés pour atténuer le risque lié aux utilisations non autorisées, l'entité doit établir une documentation qui indique comment ces moyens réalisent l'objectif d'atténuer le risque en question.

Exigence E4, section 2 de l'annexe 1 – *Actifs électroniques temporaires* gérés par une tierce partie autre que l'entité responsable

Cette annexe reconnaît également que l'entité responsable n'a aucun contrôle direct sur les *actifs électroniques temporaires* qui sont gérés par une tierce partie. L'entité responsable est néanmoins tenue de s'assurer que des moyens ont été déployés pour bloquer, détecter ou prévenir l'introduction de programmes malveillants dans les *actifs électroniques temporaires* qui ne relèvent pas de sa gestion. Les exigences ci-après indiquent aux entités comment procéder au mieux à l'examen des actifs afin de remplir leurs obligations.

Afin d'assurer un contrôle adéquat, les entités responsables peuvent choisir de conclure des ententes avec des tierces parties pour la prestation de services de soutien des *systèmes électroniques BES* et des *actifs électroniques BES* qui peuvent nécessiter l'utilisation d'*actifs électroniques temporaires*. Les entités pourront juger avantageux d'adopter les clauses normalisées du département de l'Énergie des États-Unis pour les contrats de cybersécurité dans le domaine de la fourniture d'énergie (*Cybersecurity*

Procurement Language for Energy Delivery Systems[1], avril 2014). Ces clauses d'approvisionnement peuvent aider à harmoniser les actions de l'entité responsable et des tierces parties chargées du soutien des *systèmes électroniques BES* et des *actifs électroniques BES*. Les attributs du programme de protection des infrastructures essentielles (CIP), y compris les rôles et responsabilités, les contrôles d'accès, la surveillance, la journalisation, la gestion des vulnérabilités et celle des correctifs ainsi que les interventions en cas d'incident et la récupération des sauvegardes, peuvent faire partie des prestations confiées à une tierce partie. Les entités pourront s'inspirer des chapitres General Cybersecurity Procurement Language et The Supplier's Life Cycle Security Program du document précité pour la rédaction des ententes-cadres de services, des contrats et des processus et contrôles du programme CIP.

Section 2.1 – Les entités doivent documenter et mettre en œuvre leurs processus d'atténuation du risque lié aux vulnérabilités logicielles, comportant une ou plusieurs des mesures de protection indiquées ci-après.

- Procéder à un examen de l'*actif électronique temporaire* géré par une tierce partie autre que l'entité responsable afin de déterminer si la version des correctifs de sécurité du dispositif atténue adéquatement le risque de vulnérabilités logicielles avant la connexion de l'actif *électronique temporaire* à un système visé.
- Procéder à un examen de la procédure d'application de correctifs de la tierce partie. Cet examen peut être fait lors de l'entente contractuelle, ou au plus tard avant de connecter l'*actif électronique temporaire* à un système visé. Tout comme pour l'examen de la version des correctifs de sécurité du dispositif, le choix de ce moyen vise à confirmer que l'entité responsable a atténué le risque lié aux vulnérabilités logicielles pour les systèmes visés.
- Procéder à un examen d'autres processus adoptés par la tierce partie pour atténuer le risque lié aux vulnérabilités logicielles, par exemple le renforcement du système d'exploitation, les listes blanches d'applications, les machines virtuelles, etc.
- Si elle opte pour des moyens autres que ceux qui sont suggérés pour atténuer le risque lié aux vulnérabilités logicielles, l'entité doit établir une documentation qui indique comment ces moyens réalisent l'objectif d'atténuer le risque en question.

Section 2.2 – Les entités doivent documenter et mettre en œuvre leurs processus d'atténuation du risque lié à l'introduction des programmes malveillants, comportant une ou plusieurs des mesures d'atténuation indiquées ci-après.

- Procéder à un examen des niveaux de tenue à jour des logiciels antivirus ainsi que des signatures ou des séquences de code afin de s'assurer que ces niveaux permettent à l'entité responsable d'atténuer adéquatement le risque lié à l'introduction de programmes malveillants dans un système visé.
- Procéder à un examen des processus antivirus ou de sécurisation des points terminaux de la tierce partie afin de s'assurer que ces processus permettent à l'entité responsable d'atténuer adéquatement le risque lié à l'introduction de programmes malveillants dans un système visé.
- Procéder à un examen de l'utilisation par la tierce partie de listes blanches d'applications pour atténuer le risque lié à l'introduction de programmes malveillants dans un système visé.
- Procéder à un examen de l'utilisation de systèmes d'exploitation ou de logiciels exécutables uniquement à partir de supports non inscriptibles afin de s'assurer que les supports eux-mêmes

1. http://www.energy.gov/oe/downloads/cybersecurity-procurement-language-energy-delivery-april-2014

sont exempts de tout programme malveillant. Les entités doivent examiner les processus de préparation des supports non inscriptibles ainsi que les supports eux-mêmes.
- Procéder à un examen des pratiques adoptées par la tierce partie pour le renforcement du système d'exploitation afin de s'assurer que les ports, services, applications et autres éléments inutiles ont été désactivés ou retirés, ce qui limite le risque d'introduction de programmes malveillants dans un système visé.

Section 2.3 – Déterminer si des mesures d'atténuation supplémentaires sont nécessaires, et exécuter ces mesures avant de connecter l'*actif électronique temporaire* géré par une tierce partie. Cette section vise à faire en sorte que si, après les examens effectués conformément aux sections 2.1 et 2.2, des lacunes subsistent par rapport à la posture de sécurité de l'entité responsable, la tierce partie soit tenue d'exécuter des mesures d'atténuation supplémentaires avant de connecter ses dispositifs à un système visé.

Exigence E4, section 3 de l'annexe 1 – *Supports de stockage amovibles*

Les entités ont un degré de contrôle élevé sur les *supports de stockage amovibles* destinés à être connectés à leurs *actifs électroniques BES*.

Section 3.1 – Les entités doivent documenter et mettre en œuvre leurs processus d'autorisation de l'utilisation des *supports de stockage amovibles*. Les *supports de stockage amovibles* peuvent être inscrits individuellement ou par type.

- Documenter les utilisateurs (individuellement, par groupe ou par rôle) autorisés à utiliser les *supports de stockage amovibles*. On peut inscrire à cette fin le nom de la personne, le nom d'un service ou le titre d'un poste. L'autorisation s'étend au personnel de l'entité ainsi qu'aux fournisseurs. Attention : il faut déterminer si ces utilisateurs doivent aussi avoir un accès électronique autorisé au système pertinent conformément à la norme CIP-004.
- Documenter les emplacements où les *supports de stockage amovibles* sont autorisés. On peut inscrire à cette fin un emplacement particulier ou un groupe d'emplacements.

Section 3.2 – Les entités doivent documenter et mettre en œuvre leurs processus d'atténuation du risque lié à l'introduction de programmes malveillants, comportant un ou plusieurs moyens de détecter tout programme malveillant sur les *supports de stockage amovibles* avant leur connexion à un *actif électronique BES*. La détection de programmes malveillants doit normalement se faire à partir d'un système qui ne fait pas partie d'un *système électronique BES*, afin d'atténuer le risque lié à la propagation de programmes malveillants dans le réseau des *systèmes électroniques BES* ou dans un des *actifs électroniques BES*. Si un programme malveillant est détecté, il faut le supprimer ou le neutraliser afin qu'il ne puisse pas être introduit dans un *actif électronique BES* ou un *système électronique BES*. L'entité doit aussi déterminer si la détection du programme malveillant constitue un *incident de cybersécurité*. La fréquence et le choix du moment d'utilisation des moyens de détection des programmes malveillants ont été intentionnellement exclus de l'exigence, car il existe de multiples scénarios temporels possibles pour un plan d'atténuation du risque lié à l'introduction de programmes malveillants. Les entités doivent procéder à la détection des programmes malveillants sur les *supports de stockage amovibles* avant qu'ils soient connectés à l'*actif électronique BES*. Un choix judicieux du moment des interventions de détection, documenté dans le plan de l'entité, devrait réduire le risque d'introduction de programmes malveillants dans l'*actif électronique BES* ou l'*actif électronique protégé*.

Pour la détection des programmes malveillants, les entités peuvent choisir d'utiliser des *supports de stockage amovibles* auxquels sont intégrés des outils de détection de programmes malveillants. Dans ce cas, les outils de détection intégrés au support d'information amovible doivent quand même être

utilisés en combinaison avec un *actif électronique*. La section 3.2.1 précise que l'*actif électronique* utilisé pour la détection de programmes malveillants doit être situé à l'extérieur d'un *système électronique BES* ou d'un *actif électronique protégé*.

Justification

Justification de l'exigence E1

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

Justification de l'exigence E2

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

L'alinéa 1.6 de l'exigence E1 répond à l'alinéa 48 de l'Ordonnance 829 de la FERC, qui spécifie de vérifier l'intégrité et l'authenticité des logiciels avant leur installation dans des *systèmes électroniques BES*. L'objectif de vérification de l'intégrité et de l'authenticité des logiciels vise à valider que tout logiciel installé dans un *système électronique BES* n'a pas été modifié à l'insu du fournisseur du logiciel et n'est pas contrefait.

Justification de l'exigence E3

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

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

Justification de l'exigence E4

L'exigence E4 met en œuvre les prescriptions des paragraphes 6 et 136 de l'ordonnance 791 de la FERC, qui concernent les questions de sécurité associées aux *actifs électroniques temporaires* et aux *supports de stockage amovibles* utilisés pendant une durée limitée pour des tâches comme le transfert de données, l'analyse de vulnérabilité, la maintenance ou le dépannage. Ces outils sont des vecteurs potentiels d'introduction de programmes malveillants dans une installation et, de là, dans des *actifs électroniques* ou des *systèmes électroniques BES*. Afin d'atténuer les risques associés à de tels outils, l'exigence E4 a été élaborée en fonction des objectifs de sécurité suivants :

- empêcher tout accès non autorisé ou toute transmission de logiciels malveillants aux *systèmes électroniques BES* par des *actifs électroniques temporaires* ou des *supports de stockage amovibles* ; et
- empêcher tout accès non autorisé à l'information de *système électronique BES* au moyen d'*actifs électroniques temporaires* ou de *supports de stockage amovibles*.

L'exigence E4 intègre les concepts d'autres exigences des normes CIP-010 et CIP-007 afin d'aider à définir les exigences applicables aux *actifs électroniques temporaires* et aux *supports de stockage amovibles*.

Résumé des changements – Toutes les exigences relatives aux *actifs électroniques temporaires* et aux *supports de stockage amovibles* sont regroupées dans la norme CIP-010. En raison de la nouveauté de la définition de ces types d'actifs et des exigences qui s'y appliquent, la SDT a jugé que le regroupement de ces exigences dans une seule et même norme aiderait les entités à reconnaître rapidement les exigences applicables à ces types d'actifs. La création d'une norme séparée pour ces exigences a été envisagée ; cependant, la SDT a déterminé que l'utilisation de ces types d'actifs est connexe aux processus de gestion des changements et d'analyse de vulnérabilité, et qu'il est en somme préférable de regrouper le tout dans la norme qui encadre déjà ces processus.

A. Introduction

1. **Titre :** **Cybersécurité – Gestion des risques dans la chaîne d'approvisionnement**

2. **Numéro :** **CIP-013-1**

3. **Objet :** Atténuer les risques de cybersécurité susceptibles de menacer la fiabilité du *système de production-transport d'électricité* (*BES*) en établissant des contrôles de sécurité axés sur la gestion des risques dans la chaîne d'approvisionnement des *systèmes électroniques BES*.

4. **Applicabilité :**

   4.1. Entités fonctionnelles : Dans le contexte de la présente norme, les entités fonctionnelles indiquées ci-après sont appelées collectivement « entités responsables ». Si certaines exigences visent plus spécifiquement une entité fonctionnelle ou un sous-ensemble 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 systèmes, *installations* et équipements suivants pour la protection ou la remise en charge du *BES* :

   4.1.2.1. Système de délestage en sous-fréquence (DSF) ou 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 des délestages automatiques de *charge* de 300 MW ou plus sous la commande d'un système commun détenu par l'entité responsable, sans intervention humaine.

   4.1.2.2. *Automatisme de réseau (RAS*) visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou de l'*entité régionale*.

   4.1.2.3. *Système de protection* de réseau de transport (à l'exclusion des systèmes de DSF et de DST) visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou de l'*entité régionale*.

   4.1.3. *Exploitant d'installation de production*

   4.1.4. *Propriétaire d'installation de production*

   4.1.5. *Coordonnateur de la fiabilité*

   4.1.6. *Exploitant de réseau de transport*

   4.1.7. *Propriétaire d'installation de transport*

4.2. ***Installations*** **:** Dans le contexte de la présente norme, les systèmes, *installations* et équipements suivants détenus par une entité responsable indiquée à la section 4.1 sont visés par les exigences. Si certaines exigences visent plus spécifiquement un type ou un sous-ensemble de systèmes, d'*installations* ou d'équipements, ceux-ci sont précisés explicitement.

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

4.2.1.1. 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 des délestages de *charge* automatiques de 300 MW ou plus sous la commande d'un système commun détenu par l'entité responsable, sans intervention humaine.

4.2.1.2. *Automatisme de réseau* (*RAS*) visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou de l'*entité régionale*.

4.2.1.3. *Système de protection* de réseau de *transport* (à l'exclusion des systèmes de DSF et de DST) visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou de l'*entité régionale*.

4.2.1.4. *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* :

4.2.2.1. Toutes les *installations* du *BES*.

4.2.3. Exemptions : Sont exemptés de la norme CIP-013-1 :

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

4.2.3.2. Les *actifs électroniques* associés aux réseaux de communication et aux liaisons d'échange de données entre *périmètres de sécurité électronique* (*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.

4.2.3.5. Les entités responsables qui ont déterminé n'avoir aucun *système électronique BES* classé dans les catégories « impact élevé » ou « impact moyen » selon le processus d'inventaire et de catégorisation prescrit dans la norme de fiabilité CIP-002-5 ou toute version postérieure.

5. **Date d'entrée en vigueur :** Voir le plan de mise en œuvre du projet 2016-03.

B. Exigences et mesures

E1. Chaque entité responsable doit établir un ou des plans documentés de gestion des risques de cybersécurité dans la chaîne d'approvisionnement pour les *systèmes électroniques BES* à impact moyen ou élevé. Ce ou ces plans doivent comprendre les éléments suivants : *[Facteur de risque de non-conformité : moyen] [Horizon : planification de l'exploitation]*

1.1. Un ou des processus utilisés dans la planification de l'acquisition de *systèmes électroniques BES* afin de déterminer et d'évaluer les risques de cybersécurité pour le *BES* liés aux produits ou services de fournisseurs, résultant : i) de l'acquisition et de l'installation d'équipements et de logiciels de fournisseurs ; et ii) d'une transition entre fournisseurs.

1.2. Un ou des processus utilisés dans l'acquisition de *systèmes électroniques BES*, qui prévoient les mesures suivantes, selon le cas :

1.2.1. la notification par le fournisseur des incidents constatés par celui-ci relativement aux produits ou services livrés à l'entité responsable et qui présentent pour celle-ci un risque de cybersécurité ;

1.2.2. la coordination des réponses aux incidents constatés par le fournisseur relativement aux produits ou services livrés à l'entité responsable et qui présentent pour celle-ci un risque de cybersécurité ;

1.2.3. la notification par le fournisseur lorsqu'il n'y a plus lieu d'accorder à ses représentants un accès distant ou local ;

1.2.4. la divulgation par le fournisseur de vulnérabilités connues touchant des produits ou services livrés à l'entité responsable ;

1.2.5. la vérification de l'intégrité et de l'authenticité de tous les logiciels et correctifs livrés par le fournisseur et destinés à un *système électronique BES* ; et

1.2.6. la coordination des contrôles visant i) les *accès distants interactifs* commandés par un fournisseur, et ii) les accès distants par l'entremise de systèmes de fournisseurs.

M1. Les pièces justificatives doivent comprendre un ou des plans documentés de gestion des risques de cybersécurité dans la chaîne d'approvisionnement, conformément à l'exigence.

E2. Chaque entité responsable doit mettre en œuvre le ou les plans de gestion des risques de cybersécurité dans la chaîne d'approvisionnement prescrits à l'exigence E1. *[Facteur de risque de non-conformité : moyen] [Horizon : planification de l'exploitation]*

Remarque : La mise en œuvre d'un plan n'oblige pas l'entité responsable à renégocier ou à résilier des contrats existants (y compris les modifications aux ententes-cadres ou les bons de commande). En outre, l'exigence E2 ne s'étend pas : 1) aux modalités mêmes d'un contrat d'approvisionnement ; et 2) à l'exécution et au respect du contrat par le fournisseur.

M2. Les pièces justificatives doivent comprendre une documentation attestant la mise en œuvre du ou des plans de gestion des risques de cybersécurité dans la chaîne d'approvisionnement. Exemples non limitatifs de pièces justificatives : documents de correspondance, de politique ou de travail témoignant de l'utilisation de tels plans.

E3. Chaque entité responsable doit réexaminer et faire approuver par le *cadre supérieur CIP* ou son délégataire, au moins une fois tous les 15 mois civils, le ou les plans de gestion des risques de cybersécurité dans la chaîne d'approvisionnement prescrits à l'exigence E1.
[Facteur de risque de non-conformité : moyen] [Horizon : planification de l'exploitation]

M3. Les pièces justificatives doivent comprendre le ou les plans datés de gestion des risques de cybersécurité dans la chaîne d'approvisionnement approuvés par le *cadre supérieur CIP* ou son délégataire ainsi que des pièces justificatives supplémentaires attestant le réexamen de ce ou ces plans. Exemples non limitatifs de pièces justificatives : documents de politique, historique de révisions, dossiers de réexamen ou preuves de flux de travail provenant d'un système de gestion documentaire attestant que chaque plan de gestion des risques de cybersécurité dans la chaîne d'approvisionnement a fait l'objet d'un réexamen au moins une fois tous les 15 mois civils, ainsi que l'approbation documentée par le *cadre supérieur CIP* ou son délégataire.

C. Conformité

1. Processus de surveillance de la conformité

1.1. Responsable des mesures pour assurer la conformité

Le terme « *responsable des mesures pour assurer la conformité* » (*CEA*) désigne la NERC ou l'*entité régionale*, ou toute entité désignée par un organisme gouvernemental pertinent, dans leurs rôles respectifs visant à surveiller et à assurer la conformité avec les normes de fiabilité obligatoires et exécutoires 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 afin de démontrer sa conformité. Dans les cas où la période de conservation indiquée est plus courte que le temps écoulé depuis l'audit le plus récent, le *CEA* peut demander à l'entité de fournir d'autres pièces justificatives attestant sa conformité pendant la période complète écoulée depuis l'audit le plus récent.

Chaque 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, dans le cadre d'une enquête, de conserver certaines pièces justificatives plus longtemps.

- Chaque entité responsable doit conserver des pièces justificatives pour chacune des exigences de la présente norme pendant trois années civiles.
- Si une entité responsable est jugée non conforme à une exigence, 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 dossiers de l'audit le plus récent ainsi que tous les dossiers d'audit subséquents demandés et présentés.

1.3. Programme de surveillance et de mise en application des normes

Selon la définition des règles de procédure de la NERC, l'expression « programme de surveillance et de mise en application des normes » désigne la liste des processus qui serviront à évaluer les données ou l'information afin de déterminer les résultats de conformité avec la norme de fiabilité.

Niveau de gravité de la non-conformité (VSL)

Ex.	Niveau de gravité de la non-conformité			
	VSL faible	**VSL modéré**	**VSL élevé**	**VSL critique**
E1.	L'entité responsable a établi un ou des plans documentés de gestion des risques de cybersécurité dans la chaîne d'approvisionnement, qui comprennent un ou des processus utilisés dans la planification de l'acquisition de *systèmes électroniques BES* afin de déterminer et d'évaluer les risques de cybersécurité pour le *BES* conformément à l'alinéa 1.1, et comprenant un ou des processus utilisés dans l'acquisition de *systèmes électroniques BES* conformément à l'alinéa 1.2, mais ce ou ces plans omettent une des prescriptions des alinéas 1.2.1 à 1.2.6.	L'entité responsable a établi un ou des plans documentés de gestion des risques de cybersécurité dans la chaîne d'approvisionnement, qui comprennent un ou des processus utilisés dans la planification de l'acquisition de *systèmes électroniques BES* afin de déterminer et d'évaluer les risques de cybersécurité pour le *BES* conformément à l'alinéa 1.1, et comprenant un ou des processus utilisés dans l'acquisition de *systèmes électroniques BES* conformément à l'alinéa 1.2, mais ce ou ces plans omettent au moins deux des prescriptions des alinéas 1.2.1 à 1.2.6.	L'entité responsable a établi un ou des plans documentés de gestion des risques de cybersécurité dans la chaîne d'approvisionnement, mais ce ou ces plans ne comprennent pas de processus utilisé dans la planification de l'acquisition de *systèmes électroniques BES* afin de déterminer et d'évaluer les risques de cybersécurité pour le *BES* conformément à l'alinéa 1.1, ou ne comprennent pas de processus utilisé dans l'acquisition de *systèmes électroniques BES* conformément à l'alinéa 1.2.	L'entité responsable a établi un ou des plans documentés de gestion des risques de cybersécurité dans la chaîne d'approvisionnement, mais ce ou ces plans ne comprennent pas de processus utilisé dans la planification de l'acquisition de *systèmes électroniques BES* afin de déterminer et d'évaluer les risques de cybersécurité pour le *BES* conformément à l'alinéa 1.1, et ne comprennent pas non plus de processus utilisé dans l'acquisition de *systèmes électroniques BES* conformément à l'alinéa 1.2. OU L'entité responsable n'a établi aucun plan documenté de gestion des risques de cybersécurité dans la chaîne d'approvisionnement, en contravention avec l'exigence.

Ex.	Niveau de gravité de la non-conformité			
	VSL faible	**VSL modéré**	**VSL élevé**	**VSL critique**
E2.	L'entité responsable a mis en œuvre son ou ses plans documentés de gestion des risques de cybersécurité dans la chaîne d'approvisionnement, comprenant un ou des processus utilisés dans la planification de l'acquisition de *systèmes électroniques BES* afin de déterminer et d'évaluer les risques de cybersécurité pour le *BES* conformément à l'alinéa 1.1 de l'exigence E1, et comprenant un ou des processus utilisés dans l'acquisition de *systèmes électroniques BES* conformément à l'alinéa 1.2 de l'exigence E1, mais cette mise en œuvre a omis une des prescriptions des alinéas 1.2.1 à 1.2.6.	L'entité responsable a mis en œuvre son ou ses plans documentés de gestion des risques de cybersécurité dans la chaîne d'approvisionnement, comprenant un ou des processus utilisés dans la planification de l'acquisition de *systèmes électroniques BES* afin de déterminer et d'évaluer les risques de cybersécurité pour le *BES* conformément à l'alinéa 1.1 de l'exigence E1, et comprenant un ou des processus utilisés dans l'acquisition de *systèmes électroniques BES* conformément à l'alinéa 1.2 de l'exigence E1, mais cette mise en œuvre a omis au moins deux des prescriptions des alinéas 1.2.1 à 1.2.6.	L'entité responsable a mis en œuvre son ou ses plans documentés de gestion des risques de cybersécurité dans la chaîne d'approvisionnement, mais sans mettre en œuvre un ou des processus utilisés dans la planification de l'acquisition de *systèmes électroniques BES* afin de déterminer et d'évaluer les risques de cybersécurité pour le *BES* conformément à l'alinéa 1.1 de l'exigence E1, ou sans mettre en œuvre un ou des processus utilisés dans l'acquisition de *systèmes électroniques BES* conformément à l'alinéa 1.2 de l'exigence E1.	L'entité responsable a mis en œuvre son ou ses plans documentés de gestion des risques de cybersécurité dans la chaîne d'approvisionnement, mais sans mettre en œuvre un ou des processus utilisés dans la planification de l'acquisition de *systèmes électroniques BES* afin de déterminer et d'évaluer les risques de cybersécurité pour le *BES* conformément à l'alinéa 1.1 de l'exigence E1, et sans non plus mettre en œuvre un ou des processus utilisés dans l'acquisition de *systèmes électroniques BES* conformément à l'alinéa 1.2 de l'exigence E1. OU L'entité responsable n'a mis en œuvre aucun plan documenté de gestion des risques de cybersécurité dans la chaîne d'approvisionnement, en contravention avec l'exigence.

Ex.	Niveau de gravité de la non-conformité			
	VSL faible	**VSL modéré**	**VSL élevé**	**VSL critique**
E3.	L'entité responsable a réexaminé et fait approuver par le *cadre supérieur CIP* ou son délégataire son ou ses plans de gestion des risques de cybersécurité dans la chaîne d'approvisionnement, mais dans un délai de plus de 15 mois civils et d'au plus 16 mois civils suivant le réexamen précédent.	L'entité responsable a réexaminé et fait approuver par le *cadre supérieur CIP* ou son délégataire son ou ses plans de gestion des risques de cybersécurité dans la chaîne d'approvisionnement, mais dans un délai de plus de 16 mois civils et d'au plus 17 mois civils suivant le réexamen précédent.	L'entité responsable a réexaminé et fait approuver par le *cadre supérieur CIP* ou son délégataire son ou ses plans de gestion des risques de cybersécurité dans la chaîne d'approvisionnement, mais dans un délai de plus de 17 mois civils et d'au plus 18 mois civils suivant le réexamen précédent.	L'entité responsable n'a pas réexaminé et fait approuver par le *cadre supérieur CIP* ou son délégataire son ou ses plans de gestion des risques de cybersécurité dans la chaîne d'approvisionnement dans un délai de 18 mois civils suivant le réexamen précédent.

D. Différences régionales

Aucune.

E. Documents connexes

Lien vers le plan de mise en œuvre et d'autres documents connexes importants.

Historique des versions

Version	Date	Intervention	Suivi des modifications
1	20 juillet 2017	Mise en œuvre de l'Ordonnance 829 de la FERC.	
1	10 août 2017	Approbation par le Conseil d'administration de la NERC.	

Justification

Exigence E1

L'exigence proposée met en œuvre les prescriptions de l'Ordonnance 829 de la FERC concernant la mise en œuvre par les entités d'un ou de plans spécifiant un processus d'atténuation des risques de cybersécurité dans la chaîne d'approvisionnement. Ce ou ces plans doivent répondre aux quatre objectifs suivants (Ordonnance 829, paragraphe 45) :

1) intégrité et authenticité des logiciels ;

2) accès distant par les fournisseurs ;

3) planification des systèmes d'information ; et

4) gestion des risques liés aux fournisseurs et contrôles d'approvisionnement.

Le ou les plans de gestion des risques de cybersécurité prescrits à l'exigence E1 s'appliquent aux *systèmes électroniques BES* à impact moyen ou élevé.

La mise en œuvre d'un plan de gestion des risques de cybersécurité n'oblige pas l'entité responsable à renégocier ou à résilier des contrats existants (y compris les modifications aux ententes-cadres ou les bons de commande), comme le précise l'Ordonnance 829 (paragraphe 36).

L'alinéa 1.1 de l'exigence E1 met en œuvre la prescription de l'Ordonnance 829 qui demande de déterminer et de documenter les risques de cybersécurité au cours du processus de planification et de préparation en amont de l'acquisition de *systèmes électroniques BES* (paragraphe 56). L'objectif de sécurité est d'une part d'amener les entités à envisager les risques de cybersécurité pour le *BES* liés aux produits et services de fournisseurs, résultant : i) de l'acquisition et de l'installation d'équipements et de logiciels de fournisseurs ; et ii) d'une transition entre fournisseurs. D'autre part, les entités doivent être amenées à envisager les moyens d'atténuer ces risques à l'étape de planification des *systèmes électroniques BES*.

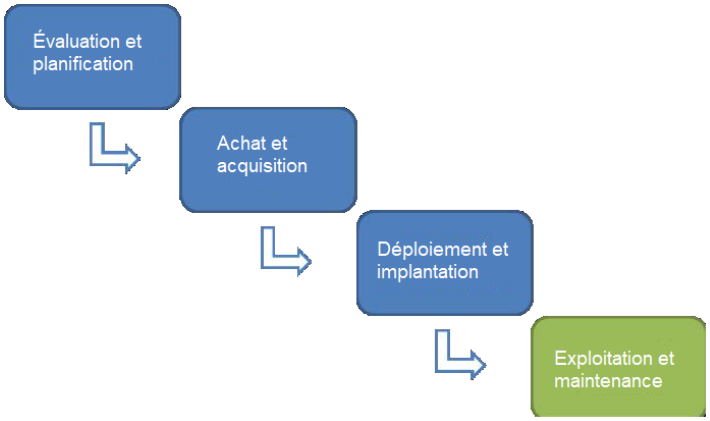
L'alinéa 1.2 de l'exigence E1 met en œuvre la prescription de l'Ordonnance 829 qui demande que des contrôles d'approvisionnement assurent l'intégration et l'application des concepts de sécurité dans les contrats futurs de *systèmes électroniques BES* (paragraphe 59). L'objectif visé est que les entités incorporent ces concepts dans leurs plans de manière que les risques pertinents soient pris en compte dans le processus d'acquisition et dans les négociations contractuelles. La mise en œuvre du plan de gestion des risques prescrit à l'alinéa 1.2 peut être réalisée dans le cadre des processus d'acquisition et de négociation contractuelle de l'entité. Par exemple, l'entité responsable peut intégrer les critères pertinents de son plan dans les appels de propositions, les négociations avec les fournisseurs, ou encore les demandes transmises à des entités chargées de négocier en son nom (ententes d'achat coopératif, etc.). L'intégration de certains contrôles dans le contrat négocié n'est pas toujours possible ; dans de tels cas, on ne considère pas que la mise en œuvre du plan de l'entité a échoué. Par ailleurs, bien qu'on s'attende à ce que l'entité responsable veille à faire respecter les dispositions contractuelles relatives à la sécurité, la mise en exécution du contrat et le respect de celui-ci par le fournisseur ne sont pas visés par cette norme de fiabilité.

L'exigence de vérifier l'intégrité et l'authenticité des logiciels (alinéa 1.2.5) vise à ce que les logiciels installés dans des *systèmes électroniques BES* ne soient pas modifiés à l'insu de leur fournisseur avant l'installation, et qu'ils ne soient pas contrefaits. L'alinéa 1.2.5 n'est pas une exigence opérationnelle qui oblige l'entité à effectuer une telle vérification ; il demande plutôt à l'entité de tenir compte de l'enjeu de l'intégrité et de l'authenticité des logiciels dans son processus contractuel, afin d'avoir ensuite les moyens de réaliser cette vérification dans le cadre de la norme CIP-010-3.

Le terme « fournisseur » utilisé dans cette norme désigne uniquement les personnes, entreprises ou autres organisations avec lesquelles l'entité responsable, ou une société affiliée, est en relation contractuelle en vue de la fourniture de *systèmes électroniques BES* et de services connexes. Ce terme exclut les autres entités inscrites auprès de la NERC qui fournissent des services de fiabilité (par exemple, des services de *responsable de l'équilibrage* ou de *coordonnateur de la fiabilité* dans le cadre des normes de fiabilité de la NERC). Un fournisseur, selon l'emploi de ce terme dans la norme, peut comprendre : i) des créateurs de logiciels ou de systèmes d'information, des fabricants de composants de système ou des prestataires de services informatiques ; ii) des revendeurs de produits ; ou iii) des intégrateurs de systèmes.

Collectivement, les dispositions de la norme CIP-013-1 concernent les contrôles d'une entité visant à gérer les risques de cybersécurité pour les *systèmes électroniques BES* pendant les phases de planification, d'acquisition et de déploiement du cycle de vie du système, selon le schéma ci-après.

Schéma du cycle de vie d'un *système électronique BES*



Exigence E2

L'exigence proposée met en œuvre les prescriptions de l'Ordonnance 829 qui demandent aux entités de réévaluer périodiquement certains contrôles de gestion des risques de cybersécurité dans la chaîne d'acquisition (paragraphe 46).

Ces réévaluations périodiques permettent aux entités de tenir leurs plans à jour et de répondre aux inquiétudes et aux vulnérabilités, existantes ou émergentes, concernant la chaîne d'approvisionnement. Les entités peuvent, par exemple, prendre en compte les directives ou autres informations provenant :

- de la NERC ou de l'E-ISAC ;
- de l'ICS-CERT ;
- du Centre canadien de réponse aux incidents cybernétiques (CCRIC).

Les entités responsables ne sont pas obligées de renégocier ou de résilier des contrats existants (y compris des modifications aux ententes-cadres ou des bons de commande) lorsqu'elles mettent en œuvre un plan mis à jour ; la note de l'exigence E2 s'applique à la mise en œuvre non seulement des nouveaux plans, mais aussi des plans mis à jour).