Normes de fiabilité (version française)

A. Introduction

1. Titre : Cybersécurité — Catégorisation des systèmes électroniques BES

2. Numéro : CIP-002-5.1a

3. Objet : Inventorier et catégoriser les *systèmes électroniques BES* et leurs *actifs électroniques BES* connexes, pour l'application des exigences de cybersécurité proportionnelle à l'impact négatif que la perte, la compromission ou la mauvaise utilisation de ces *systèmes électroniques BES* pourrait avoir sur l'exploitation fiable du *BES*. L'inventaire et la catégorisation des *systèmes électroniques BES* permettent d'établir une protection appropriée contre les compromissions qui pourraient entraîner un fonctionnement incorrect ou une instabilité du *BES*.

4. Applicabilité :

4.1. Entités fonctionnelles : Dans le contexte des exigences de la présente norme, les entités fonctionnelles indiquées ci-après seront appelées collectivement les « entités responsables ». Dans le cas des exigences de cette norme qui visent une entité fonctionnelle particulière ou un sous-ensemble particulier d'entités fonctionnelles, la ou les entités fonctionnelles sont précisées explicitement.

4.1.1. ***Responsable de l'équilibrage***

4.1.2. ***Distributeur* qui possède** un ou plusieurs des systèmes, *installations* et équipements suivants pour la protection ou la remise en charge du *BES* :

4.1.2.1. Chaque système de délestage de charge en sous-fréquence (DSF) ou de délestage de charge en sous-tension (DST) qui :

4.1.2.1.1. fait partie d'un programme de délestage de *charge* visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou de l'*entité régionale*, et

4.1.2.1.2. effectue du délestage automatique de *charge* de 300 MW ou plus par un système de commande commun détenu par l'entité responsable, sans intervention humaine.

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

4.1.2.3. Chaque *système de protection* applicable au *transport* (excluant les systèmes DSF et DST) visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou de l'*entité régionale*.

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

4.1.3. ***Exploitant d'installation de production***

4.1.4. ***Propriétaire d'installation de production***

4.1.5. ***Coordonnateur des échanges* ou *responsable des échanges***

4.1.6. ***Coordonnateur de la fiabilité***

4.1.7. ***Exploitant de réseau de transport***

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

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

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

4.2.1.1. Chaque système DSF ou DST qui :

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

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

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

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

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

4.2.2. **Entités responsables indiquées en 4.1, sauf les *distributeurs*** :
Toutes les *installations* du *BES*.

4.2.3. **Exemptions :** Sont exemptés de la norme CIP-002-5.1a :

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, 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 :

1. **24 mois minimum** – La norme CIP-002-5.1a entrera en vigueur soit le 1er juillet 2015, soit le premier jour civil du neuvième trimestre civil suivant l'entrée en vigueur de l'ordonnance d'approbation réglementaire appropriée, selon le délai le plus long.
2. Dans les territoires où aucune approbation réglementaire n'est requise, la norme CIP-002-5.1a entrera en vigueur le premier jour du neuvième trimestre civil suivant l'approbation par le Conseil d'administration, ou selon les modalités d'approbation prévues par la loi pour les organismes gouvernementaux chargés de la fiabilité électrique (ERO).

6. Contexte :

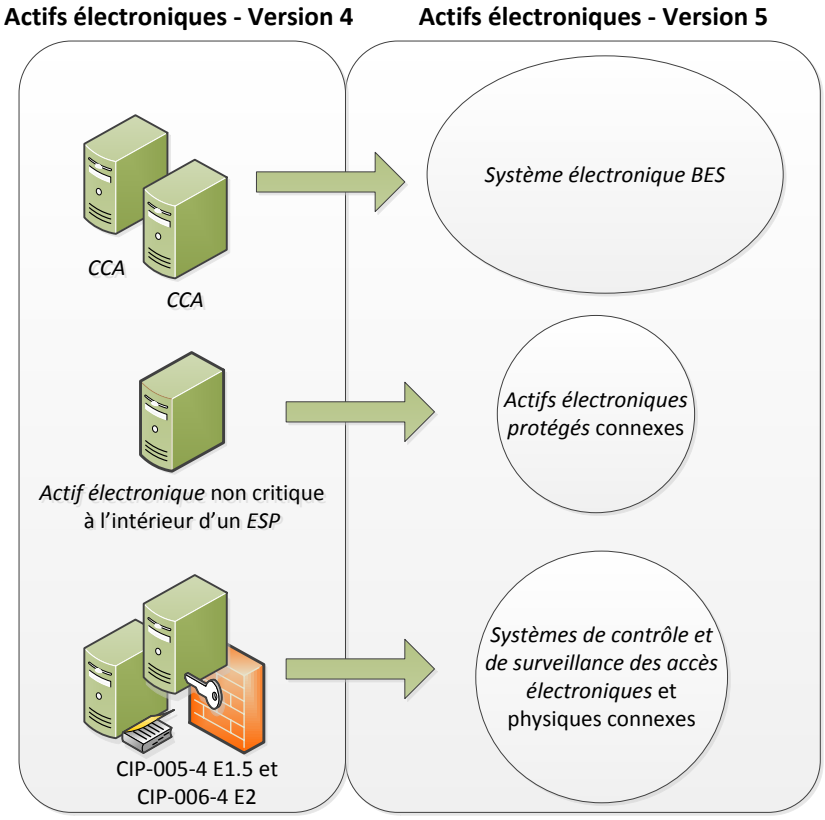
La présente norme fournit des critères précis pour que les entités responsables visées catégorisent leurs *systèmes électroniques BES* en se basant sur l'impact de leurs *installations*, systèmes et équipements qui y sont associés, lesquels, s'ils étaient détruits, dégradés, mal utilisés ou autrement rendus indisponibles, affecteraient l'exploitation fiable du *système de production-transport d'électricité*. La démarche de cette norme est basée sur plusieurs concepts.

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 et les critères de l'annexe 1 de la norme CIP-002 utilisent un seuil de 300 MW pour les systèmes DSF et DST. Ce seuil particulier de 300 MW pour les systèmes DSF et DST provient de la version 1 des normes CIP sur la cybersécurité. Ce seuil demeure à 300 MW puisqu'il concerne spécifiquement les systèmes DST et DSF, qui constituent des efforts de dernier recours pour sauver le *système de production-transport d'électricité*. Un examen des tolérances des systèmes DSF définies dans les normes de fiabilité régionales pour les exigences des programmes DSF à ce jour indique que la valeur historique de 300 MW représente une valeur de seuil adéquate et raisonnable pour les tolérances d'exploitation admissibles des systèmes DSF.

Systèmes électroniques BES

Une des différences fondamentales entre les versions 4 et 5 des normes CIP sur la cybersécurité est le passage de la désignation des *actifs électroniques critiques* vers la désignation des *systèmes électroniques BES*. Ce changement résulte de l'examen du cadre de gestion du risque du NIST par l'équipe de rédaction et de l'utilisation d'un terme analogue, « système d'information », comme cible pour la catégorisation et l'application des mesures de sécurité.



Dans la transition de la version 4 vers la version 5, un *système électronique BES* peut être simplement considéré comme un regroupement d'*actifs électroniques critiques* (tel que ce terme est utilisé dans la version 4). Les normes CIP sur la cybersécurité utilisent le terme « *système électronique BES* » essentiellement pour désigner plus généralement l'objet d'une exigence. Par exemple, il devient possible d'appliquer des exigences concernant le rétablissement et la protection contre les maliciels à un groupe plutôt qu'à des *actifs électroniques* individuels ; ainsi, il devient plus clair dans l'exigence que la protection contre les maliciels s'applique au système dans son ensemble et que la conformité individuelle de chaque dispositif peut ne pas être nécessaire.

Une autre raison d'utiliser le terme « *système électronique BES* » est de fournir un niveau pratique auquel une entité responsable peut organiser la mise en œuvre

documentée des exigences et des pièces justificatives de conformité. Les entités responsables peuvent utiliser le concept bien développé de plan de sécurité pour chaque *système électronique BES* afin de documenter les programmes, processus et plans en place visant à se conformer aux exigences de sécurité.

Il est laissé à la discrétion de l'entité responsable de déterminer le niveau de granularité pour délimiter un *système électronique BES*, compte tenu des éléments de la définition de *système électronique BES*. Par exemple, l'entité responsable pourrait choisir de considérer l'ensemble d'un système de commande de centrale comme un seul *système électronique BES*, ou choisir de considérer certaines parties de ce système comme des *systèmes électroniques BES* distincts. L'entité responsable devrait prendre en considération le contexte opérationnel et le cadre de gestion lorsqu'elle définit les limites d'un *système électronique BES*, de manière à maximiser l'efficience de son fonctionnement sécurisé. Définir des limites trop étroites pourrait entraîner des redondances dans les processus administratifs et les autorisations, tandis que définir des limites trop larges pourrait rendre le fonctionnement sécurisé du *système électronique BES* difficile à surveiller et à évaluer.

Exploitation fiable du *BES*

La portée d'application des normes CIP sur la cybersécurité est limitée aux *systèmes électroniques BES* qui auraient un impact sur l'exploitation fiable du *BES*. Afin d'identifier les *systèmes électroniques BES*, les entités responsables déterminent si le *système électronique BES* effectue ou soutient une des fonctions de fiabilité du *BES* selon les tâches de fiabilité associées à leur fonction de fiabilité et les responsabilités correspondantes de l'entité fonctionnelle, définies par ses relations avec les autres entités fonctionnelles dans le modèle fonctionnel de la NERC. Cela fait en sorte que la portée d'application **initiale** inclut seulement les *systèmes électroniques BES* et leurs *actifs électroniques BES* connexes qui assurent ou soutiennent l'exploitation fiable du *BES*. La définition du terme « *actif électronique BES* » fournit la base de cette portée d'application.

Exploitation en temps réel

Une caractéristique de l'*actif électronique BES* est sa portée d'application en temps réel. L'horizon temporel qui est significatif pour les *systèmes électroniques BES* et les *actifs électroniques BES* visés par l'application de la version 5 des normes CIP sur la cybersécurité est défini comme étant celui qui est important pour l'exploitation fiable en temps réel du *BES*. Pour décrire l'horizon temporel de façon plus précise qu'au moyen de l'expression « *temps réel* », les *actifs électroniques BES* sont des *actifs électroniques* qui, s'ils devenaient indisponibles, dégradés ou mal utilisés, auraient un impact négatif sur le fonctionnement fiable du *BES* dans les 15 minutes du début de la compromission. Cette fenêtre de temps ne doit pas tenir compte ici de l'activation d'*actifs électroniques BES* ou de *systèmes électroniques BES* redondants : du point de vue de la cybersécurité, la redondance n'atténue pas les vulnérabilités de cybersécurité.

Critères de catégorisation

Les critères énoncés à l'annexe 1 servent à catégoriser les *systèmes électroniques BES* en catégories d'impact. L'exigence E1 demande de dresser la liste des *systèmes électroniques BES* classés dans les catégories Impact élevé et Impact moyen seulement. Tous les *systèmes électroniques BES* d'*installations* auxquelles ne s'appliquent pas les critères de catégorisation 1.1 à 1.4 et 2.1 à 2.11 de l'annexe 1 – Critères d'évaluation de l'impact tombent par défaut dans la catégorie Impact faible.

Ce processus général de catégorisation des *systèmes électroniques BES* en fonction de l'impact sur l'exploitation fiable du *BES* est cohérent avec l'approche de gestion du risque aux fins de l'application des exigences de cybersécurité dans le reste des normes CIP sur la cybersécurité version 5.

Systèmes de contrôle ou de surveillance des accès électroniques*, *systèmes de contrôle des accès physiques* et *actifs électroniques protégés* associés aux *systèmes électroniques BES

Les *systèmes électroniques BES* comportent des *actifs électroniques* associés qui, s'ils sont compromis, présentent une menace pour le *système électronique BES* en raison : a) de leur emplacement à l'intérieur du *périmètre de sécurité électronique* (*actifs électroniques protégés*), ou b) de la fonction de contrôle de sécurité qu'ils remplissent (*systèmes de contrôle ou de surveillance des accès électroniques* et *systèmes de contrôle des accès physiques*). Ces *actifs électroniques* comprennent :

***Systèmes de contrôle ou de surveillance des accès électroniques* (*EACMS*)** – Exemples : *points d'accès électroniques*, *systèmes intermédiaires*, serveurs d'authentification (serveurs Radius, serveurs Active Directory, autorités de certification, etc.), systèmes de surveillance des événements de sécurité et systèmes de détection des intrusions.

***Systèmes de contrôle des accès physiques* (*PACS*)** – Exemples : serveurs d'authentification et systèmes d'accès à carte ou à porte-nom.

***Actifs électroniques protégés* (*PCA*)** – Exemples, dans la mesure où ils se trouvent à l'intérieur de l'ESP : serveurs de fichiers, serveurs FTP, serveurs de temps, commutateurs de réseau local, imprimantes réseau, enregistreurs numériques de défauts et systèmes de surveillance des émissions.

B. Exigences et mesures

E1. Chaque entité responsable doit mettre en œuvre un processus qui examine chacun des actifs suivants aux fins des alinéas 1.1 à 1.3 : *[Facteur de risque de non-conformité : élevé] [Horizon : planification de l'exploitation]*

- **i.** *centres de contrôle* et *centres de contrôle* de repli ;
- **ii.** postes de transport ;
- **iii.** ressources de production ;
- **iv.** systèmes et installations essentiels à la remise en charge du réseau, y compris les *ressources à démarrage autonome* et les *chemins de démarrage* ainsi que les exigences relatives aux manœuvres initiales ;
- **v.** *automatismes de réseau* qui contribuent à la fiabilité du *système de production-transport d'électricité* ; et
- **vi.** pour les *distributeurs*, *systèmes de protection* indiqués à l'alinéa 4.2.1 de la section Applicabilité ci-dessus.

1.1. répertorier chacun des *systèmes électroniques BES* à impact élevé, selon la section 1 de l'annexe 1, s'il y en a, dans chaque actif ;

1.2. répertorier chacun des *systèmes électroniques BES* à impact moyen, selon la section 2 de l'annexe 1, s'il y en a, dans chaque actif ; et

1.3. répertorier chaque actif qui comporte un *système électronique BES* à impact faible, selon la section 3 de l'annexe 1, s'il y en a (une liste des *systèmes électroniques BES* à impact faible n'est pas exigée).

M1. Les pièces justificatives acceptables comprennent, sans s'y limiter, les listes électroniques ou papier datées requises en vertu de l'exigence E1 et de ses alinéas 1.1 et 1.2.

E2. L'entité responsable doit : *[Facteur de risque de non-conformité : faible] [Horizon : planification de l'exploitation]*

2.1 passer en revue les répertoires établis selon l'exigence E1 et ses alinéas (et les mettre à jour en cas de changement constaté) au moins une fois tous les 15 mois civils, même si aucun élément n'a été répertorié selon l'exigence E1 ; et

2.2 faire approuver par son *cadre supérieur CIP* ou son délégué les répertoires établis selon l'exigence E1 au moins une fois tous les 15 mois civils, même si aucun élément n'a été répertorié selon l'exigence E1.

M2. Les pièces justificatives acceptables comprennent, sans s'y limiter, des documents électroniques ou papier datés attestant que l'entité responsable a passé en revue et mis à jour, lorsque nécessaire, les identifications exigées selon l'exigence E1 et ses alinéas, et qu'elle a fait approuver par son *cadre supérieur CIP* ou son délégué les répertoires établis selon l'exigence E1 et ses alinéas au moins une fois tous les 15 mois

civils, même si aucun élément n'a été répertorié selon l'exigence E1 et ses alinéas, conformément à l'exigence E2.

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 visée soit détenue, exploitée ou contrôlée par l'*entité régionale*. Dans de tels cas, l'organisation de fiabilité électrique (ERO), une *entité régionale* approuvée par la FERC ou un autre organisme gouvernemental pertinent joue le rôle du *CEA*.

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 les pièces justificatives attestant sa conformité selon les modalités indiquées 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	Niveaux de gravité de la non-conformité (CIP-002-5.1)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
E1	**Planification de l'exploitation**	**Élevé**	Pour les entités responsables qui ont plus de 40 actifs *BES* au total à l'exigence E1, 5 % ou moins des actifs *BES* n'ont pas été examinés selon l'exigence E1. OU Pour les entités responsables qui ont 40 actifs *BES* au total ou moins, deux actifs *BES* ou moins à l'exigence E1 n'ont pas été examinés selon l'exigence E1. OU Pour les entités responsables qui ont plus de 100 *systèmes électroniques BES* à impact élevé ou moyen au total, 5 % ou moins des *systèmes*	Pour les entités responsables qui ont plus de 40 actifs *BES* au total à l'exigence E1, plus de 5 %, mais au plus 10 % des actifs *BES* n'ont pas été examinés selon l'exigence E1. OU Pour les entités responsables qui ont 40 actifs *BES* au total ou moins, plus de deux, mais au plus quatre actifs *BES* à l'exigence E1 n'ont pas été examinés selon l'exigence E1. OU Pour les entités responsables qui ont plus de 100 *systèmes électroniques BES* à impact élevé ou moyen au total, plus de	Pour les entités responsables qui ont plus de 40 actifs *BES* au total à l'exigence E1, plus de 10 %, mais au plus 15 % des actifs *BES* n'ont pas été examinés selon l'exigence E1. OU Pour les entités responsables qui ont 40 actifs *BES* au total ou moins, plus de quatre, mais au plus six actifs *BES* à l'exigence E1 n'ont pas été examinés selon l'exigence E1. OU Pour les entités responsables qui ont plus de 100 *systèmes électroniques BES* à impact élevé ou moyen au total, plus de	Pour les entités responsables qui ont plus de 40 actifs *BES* au total à l'exigence E1, plus de 15 % des actifs *BES* n'ont pas été examinés selon l'exigence E1. OU Pour les entités responsables qui ont 40 actifs *BES* au total ou moins, plus de six actifs *BES* à l'exigence E1 n'ont pas été examinés selon l'exigence E1. OU Pour les entités responsables qui ont plus de 100 *systèmes électroniques BES* à impact élevé ou moyen au total, plus de 15 % des *systèmes*

Ex.	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-002-5.1)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
			électroniques BES répertoriés n'ont pas été catégorisés ou ont été incorrectement catégorisés dans une catégorie inférieure. OU Pour les entités responsables qui ont 100 *systèmes électroniques BES* à impact élevé ou moyen ou moins au total, cinq des *systèmes électroniques BES* répertoriés ou moins n'ont pas été catégorisés ou ont été incorrectement catégorisés dans une catégorie inférieure. OU Pour les entités responsables qui ont plus de 100 *systèmes électroniques BES*	5 %, mais au plus 10 % des *systèmes électroniques BES* répertoriés n'ont pas été catégorisés ou ont été incorrectement catégorisés dans une catégorie inférieure. OU Pour les entités responsables qui ont 100 *systèmes électroniques BES* à impact élevé ou moyen ou moins au total, plus de cinq, mais au plus 10 *systèmes électroniques BES* répertoriés n'ont pas été catégorisés ou ont été incorrectement catégorisés dans une catégorie inférieure. OU Pour les entités responsables qui ont	10 %, mais au plus 15 % des *systèmes électroniques BES* répertoriés n'ont pas été catégorisés ou ont été incorrectement catégorisés dans une catégorie inférieure. OU Pour les entités responsables qui ont 100 *systèmes électroniques BES* à impact élevé ou moyen ou moins au total, plus de 10, mais au plus 15 *systèmes électroniques BES* répertoriés n'ont pas été catégorisés ou ont été incorrectement catégorisés dans une catégorie inférieure. OU Pour les entités responsables qui ont	*électroniques BES* répertoriés n'ont pas été catégorisés ou ont été incorrectement catégorisés dans une catégorie inférieure. OU Pour les entités responsables qui ont 100 *systèmes électroniques BES* à impact élevé ou moyen ou moins au total, plus de 15 *systèmes électroniques BES* répertoriés n'ont pas été catégorisés ou ont été incorrectement catégorisés dans une catégorie inférieure. OU Pour les entités responsables qui ont plus de 100 *systèmes électroniques BES*

Ex.	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-002-5.1)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
			à impact élevé ou moyen au total, 5 % ou moins des *systèmes électroniques BES* à impact élevé ou moyen n'ont pas été répertoriés. OU Pour les entités responsables qui ont 100 *systèmes électroniques BES* à impact élevé ou moyen ou moins au total, cinq *systèmes électroniques BES* à impact élevé ou moyen ou moins n'ont pas été répertoriés.	plus de 100 *systèmes électroniques BES* à impact élevé ou moyen au total, plus de 5 %, mais au plus 10 % des *systèmes électroniques BES* à impact élevé ou moyen n'ont pas été répertoriés. OU Pour les entités responsables qui ont 100 *systèmes électroniques BES* à impact élevé ou moyen ou moins au total, plus de cinq, mais au plus 10 *systèmes électroniques BES* à impact élevé ou moyen ou moins n'ont pas été répertoriés.	plus de 100 *systèmes électroniques BES* à impact élevé ou moyen au total, plus de 10 %, mais au plus 15 % des *systèmes électroniques BES* à impact élevé ou moyen n'ont pas été répertoriés. OU Pour les entités responsables qui ont 100 *systèmes électroniques BES* à impact élevé ou moyen ou moins au total, plus de 10, mais au plus 15 *systèmes électroniques BES* à impact élevé ou moyen ou moins n'ont pas été répertoriés.	à impact élevé ou moyen au total, plus de 15 % des *systèmes électroniques BES* à impact élevé ou moyen n'ont pas été répertoriés. OU Pour les entités responsables qui ont 100 *systèmes électroniques BES* à impact élevé ou moyen ou moins au total, plus de 15 *systèmes électroniques BES* à impact élevé ou moyen n'ont pas été répertoriés.
E2	**Planification de l'exploitation**	**Faible**	L'entité responsable n'a pas effectué son passage en revue et sa	L'entité responsable n'a pas effectué son passage en revue et sa	L'entité responsable n'a pas effectué son passage en revue et sa	L'entité responsable n'a pas effectué son passage en revue et sa

Ex.	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-002-5.1)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
			mise à jour des répertoires établis selon E1 dans les 15 mois civils, mais l'a fait au plus dans les 16 mois civils, du passage en revue précédent. (E2.1) OU L'entité responsable n'a pas obtenu l'approbation des répertoires établis selon E1 par le *cadre supérieur CIP* ou son délégué conformément à l'exigence E2 dans les 15 mois civils, mais l'a fait au plus dans les 16 mois civils de l'approbation précédente. (E2.2)	mise à jour des répertoires établis selon E1 dans les 16 mois civils, mais l'a fait au plus dans les 17 mois civils, du passage en revue précédent. (E2.1) OU L'entité responsable n'a pas obtenu l'approbation des répertoires établis selon E1 par le *cadre supérieur CIP* ou son délégué conformément à l'exigence E2 dans les 16 mois civils, mais l'a fait en au plus dans les 17 mois civils de l'approbation précédente. (E2.2)	mise à jour des répertoires établis selon E1 dans les 17 mois civils, mais l'a fait au plus dans les 18 mois civils, du passage en revue précédent. (E2.1) OU L'entité responsable n'a pas obtenu l'approbation des répertoires établis selon E1 par le *cadre supérieur CIP* ou son délégué conformément à l'exigence E2 dans les 17 mois civils, mais l'a fait en au plus dans les 18 mois civils de l'approbation précédente. (E2.2)	mise à jour des répertoires établis selon E1 dans les 18 mois civils du passage en revue précédent. (E2.1) OU L'entité responsable n'a pas obtenu l'approbation des répertoires établis selon E1 par le *cadre supérieur CIP* ou son délégué conformément à l'exigence E2 dans les 18 mois civils de l'approbation précédente. (E2.2)

D. Différences régionales

Aucune.

E. Interprétations

Aucune.

F. Documents connexes

Aucun.

CIP-002-5.1a – Annexe 1

Critères de degré d'impact

Les critères définis à la présente annexe ne sont pas des exigences de conformité autonomes, mais des éléments de caractérisation du degré d'impact auxquels renvoient les exigences.

1. Impact élevé (H)

Chaque *système électronique BES* utilisé par et situé dans une des installations suivantes :

1.1. Chaque *centre de contrôle* ou *centre de contrôle* de repli utilisé pour s'acquitter des obligations fonctionnelles du *coordonnateur de la fiabilité*.

1.2. Chaque *centre de contrôle* ou *centre de contrôle* de repli utilisé pour s'acquitter des obligations fonctionnelles du *responsable de l'équilibrage* pour : 1) une production totale de 3 000 MW ou plus dans une même *Interconnexion*, ou 2) au moins un actif qui répond au critère 2.3, 2.6 ou 2.9.

1.3. Chaque *centre de contrôle* ou *centre de contrôle* de repli utilisé pour s'acquitter des obligations fonctionnelles de l'*exploitant de réseau de transport* pour au moins un actif qui répond au critère 2.2, 2.4, 2.5, 2.7, 2.8, 2.9 ou 2.10.

1.4 Chaque *centre de contrôle* ou *centre de contrôle* de repli utilisé pour s'acquitter des obligations fonctionnelles de l'*exploitant d'installation de production* pour au moins un actif qui répond au critère 2.1, 2.3, 2.6 ou 2.9.

2. Impact moyen (M)

Chaque *système électronique BES,* non inclus dans la section 1 ci-dessus, associé à un des éléments suivants :

2.1. Production en service, pour chaque ensemble de groupes de production à une même centrale, dont la puissance active nominale nette totale la plus élevée des 12 mois civils précédents est de 1 500 MW ou plus dans une même *Interconnexion*. Pour chaque ensemble de groupes de production, les seuls *systèmes électroniques BES* qui répondent à ce critère sont les *systèmes électroniques BES* partagés qui pourraient, dans un délai de 15 minutes, avoir un impact négatif sur l'exploitation fiable de toute combinaison de groupes de production qui, ensemble, représentent 1 500 MW ou plus dans une même *Interconnexion*.

2.2. Chaque ressource ou groupe de ressources de puissance réactive du *BES* à un même emplacement (à l'exclusion des *installations* de production) dont la *puissance réactive* nominale maximale totale est de 1 000 Mvar ou plus (à l'exclusion de ceux aux *installations* de production). Les seuls *systèmes électroniques BES* qui répondent à ce

critère sont les *systèmes électroniques BES* partagés qui pourraient, dans un délai de 15 minutes, avoir un impact négatif sur l'exploitation fiable de toute combinaison de ressources qui au total représentent 1 000 Mvar ou plus.

2.3. Chaque *installation* de production que le *coordonnateur de la planification* ou le *planificateur de réseau de transport* désigne comme étant nécessaire pour éviter un *impact négatif sur la fiabilité* dans un horizon de planification de plus d'un an, et dont le *propriétaire d'installation de production* ou l'*exploitant d'installation de production* a été informé.

2.4. *Installations* de *transport* exploitées à 500 kV ou plus. Aux fins de ce critère, le jeu de barres collectrices d'une centrale de production n'est pas considéré comme une *installation* de *transport*, mais comme une partie de l'*installation* de raccordement de la production.

2.5. *Installations* de *transport* exploitées entre 200 et 499 kV dans un même poste, dans les cas où le poste est raccordé à une tension de 200 kV ou plus à au moins trois autres postes de *transport* et ayant une « valeur pondérée totale » de plus de 3 000 selon le tableau ci-dessous. La « valeur pondérée totale » pour un même poste est déterminée en faisant la somme des « valeurs pondérées par ligne » indiquées au tableau ci-dessous pour chaque *ligne de transport BES* d'arrivée et de départ qui le relie à un autre poste de *transport*. Aux fins de ce critère, le jeu de barres collectrices d'une centrale de production n'est pas considéré comme une *installation* de *transport*, mais comme une partie de l'*installation* de raccordement de la production.

Tension d'une ligne	Valeur pondérée par ligne
Moins de 200 kV (sans objet)	(sans objet)
200 à 299 kV	700
300 à 499 kV	1300
500 kV et plus	0

2.6. Groupes de production d'une même centrale ou *installations* de *transport* d'un même poste qui sont désignés par leur *coordonnateur de la fiabilité*, leur *responsable de la planification* ou leur *planificateur de réseau de transport* comme essentiels au calcul des *limites d'exploitation pour la fiabilité de l'Interconnexion* (*IROL*) et leurs contingences associées.

2.7. *Installations* de *transport* désignées comme essentielles pour respecter les *exigences relatives à l'interface de centrale nucléaire*.

2.8. *Installations* de *transport*, y compris les *installations* de raccordement de la production, qui fournissent le raccordement de la production nécessaire pour raccorder la sortie du groupe de production aux *réseaux* de *transport* et qui, si elles étaient détruites, dégradées, mal utilisées ou autrement rendues indisponibles,

entraîneraient la perte d'*installations* de production répertoriées par un *propriétaire d'installation de production* en vertu du critère 2.1 ou 2.3 de l'annexe 1.

2.9. Chaque *automatisme de réseau* (*SPS*), *plan de défense* (*RAS*) ou système de manœuvre automatisé qui commande des *éléments* du *BES* qui, s'ils étaient détruits, dégradés, mal utilisés ou autrement rendus indisponibles, provoqueraient le dépassement d'une ou de plusieurs *limites d'exploitation pour la fiabilité de l'Interconnexion* (*IROL*) en raison de leur défaut de fonctionner de la manière prévue ou entraîneraient la réduction d'une ou de plusieurs *IROL* s'ils étaient détruits, dégradés, mal utilisés ou autrement rendus indisponibles.

2.10. Chaque système ou groupe d'*éléments* qui effectue du délestage de *charge* automatique, en vertu d'un système de commande commun et sans intervention humaine, de 300 MW ou plus en mettant en œuvre du délestage de charge en sous-tension (DST) ou du délestage de charge en sous-fréquence (DSF) selon un programme de délestage de charge soumis à une ou plusieurs exigences d'une norme de fiabilité de la NERC ou régionale.

2.11. Chaque *centre de contrôle* ou *centre de contrôle* de repli, non inclus dans la catégorie Impact élevé (H) ci-dessus, utilisé pour s'acquitter des obligations fonctionnelles de l'*exploitant d'installation de production* pour une puissance active nominale nette totale maximale, pour les 12 mois civils précédents, de 1 500 MW ou plus dans une même *Interconnexion*.

2.12. Chaque *centre de contrôle* ou *centre de contrôle* de repli utilisé pour s'acquitter des obligations fonctionnelles de l'*exploitant de réseau de transport* non inclus dans la catégorie Impact élevé (H) ci-dessus.

2.13. Chaque *centre de contrôle* ou *centre de contrôle* de repli, non inclus dans la catégorie Impact élevé (H) ci-dessus, utilisé pour s'acquitter des obligations fonctionnelles du *responsable de l'équilibrage* pour une production de 1 500 MW ou plus dans une même *Interconnexion*.

3. Impact faible (L)

Systèmes électroniques BES non inclus dans les sections 1 et 2 ci-dessus, qui sont associés à l'un ou l'autre des actifs suivants et qui répondent aux critères d'applicabilité de l'alinéa 4.2. Installations de la section 4. Applicabilité de la présente norme :

3.1. *centres de contrôle* et *centres de contrôle* de repli ;

3.2. postes de transport ;

3.3. ressources de production ;

3.4. systèmes et installations essentiels à la remise en charge du réseau, y compris les *ressources à démarrage autonome* et les *chemins de démarrage* ainsi que les exigences relatives aux manœuvres initiales ;

3.5. *automatismes de réseau* qui soutiennent l'exploitation fiable du *système de production-transport d'électricité* ;

3.6. pour les *distributeurs*, *systèmes de protection* indiqués à l'alinéa 4.2.1. de la section Applicabilité ci-dessus.

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. 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 visés détenus par les *distributeurs*. Bien que le terme « *installations* » dans le glossaire de la NERC comprenne déjà la caractéristique *BES*, l'utilisation additionnelle du terme « *BES* » vise ici à renforcer la portée d'applicabilité pour ces *installations*, en particulier dans cette section sur l'applicabilité. Cela établit quels sont les *installations*, systèmes et équipements visés par les normes. Cette section est particulièrement importante dans la norme CIP-002-5.1a et délimite l'ensemble des *installations*, systèmes et équipements auxquels s'appliquent les critères de l'annexe 1. C'est important, car cela détermine les *installations*, systèmes et équipements qui sont classés dans la catégorie Impact faible, après filtrage de ceux qui répondent aux critères des catégories Impact élevé et Impact moyen.

Dans le but de répertorier les groupes d'*installations*, de systèmes et d'équipements (par leur emplacement ou autrement), l'entité responsable examine les actifs de la façon décrite à l'exigence E1 de la norme CIP-002-5.1a. Il s'agit d'une démarche familière pour les entités responsables qui ont à se conformer aux versions 1, 2, 3 et 4 des normes CIP pour les *actifs critiques*. Comme dans les versions 1, 2, 3 et 4, les entités responsables peuvent utiliser des postes, des centrales et des *centres de contrôle* dans un même emplacement pour désigner ces groupes d'*installations*, de systèmes et d'équipements.

CIP-002-5.1a

La norme CIP-002-5.1a stipule que les entités responsables visées doivent catégoriser leurs *systèmes électroniques BES* et les *actifs électroniques BES* connexes selon les critères de l'annexe 1. Un *actif électronique BES* inclut dans sa définition : « s'il était endommagé, mal utilisé ou rendu indisponible entraînerait, dans les 15 minutes […] un impact négatif sur […] l'exploitation fiable du *BES* ».

Ce qui suit donne des indications qu'une entité responsable peut utiliser pour désigner les *systèmes électroniques BES* qui seraient visés. Le concept de service de fiabilité du *BES* est utile à cet égard, car il offre à l'entité responsable une méthode définie pour déterminer les *systèmes électroniques BES* auxquels s'applique la norme CIP-002-5.1a. Ce concept établit une liste de services de fiabilité du *BES*. Ces services comprennent :

Réponse dynamique aux conditions du *BES*
Équilibre production-charge
Régulation de la fréquence (puissance active)
Régulation de la tension (puissance réactive)
Gestion des contraintes
Surveillance et contrôle
Remise en charge du *BES*
Connaissance de la situation
Coordination et communication en temps réel entre les entités

La responsabilité de l'exploitation fiable du *BES* est répartie entre toutes les catégories d'entités. Chaque catégorie d'entités apporte une contribution particulière à l'exploitation fiable et l'exposé qui suit aide à déterminer quelle catégorie d'entités, dans le contexte des entités fonctionnelles auxquelles ces normes CIP s'appliquent, effectue quel service de fiabilité, dans le cadre d'un processus de détermination des *systèmes électroniques BES* qui seraient visés. Ce qui suit donne des indications pour aider les entités responsables à déterminer les services de fiabilité applicables selon leur catégorie d'entité (fonction).

Catégorie d'entité	RC	BA	TOP	TO	DP	GOP	GO
Réponse dynamique		X	X	X	X	X	X
Équilibre production-charge	X	X	X	X	X	X	X
Régulation de la fréquence		X				X	X
Régulation de la tension			X	X	X		X
Gestion des contraintes	X		X			X	
Surveillance et contrôle			X			X	
Remise en charge			X			X	
Connaissance de la situation	X	X	X			X	
Coordination entre les entités	X	X	X	X		X	X

Réponse dynamique

Le service de réponse dynamique comprend les actions effectuées par des *éléments* ou des sous-systèmes du *BES* qui sont lancés automatiquement pour amorcer une réponse à une condition du *BES*. Ces actions sont lancées par un seul élément ou dispositif de commande ou par une combinaison de tels éléments ou dispositifs agissant de concert pour effectuer une

action ou pour engendrer une condition en réponse à l'action ou à la condition initiale. Les types de réponses dynamiques qui peuvent être considérés comme ayant un impact potentiel sur le *BES* sont les suivants :

- Réserves tournantes (réserves pour contingence)
  - Fourniture d'une réserve de production au besoin (GO et GOP)
  - Surveillance de l'adéquation des réserves (BA)
- Réponse du régulateur de vitesse
  - Système de commande agissant sur le régulateur de vitesse (GO)
- *Systèmes de protection* (transport et production)
  - Lignes, jeux de barres, transformateurs et groupes turbine-alternateur (DP, TO, TOP, GO et GOP)
  - Protection de zone sur défaillance de disjoncteur (DP, TO et TOP)
  - Protection de disjoncteur (DP, TO et TOP)
  - Courant, fréquence, vitesse et phase (TO, TOP, GO et GOP)
- *Automatismes de réseau* ou *plans de défense*
  - Capteurs, relais et disjoncteurs, possiblement logiciels (DP, TO et TOP)
- Protection par relais de surfréquence et de sous-fréquence (comprend le délestage de charge automatique)
  - Capteurs, relais et disjoncteurs (DP)
- Protection par relais de surtension et de sous-tension (comprend le délestage de charge automatique)
  - Capteurs, relais et disjoncteurs (DP)
- Stabilisateurs de puissance (GO)

Équilibre production-charge

Le service d'équilibre production-charge comprend les activités, actions et conditions nécessaires pour surveiller et régler la production et la charge dans l'horizon de planification de l'exploitation et en temps réel. Les aspects de la fonction d'équilibre production-charge comprennent ce qui suit, mais n'y sont pas limités :

- Calcul de l'*écart de réglage de la zone* (*ACE*)
  - Sources de données sur le terrain (transits d'interconnexion en temps réel, sources de fréquence, écart de temps, etc.) (TO et TOP)
  - Logiciels utilisés pour effectuer les calculs (BA)

- Gestion de la demande
  - Capacité de détecter les besoins de modulation de la charge (BA)
  - Capacité de moduler la charge (TOP et DP)
- Délestages de *charge* commandés manuellement
  - Capacité de détecter les besoins de modulation de la charge (BA)
  - Capacité de moduler la charge (TOP et DP)
- Réserve arrêtée (réserve pour contingence)
  - Connaissance de l'état de marche, de la capacité, du taux de rampe et du temps de démarrage des groupes (GO et BA)
  - Démarrage des groupes de production et fourniture de l'énergie (GOP)

Régulation de la fréquence (puissance active)

Le service de régulation de la fréquence comprend les activités, actions et conditions qui assurent, en temps réel, que la fréquence demeure à l'intérieur de limites acceptables pour la fiabilité et l'exploitabilité du *BES*. Les aspects de la fonction de régulation de la fréquence comprennent ce qui suit, mais y sont limités :

- Contrôle de la production (par exemple, *AGC*)
  - *ACE*, production actuelle des groupes, taux de rampe, caractéristiques des groupes (BA, GOP et GO)
  - Logiciels pour le calcul des réglages à apporter aux groupes (BA)
  - Transmission des réglages aux différents groupes (GOP)
  - Mise en œuvre d'ajustements par les dispositifs de réglage des groupes (GOP)
- Régulation (réserves réglantes)
  - Source de fréquence, programme (BA)
  - Système de commande de régulateur (GO)

Régulation de la tension (puissance réactive)

Le service de régulation de la tension comprend les activités, actions et conditions qui assurent, en temps réel, que la tension demeure à l'intérieur de limites acceptables pour la fiabilité et l'exploitabilité du *BES*. Les aspects de la fonction de régulation de la tension comprennent ce qui suit, mais n'y sont pas limités :

- Régulation automatique de la tension (AVR)
  - Capteurs, système de commande de stator et rétroaction (GO)
- Ressources capacitives

  - État, commande (manuelle ou automatique) et rétroaction (TOP, TO et DP)
- Ressources inductives (changeurs de prises de transformateur ou bobines d'inductance)
  - État, commande (manuelle ou automatique) et rétroaction (TOP, TO et DP)
- Compensateurs statiques (SVC)
  - État, calculs, commande (manuelle ou automatique) et rétroaction (TOP, TO et DP)

Gestion des contraintes

La gestion des contraintes comprend les activités, actions et conditions qui sont nécessaires pour assurer que les éléments du *BES* fonctionnent à l'intérieur de leurs limites de conception et des contraintes établies pour la fiabilité et l'exploitabilité du *BES*. Les aspects de la gestion des contraintes comprennent, mais n'y sont pas limités :

- *Capacité de transfert disponible* (ATC) (TOP)
- Programmes d'échange (TOP et RC)
- Corrections à la répartition de la production et affectation des groupes (GOP)
- Détermination et surveillance des *SOL* et des *IROL* (TOP et RC)
- Détermination et surveillance des *interfaces de transit* (TOP et RC)

Surveillance et contrôle

La surveillance et le contrôle comprennent les activités, actions et conditions qui assurent la surveillance et le contrôle des *éléments* du *BES*. Voici un exemple d'aspect de la surveillance et du contrôle :

- Toutes les méthodes de manœuvre des disjoncteurs et des sectionneurs
  - SCADA (TOP et GOP)
  - Automatisation des postes (TOP)

Remise en charge du *BES*

Le service de remise en charge du *BES* comprend les activités, actions et conditions nécessaires pour passer d'un état d'arrêt à une situation d'exploitation permettant le transport d'énergie sans aide externe. Les aspects de la fonction de remise en charge du *BES* comprennent ce qui suit, mais n'y sont pas limités :

- Remise en charge, y compris le chemin de démarrage planifié
  - Au moyen de groupes à démarrage autonome (TOP et GOP)
  - Au moyen de lignes d'interconnexion (TOP et GOP)
- Alimentation électrique externe de centrale nucléaire (TOP, TO, BA, RC, DP, GO et GOP)

- Coordination (TOP, TO, BA, RC, DP, GO et GOP)

Connaissance de la situation

La fonction de connaissance de la situation comprend les activités, actions et conditions établies par des politiques, des directives ou des procédures d'exploitation normalisées nécessaires pour évaluer la situation courante du *BES* et pour prévoir les effets de changements planifiés ou non planifiés sur les conditions d'exploitation. Les aspects de la fonction de connaissance de la situation comprennent :

- Surveillance et alarmes (par exemple des alarmes EMS) (TOP, GOP, RC et BA)
- Gestion des changements (TOP, GOP, RC et BA)
- Planification du jour même et du jour suivant (TOP)
- Analyse des contingences (RC)
- Surveillance de la fréquence (BA et RC)

Coordination entre les entités

La fonction de coordination et de communication entre les entités comprend les activités, actions et conditions établies par des politiques, des directives ou des procédures d'exploitation normalisées nécessaires pour la coordination et la communication entre les entités responsables afin d'assurer la fiabilité et l'exploitabilité du *BES*. Les aspects de la fonction de coordination et de communication entre les entités comprennent :

- Échanges programmés (BA, TOP, GOP et RC)
- Données d'exploitation et état des installations (TO, TOP, GO, GOP, RC et BA)
- Directives d'exploitation (TOP, RC et BA)

Applicabilité aux distributeurs

Il est attendu que seuls les *distributeurs* qui détiennent ou exploitent des installations qui se qualifient à la section Applicabilité seront visés par la version 5 des normes de cybersécurité. Les *distributeurs* qui ne détiennent ni n'exploitent des installations qui se qualifient ne sont pas visés par ces normes. Les critères d'applicabilité sont fondés sur les exigences d'inscription au titre de *distributeur* et sur les exigences de la norme EOP-005 de la NERC visant les *distributeurs*.

Exigence E1

L'exigence E1 met en œuvre une méthode de catégorisation des *systèmes électroniques BES* selon leur impact sur le *BES*. Dans l'équation traditionnelle d'évaluation du risque, cette méthode réduit la mesure du risque à l'évaluation de l'impact (la conséquence), en supposant un indice de vulnérabilité de 1 (les systèmes sont présumés vulnérables) et une probabilité de

menace de 1 (probabilité de 100 %). Les critères de l'annexe 1 permettent de mesurer le degré d'impact des actifs *BES* desservis par les *systèmes électroniques BES*.

Les entités responsables sont tenues de répertorier et de catégoriser les *systèmes électroniques BES* dont l'impact est élevé ou moyen. Les *systèmes électroniques BES* pour les actifs *BES* qui ne répondent pas aux critères 1.1 à 1.4 et 2.1 à 2.11 de l'annexe 1 sont classés par défaut dans la catégorie Impact faible.

Annexe 1

Application générale

Dans l'application des critères de l'annexe 1, les entités responsables doivent prendre note que l'approche utilisée est basée sur l'impact du *système électronique BES* tel que mesuré par les critères précis définis à l'annexe 1.

- Lorsque l'équipe de rédaction utilise le terme « *installations* », les entités responsables disposent d'une certaine latitude pour déterminer les *installations* concernées. Le terme « *installation* » est défini dans le glossaire de la NERC comme un « ensemble d'équipements électriques qui fonctionnent comme un seul *élément* du *système de production-transport d'électricité* (exemples : ligne, groupe de production, compensateur shunt, transformateur, etc.). » Dans la plupart des cas, les critères se rapportent à un groupe d'*installations* dans un emplacement donné qui contribue à l'exploitation fiable du *BES*. Par exemple, pour les actifs de *transport*, le poste peut être désigné comme le groupe d'*installations*. Cependant, dans un poste qui comprend à la fois de l'équipement utilisé pour l'exploitation du *BES* et de l'équipement utilisé seulement pour les activités de distribution, il peut être préférable pour l'entité responsable de considérer seulement le groupe d'*installations* utilisé pour l'exploitation du *BES*. Dans ce cas, l'entité responsable peut désigner le groupe d'*installations* par son emplacement, avec des indications pour cibler le groupe d'*installations* qui contribue à l'exploitation fiable du *BES*, comme étant les *installations* qui sont visées par les critères de catégorisation des *systèmes électroniques BES*. Les *installations* de production sont traitées séparément à la section Production ci-après. Dans la norme CIP-002-5.1a, ces groupes d'*installations*, de systèmes et d'équipements sont parfois appelés « actifs *BES* ». Par exemple, un actif *BES* répertorié peut être un poste, une centrale de production ou un *centre de contrôle* nommé. Les entités responsables disposent d'une souplesse dans la manière de grouper les *installations*, systèmes et équipements à un emplacement donné.
- Dans certains cas, un *système électronique BES* peut être catégorisé parce qu'il répond à plusieurs critères. Dans de tels cas, l'entité responsable peut choisir de documenter tous les critères qui mènent à la catégorisation. Cela évitera une catégorisation incorrecte lorsqu'il cesse de répondre à l'un des critères, mais qu'il répond encore à un autre.
- Il est recommandé que chaque *système électronique BES* soit répertorié par une seule entité responsable. En cas de propriété commune, il est conseillé aux entités responsables

propriétaires de s'entendre formellement sur la désignation d'une entité responsable à titre de responsable de la conformité aux normes.

Impact élevé (H)

Cette catégorie comprend les *systèmes électroniques BES*, utilisés par et dans des *centres de contrôle* (et les centres informatiques connexes inclus dans la définition de *centres de contrôle*), qui s'acquittent des obligations fonctionnelles du *coordonnateur de la fiabilité* (RC), du *responsable de l'équilibrage* (BA), de l'*exploitant de réseau de transport* (TOP) ou de l'*exploitant d'installation de production* (GOP) telles que définies dans le modèle fonctionnel de la NERC à la rubrique « Tasks » de la fonction pertinente et à la rubrique « Relationship with Other Entities » de l'entité fonctionnelle, et qui répondent aux critères 1.1, 1.2, 1.3 ou 1.4 de l'annexe 1. Bien que les entités inscrites au titre des entités fonctionnelles susmentionnées soient explicitement visées, il peut y avoir des cas d'ententes par lesquelles certaines des obligations fonctionnelles d'un *exploitant de réseau de transport* (TOP) sont déléguées à un *propriétaire d'installation de transport* (TO). Dans de tels cas, les *systèmes électroniques BES* des *centres de contrôle* du TO qui s'acquittent de ces obligations fonctionnelles pourraient être classés dans la catégorie Impact élevé. Les critères sont axés spécifiquement sur les obligations fonctionnelles, et non nécessairement sur les installations du RC, du BA, du TOP ou du GOP. Il est à noter que la définition de *centre de contrôle* renvoie spécifiquement aux tâches de fiabilité du RC, du BA, du TOP et du GOP. Un *système électronique BES* de TO dans une installation de TO qui ne remplit pas ces tâches, et qui n'a pas d'entente avec un TOP pour les remplir, ne répond pas à la définition de *centre de contrôle*. Cependant, si ce *système électronique BES* commande une ou des installations qui répondent aux critères de la catégorie Impact moyen, ce *système électronique BES* serait catégorisé comme un *système électronique BES* à impact moyen.

Le seuil de 3 000 MW défini au critère 1.2 pour les *centres de contrôle* de BA assure une différentiation suffisante du seuil défini pour les *centres de contrôle* à impact moyen de BA. Une analyse des empreintes des BA montre que la plupart des BA dont l'impact est important sont couverts par ce critère.

Des seuils supplémentaires, définis dans les critères, s'appliquent à cette catégorie.

Impact moyen (M)

Production

Les critères de la catégorie Impact moyen de l'annexe 1 qui s'appliquent généralement aux *propriétaires* et aux *exploitants d'installation de production* (GO et GOP) sont les critères 2.1, 2.3, 2.6, 2.9 et 2.11. Le critère 2.13, qui s'applique aux *centres de contrôle* de BA, est également inclus ici.

- Le critère 2.1 désigne comme étant à Impact moyen les *systèmes électroniques BES* qui influent sur des ressources de production dont la capacité en *puissance active nette* est supérieure à 1 500 MW. Le critère de 1 500 MW est partiellement tiré des exigences de

réserve pour contingence de la norme BAL-002 de la NERC, dont l'objet est de « faire en sorte que le *responsable de l'équilibrage* soit en mesure d'utiliser sa *réserve pour contingence* afin d'équilibrer les ressources et la demande, et de rétablir la fréquence de l'*Interconnexion* à l'intérieur des limites définies suivant une *perturbation à déclarer* ». En particulier, elle exige qu'« Au minimum, le *responsable de l'équilibrage* ou le *groupe de partage des réserves* doit disposer d'une *réserve pour contingence* suffisante afin de se prémunir contre la contingence simple la plus grave. » L'équipe de rédaction a utilisé 1 500 MW comme chiffre provenant des *réserves pour contingence* les plus importantes exploitées par divers BA dans toutes les régions.

Par l'utilisation de la capacité en *puissance active* nette, l'équipe de rédaction a cherché à utiliser une valeur qui pourrait être vérifiée d'après les exigences existantes proposées dans la norme MOD-024 de la NERC et compte tenu des efforts de développement actuels dans ce secteur.

En utilisant le critère précis de 1 500 MW, l'intention de l'équipe de rédaction est de s'assurer que les *systèmes électroniques BES* ayant des vulnérabilités de mode commun qui pourraient entraîner la perte de 1 500 MW ou plus de production à une même centrale pour un groupe de production ou un ensemble de groupe de production soient protégés adéquatement.

L'équipe de rédaction a aussi utilisé d'autres paramètres de temps et de valeur pour s'assurer que les critères précis et leurs valeurs de comparaison soient relativement stables au cours de la période d'examen. Lorsque plusieurs valeurs de capacité en *puissance active* nette pouvaient être utilisées pour classer une installation selon ces critères précis, la valeur la plus élevée a été utilisée.

- Pour le critère 2.3, l'équipe de rédaction a cherché à s'assurer que les *systèmes électroniques BES* pour les *installations* de production désignées par le *coordonnateur de la planification* ou le *planificateur de réseau de transport* comme étant nécessaires pour éviter des *impacts négatifs sur la fiabilité* du *BES* dans un horizon de planification d'un an ou plus soient catégorisés comme étant à Impact moyen. En spécifiant un horizon de planification d'un an ou plus, l'intention est de s'assurer qu'il s'agit de groupes qui sont répertoriés dans le cadre d'une planification de fiabilité « à long terme », s'étendant sur une période d'exploitation d'au moins 12 mois. Cela ne signifie pas nécessairement que le jour où le groupe sera exploité est dans plus d'un an, mais plutôt que la période de planification est de plus de un an ; on cherche spécifiquement à éviter que le critère s'applique à une production destinée à remédier à des problèmes urgents de fiabilité à court terme. De telles *installations* peuvent être désignées comme « indispensables à la fiabilité » (*Reliability Must Run*), et il ne faut pas les confondre avec les installations de production désignées comme indispensables (*must run*) pour la stabilisation du marché. Comme l'emploi de l'expression « *must run* » entraîne une certaine confusion à bien des égards, l'équipe de rédaction a choisi de l'éviter et a formulé l'exigence dans un langage de fiabilité plus générique. En particulier, l'accent mis sur la prévention des *impacts négatifs sur la fiabilité* impose que ces groupes soient désignés comme indispensables aux fins de la fiabilité au-delà de l'échelle

locale. Les groupes désignés comme indispensables au maintien de la tension à l'échelle locale ne seraient généralement pas désignés comme tels. En l'absence de *coordonnateur de la planification* désigné, le *planificateur de réseau de transport* est l'entité inscrite qui effectue cette désignation.

Si des études de réseau permettent de conclure que le fonctionnement d'un groupe est indispensable à la fiabilité du *BES*, par exemple en cas de contingence de catégorie C3 telle que définie dans la norme TPL-003, les *systèmes électroniques BES* pour ce groupe sont alors catégorisés comme étant à Impact moyen.

Les normes TPL exigent que, si les études et plans indiquent le besoin d'actions supplémentaires, ces études et plans soient communiqués par le *coordonnateur de la planification* ou le *planificateur de réseau de transport* par écrit à l'*entité régionale* ou au RRO. Les actions nécessaires pour la mise en œuvre de ces plans par les parties concernées (propriétaires ou exploitants d'installation de production, *coordonnateurs de la fiabilité* ou autre partie nécessaire) sont habituellement officialisées sous la forme d'une entente ou d'un contrat.

- Le critère 2.6 vise les *systèmes électroniques BES* des *installations* de production désignées comme essentielles pour le calcul des *IROL* et de leurs contingences associées, comme il est spécifié aux exigences E5.1.1 et E5.1.3 de la norme FAC-014-2, *Établir et communiquer les limites d'exploitation du réseau*.

  Les *IROL* peuvent être basées sur des phénomènes de *réseau* dynamiques comme l'instabilité ou l'effondrement de la tension. Le calcul de ces *IROL* et de leurs contingences associées tient souvent compte de l'effet de l'inertie de la production et de la réponse des AVR.

- Le critère 2.9 catégorise les *systèmes électroniques BES* associés aux *automatismes de réseau* et aux *plans de défense* comme étant à Impact moyen. Les *automatismes de réseau* et les *plans de défense* peuvent être mis en œuvre pour prévenir les perturbations qui entraîneraient un dépassement des *IROL* s'ils n'assuraient pas la fonction requise au moment voulu ou s'ils avaient un fonctionnement non conforme à leurs critères de conception. Les *propriétaires d'installation de production* et les *exploitants d'installation de production* qui possèdent des *systèmes électroniques BES* pour de tels automatismes de réseau et plans de défense les classent dans la catégorie Impact moyen.

- Le critère 2.11 classe dans la catégorie Impact moyen les *systèmes électroniques BES* utilisés par et dans des *centres de contrôle* qui s'acquittent des obligations fonctionnelles de l'*exploitant d'installation de production* pour une production totale de 1 500 MW ou plus dans une seule Interconnexion, et qui n'ont pas déjà été inclus dans la partie 1.

- Le critère 2.13 classe dans la catégorie Impact moyen les *centres de contrôle* de BA qui « contrôlent » une production de 1 500 MW ou plus dans une même Interconnexion et qui n'ont pas déjà été inclus dans la partie 1. Le seuil de 1 500 MW est cohérent avec le degré d'impact et le raisonnement indiqué pour le critère 2.1.

Transport

Dans le texte original en anglais, la SDT utilise les expressions « Transmission Facilities at a single station or substation » et « Transmission stations or substations » pour reconnaître l'existence des termes « stations » et « substations ». Plusieurs entités de l'industrie appellent « substation » un emplacement avec des frontières physiques (clôture, mur, etc.) qui renferme au moins un autotransformateur. Des emplacements ne renfermant pas d'autotransformateurs existent également, et plusieurs entités de l'industrie appellent ceux-ci des « stations » ou « switchyards ». Par conséquent, la SDT a choisi d'utiliser les deux termes « station » et « substation » pour référer aux emplacements où des ensembles d'installations de transport existent ; en français, ces deux notions sont rendues dans le texte par le mot « poste ».

- Les critères 2.2, 2.4 à 2.10 et 2.12 de l'annexe 1 s'appliquent aux *propriétaires d'installation de transport* et aux *exploitants de réseau de transport*. Dans plusieurs de ces critères, le seuil d'impact est défini comme la capacité d'une défaillance ou d'une compromission d'un système à entraîner le dépassement d'une ou de plusieurs *limites d'exploitation pour la fiabilité de l'Interconnexion* (*IROL*). Le critère 2.2 couvre les *systèmes électroniques BES* pour les *installations* de *réseaux* de *transport* qui fournissent des ressources de puissance réactive permettant d'améliorer et de préserver la fiabilité du *BES*. La valeur nominale est utilisée ici, car il n'y a pas d'exigence de la NERC pour vérifier la capacité réelle de ces *installations*. La valeur de 1 000 Mvar utilisée dans ce critère est une valeur jugée raisonnable pour déterminer la criticité de l'impact.

- Le critère 2.4 couvre les *systèmes électroniques BES* pour toute *installation* de *transport* située dans un poste exploité à 500 kV ou plus. Bien que l'équipe de rédaction considère que les *installations* exploitées à 500 kV ou plus ne nécessitent pas de précisions supplémentaires quant à leur rôle dans le système de réseaux interconnectés formant le *BES*, les *installations* dans le bas de la fourchette THT devraient avoir des critères supplémentaires pour inclusion dans la catégorie Impact moyen.

  Il est à noter que si le jeu de barres collectrices d'une centrale de production (la centrale est plus petite que le seuil établi pour la production au critère 2.1) est exploité à 500 kV, ce jeu de barres devrait être considéré comme une *installation* de raccordement de la production et non comme une *installation* de *transport*, selon le document *Final Report from the Ad Hoc Group for Generation Requirements at the Transmission Interface*. Ce jeu de barres collectrices ne serait pas une installation pour un *système électronique BES* à impact moyen, car il ne touche pas significativement le réseau de *transport* à 500 kV ; il ne touche qu'une centrale qui se trouve sous le seuil de production.

- Le critère 2.5 couvre les *systèmes électroniques BES* pour les installations dans le bas de la fourchette de transport du *BES* avec des restrictions pour l'inclusion, si elles sont jugées très susceptibles d'avoir un impact significatif sur le *BES*. Bien que ce critère ait été défini dans le cadre du raisonnement exigeant la protection contre tout impact significatif sur le *BES*, l'équipe de rédaction a inclus dans ce critère des restrictions supplémentaires qui assureraient un degré suffisant d'impact sur le *BES*. Ainsi, l'équipe de rédaction :

    - exclut les installations radiales qui fourniraient du soutien pour une seule installation de production ;

    - spécifie le raccordement à au moins trois postes de transport pour s'assurer que le degré d'impact soit approprié.

  La valeur pondérée totale de 3 000 a été obtenue à partir des valeurs pondérées liées à trois lignes à 345 kV et à cinq lignes à 230 kV à un poste de transport. La valeur pondérée totale sert à représenter l'impact réel sur le *BES*, indépendamment de la tension nominale de chaque ligne et de la combinaison de lignes de différentes tensions nominales.

  De plus, dans le document *Integrated Risk Assessment Approach – Refinement to Severity Risk Index – Attachment 1* de la NERC, le rapport a utilisé une charge de ligne moyenne en MVA basée sur la tension nominale :

    - 230 kV –> 700 MVA
    - 345 kV –> 1 300 MVA
    - 500 kV –> 2 000 MVA
    - 765 kV –> 3 000 MVA

  Pour ce qui est de déterminer les lignes visées et les raccordements à d'« autres postes de *transport* », les éléments suivants devraient être considérés :

    - Dans le cas des autotransformateurs d'un poste, les entités responsables disposent d'une latitude pour déterminer si les groupes d'*installations* sont considérés comme un seul emplacement de poste ou plusieurs postes. Dans la plupart des cas, les entités responsables les considéreraient probablement comme des *installations* à un seul poste, à moins qu'elles soient dispersées géographiquement. Dans le cas de transformateurs situés à l'intérieur de la « clôture » d'un poste, les autotransformateurs peuvent ne pas compter comme des raccordements distincts à d'autres postes. L'utilisation de *systèmes électroniques BES* communs serait de nature à invalider toute autre considération. Dans le cas d'autotransformateurs dispersés géographiquement par rapport à un emplacement de poste, le calcul tiendrait compte de tous les raccordements d'arrivée et de départ à chaque poste.

    - Les lignes à dérivations multiples sont censées représenter une seule valeur pondérée par ligne et influent sur le nombre de raccordements à d'autres postes.

Ainsi, une seule ligne à 230 kV à dérivations multiples entre trois postes de *transport* représenterait une valeur pondérée totale de 700 et raccorderait des *installations* de *transport* d'un seul poste à deux autres postes de *transport*.

- Les lignes multiples entre deux postes de *transport* sont censées représenter plusieurs valeurs pondérées par ligne, mais ces lignes multiples entre les deux postes raccordent seulement un poste à un autre poste. Ainsi, deux lignes à 345 kV entre deux postes de *transport* représenteraient une valeur pondérée totale de 2 600, et raccorderaient les *installations* de *transport* d'un seul poste à un autre poste de *transport*.

La restriction du critère 2.5 pour les *installations* de *transport* dans un poste de *transport* est basée sur deux conditions distinctes :

1. La première condition est que les *installations de transport* à un seul poste dans le cas où le poste est raccordé, à des niveaux de tension de 200 kV ou plus, à trois (3) autres postes, à trois autres postes. Cette condition vise à assurer que les raccordements exploités à des tensions de 500 kV ou plus soient également compris dans le compte des raccordements à d'autres postes.
2. La deuxième condition est que la valeur totale de toutes les lignes d'arrivée ou de départ du poste doit dépasser 3 000. Cette condition ne tient pas compte des lignes exploitées à moins de 200 kV ou à 500 kV et plus, ce dernier cas étant déjà classé « à impact moyen » selon le critère 2.4 : il n'y a pas de valeur à assigner aux lignes dont la tension est de moins de 200 kV ou de 500 kV et plus dans le tableau des valeurs pour la contribution à la valeur combinée de 3 000.

Les *installations* de *transport* dans le poste doivent répondre à ces deux conditions pour être considérées comme répondant au critère 2.5.

- Le critère 2.6 couvre les *systèmes électroniques BES* pour les *installations* de *transport* qui ont été désignées comme essentielles pour le calcul des *IROL* et de leurs contingences associées, comme il est spécifié aux exigences E5.1.1 et E5.1.3 de la norme FAC-014-2, *Établir et communiquer les limites d'exploitation du réseau*.

- Le critère 2.7 est tiré de l'exigence E9.2.2 de la norme NUC-001 de la NERC, pour le soutien des *installations* nucléaires. La norme NUC-001 assure que la fiabilité des *exigences relatives à l'interface de centrale nucléaire* (*NPIR*) est assurée par une coordination adéquate entre le *propriétaire* ou l'*exploitant d'installation de production* nucléaire et son fournisseur de *transport* « afin que l'exploitation et les arrêts de centrale se déroulent en toute sécurité ». En particulier, il y a des exigences spécifiques pour coordonner la sécurité physique et la cybersécurité de ces interfaces.

- Le critère 2.8 désigne comme « à impact moyen » les *systèmes électroniques BES* qui ont un impact sur les *installations* de *transport* nécessaires pour des installations de production qui respectent les conditions du critère 2.1 (*installations* de production avec une puissance de plus de 1 500 MW) et 2.3 (*installations* de production généralement désignées comme

indispensables à la fiabilité de la zone étendue dans l'horizon de planification). L'entité responsable peut demander une déclaration formelle du propriétaire d'installation de production quant à la qualification des *installations* de production raccordées à ses réseaux de *transport*.

- Le critère 2.9 désigne comme « à impact moyen » les *systèmes électroniques BES* pour les *automatismes de réseau* (*SPS*), les *plans de défense* (*RAS*) ou les systèmes de manœuvre automatisés installés afin d'assurer l'exploitation du *BES* à l'intérieur des *IROL*. La dégradation, la compromission ou l'indisponibilité de ces *systèmes électroniques BES* entraînerait le dépassement des *IROL* s'ils ne fonctionnaient pas tels que conçus. Selon la définition du terme *IROL*, la perte ou la compromission de l'un ou l'autre de ceux-ci a des impacts sur la *zone étendue*.

- Le critère 2.10 désigne comme « à impact moyen » les *systèmes électroniques BES* pour les systèmes ou *éléments* qui effectuent, sans intervention humaine, un délestage de charge automatique de 300 MW ou plus. La SDT a passé un temps considérable à discuter de la formulation du critère 2.10, et choisi le mot « chaque » pour indiquer que le critère s'applique à un système ou une *installation* distincte. Dans la rédaction de ce critère, l'équipe de rédaction a cherché à inclure seulement les systèmes qui ne nécessitent pas d'intervention humaine, et a ciblé en particulier les *installations* et les systèmes de délestage de charge en sous-fréquence (DSF) et les systèmes et les *éléments* de délestage de charge en sous-tension (DST) qui seraient visés par une exigence de délestage de charge régionale visant à prévenir un *impact négatif sur la fiabilité*. Ceux-ci comprennent les systèmes automatisés DSF et DST capables de délester 300 MW de charge ou plus. Il est à noter que les systèmes qui ont besoin d'une intervention humaine pour leur armement, mais qui une fois armés se déclenchent automatiquement, doivent être considérés comme ne nécessitant pas d'intervention humaine et devraient être désignés comme « à impact moyen ». Le seuil de 300 MW a été défini comme la valeur de charge totale en MW la plus élevée, définie selon les normes de délestage de charge régionales pertinentes, pour les 12 mois précédents afin de tenir compte des fluctuations saisonnières.

  Ce seuil particulier de 300 MW provient de la version 1 des normes CIP. La SDT est d'avis que ce seuil doit être inférieur à l'exigence de production de 1 500 MW puisqu'il concerne spécifiquement le DST et le DSF, qui constituent des efforts de dernier recours pour sauver le *système de production-transport d'électricité* et requièrent donc un seuil plus bas. Un examen des tolérances DSF définies dans les normes de fiabilité régionales pour les besoins des programmes 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 du DSF.

  Dans l'ERCOT, les *charges* agissant comme des ressources (*Loads Acting as Resources* [LaaR]) du programme de gestion de la demande ne fait pas partie du programme de délestage régional, mais d'un marché de services complémentaires. En général, les programmes de gestion de la demande semblables qui ne font pas partie des programmes de délestage de charge de fiabilité de la NERC ou régionaux, mais qui sont offerts comme

composantes d'un marché de services complémentaires, ne se qualifient pas selon ce critère.

Le libellé de la section 4 pour les DSF et DST et du critère 2.10 de l'annexe 1 est formulé de manière à être cohérent avec les exigences énoncées dans les normes PRC pour les DSF et les DST.

- Le critère 2.12 catégorise comme « à impact moyen » les *systèmes électroniques BES* utilisés par et dans les *centres de contrôle* et les centres informatiques connexes qui s'acquittent des obligations fonctionnelles d'un *exploitant de réseau de transport* et qui n'ont pas déjà été catégorisés comme « à impact élevé ».

- Le critère 2.13 catégorise comme « à impact moyen » les *centres de contrôle* de BA qui « contrôlent » une production de 1 500 MW ou plus dans une même *Interconnexion*. Le seuil de 1 500 MW est cohérent avec le degré d'impact et le raisonnement indiqué pour le critère 2.1.

Impact faible (L)

Les *systèmes électroniques BES* qui ne tombent pas dans les catégories Impact élevé ou Impact moyen tombent par défaut dans la catégorie Impact faible. Il est à noter que les *systèmes électroniques BES* à impact faible n'ont pas à être répertoriés individuellement.

Installations de remise en charge

- Plusieurs commentaires sur la version 5 des normes CIP suggèrent que les entités qui possèdent des *ressources à démarrage autonome* et des *chemins de démarrage* pourraient choisir de retirer ces services afin d'éviter des coûts de conformité plus élevés. Par exemple, un *coordonnateur de la fiabilité* a signalé une diminution de 25 % du nombre des *ressources à démarrage autonome* depuis l'entrée en vigueur de la version 1 des normes, et un nombre accru d'entités pourraient décider de faire un tel choix avec la version 5.

  Devant ce constat, l'équipe de rédaction de la version 5 des normes CIP a consulté informellement les comités de planification et d'exploitation de la NERC. Ces comités indiquent avoir déjà constaté une diminution du nombre des *ressources à démarrage autonome* en raison d'une augmentation des coûts de conformité aux normes CIP, des règles environnementales et d'autres risques ; le fait de les maintenir, dans la version 5, dans une catégorie qui augmenterait substantiellement les coûts de conformité pourrait entraîner un amoindrissement encore plus grand d'un bassin de ressources vulnérable.

  En réponse à ces considérations, l'équipe de rédaction a recatégorisé les actifs de remise en charge, comme les *ressources à démarrage autonome* et les *chemins de démarrage*, les faisant passer de la catégorie Impact moyen (comme c'était le cas dans les premières versions de travail) à la catégorie Impact faible. Cela ne libère pas les propriétaires de ces actifs de toute responsabilité, comme cela aurait été le cas dans les versions 1 à 4 de la norme CIP-002 (puisque seuls les *actifs électroniques* à connectivité routable qui sont essentiels aux actifs de remise en charge sont inclus dans ces versions). En vertu de la catégorisation Impact faible, ces actifs seront protégés dans les domaines de sensibilisation

à la cybersécurité, de contrôle des accès physiques et de contrôle des accès électroniques, et seront soumis à des obligations quant aux interventions en cas d'incident. Il s'agit néanmoins, en fin de compte, d'un gain net pour la fiabilité du *BES*, puisque beaucoup de ces actifs ne répondent pas aux critères d'inclusion des versions 1 à 4.

En pesant les risques pour la fiabilité générale du *BES*, l'équipe de rédaction a conclu que cette recatégorisation représente l'option la moins préjudiciable à la fonction de remise en charge, et donc à la fiabilité générale du *BES*. Le retrait des *ressources à démarrage autonome* et des *chemins de démarrage* de la catégorie Impact moyen est dans l'intérêt de la fiabilité d'ensemble, car autrement on assisterait vraisemblablement à une diminution du nombre des *ressources à démarrage autonome* disponibles pour une remise en charge rapide en cas de besoin.

Les *systèmes électroniques BES* pour les ressources de production qui ont été désignées comme *ressources à démarrage autonome* dans le plan de remise en charge de l'*exploitant de réseau de transport* tombent par défaut dans la catégorie Impact faible. La norme EOP-005-2 de la NERC stipule que l'*exploitant de réseau de transport* doit avoir un plan de remise en charge, et que ce plan doit préciser la liste de ses *ressources à démarrage autonome* ainsi que les exigences d'essai de ces ressources. Ce critère se limite aux *ressources à démarrage autonome* désignées comme telles dans le plan de remise en charge de l'*exploitant de réseau de transport*. Le terme « plan de capacité de démarrage autonome » a été retiré du Glossaire.

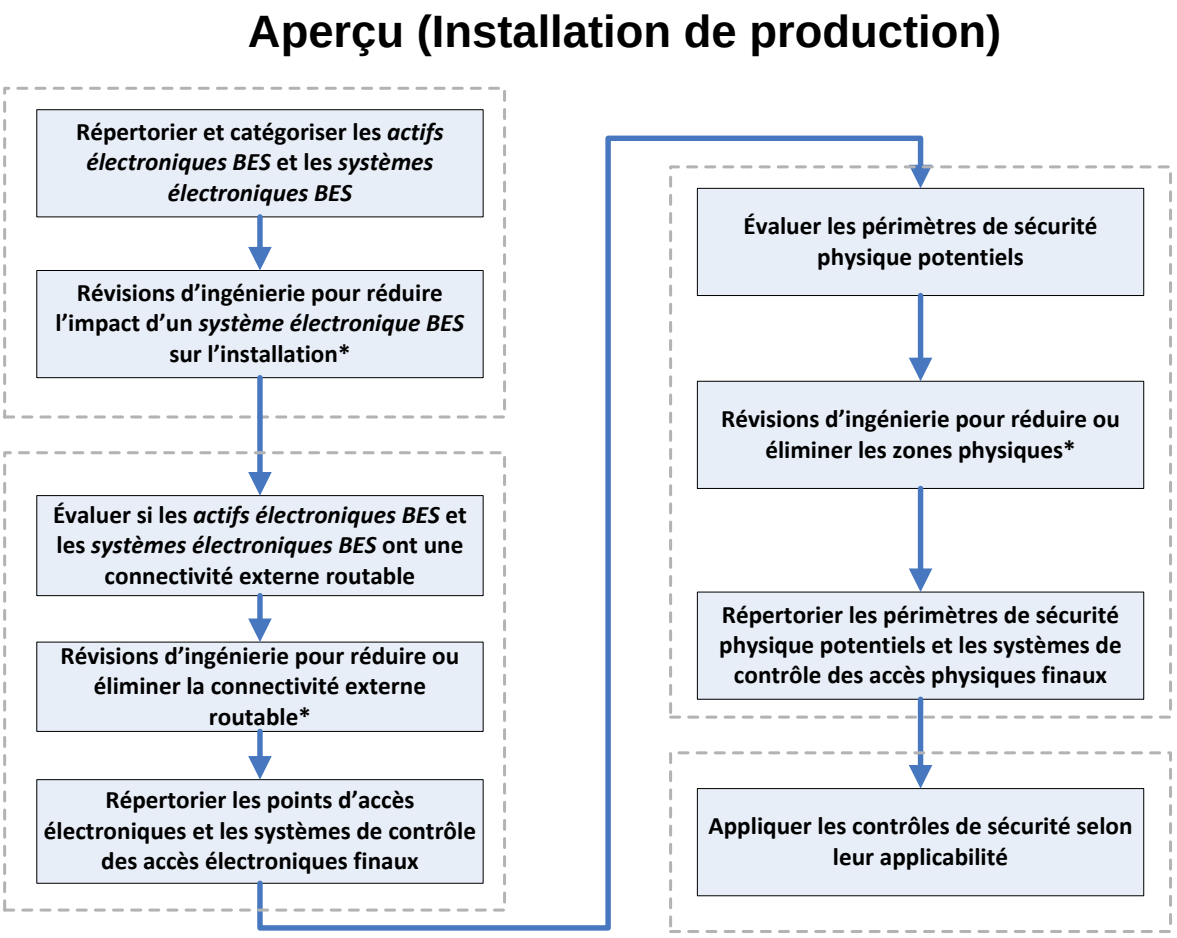
En ce qui concerne la communication aux propriétaires et aux exploitants d'actifs du *BES* de leur rôle dans le plan de remise en charge, l'*exploitant de réseau de transport* est tenu par la norme EOP-005-2 de la NERC de « fournir aux entités identifiées dans son plan de remise en charge approuvé, une description de tout changement apporté à leurs rôles et à leurs tâches spécifiques avant la date d'entrée en vigueur du plan ».

- Les *systèmes électroniques BES* des *installations* et des *éléments* comprenant les *chemins de démarrage* et respectant les exigences relatives aux manœuvres initiales depuis la *ressource à démarrage autonome* jusqu'au premier point de raccordement du ou des groupes de production à démarrer désignés dans le plan de remise en charge de l'*exploitant de réseau de transport*, tombent par défaut dans la catégorie Impact faible ; ces systèmes sont néanmoins désignés explicitement dans la version 5 des normes CIP. Cette exigence d'inclusion dans la portée est tirée des exigences de la norme EOP-005-2 de la NERC, qui stipule que l'*exploitant de réseau de transport* doit indiquer dans son plan de remise en charge les *chemins de démarrage* et les exigences concernant les manœuvres initiales pour la *ressource à démarrage autonome* et les groupes de production à démarrer.

  Les *distributeurs* noteront qu'ils ont peut-être des *systèmes électroniques BES* visés par la présente norme s'ils ont des *éléments* indiqués dans le plan de remise en charge de l'*exploitant de réseau de transport* et qui font partie du *chemin de démarrage*.

Cas d'utilisation : déroulement du processus CIP

Le cas suivant de déroulement du processus CIP pour un exploitant ou un propriétaire d'installation de production a été fourni par un participant à l'élaboration de la version 5 des normes et est présenté ici à titre d'exemple d'un processus utilisé pour répertorier et catégoriser les *systèmes électroniques BES* et les *actifs électroniques BES* ; pour examiner, élaborer et mettre en œuvre des stratégies d'atténuation des risques globaux ; et pour appliquer les mesures de sécurité pertinentes.



*** Les révisions d'ingénierie devront être évaluées quant à la justification de leur coût, aux exigences opérationnelles et de sécurité, aux besoins de soutien et aux limitations techniques.**

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

Les *systèmes électroniques BES* à chaque emplacement ont un impact sur l'exploitation fiable du *système de production-transport d'électricité* qui varie. L'annexe 1 fournit un ensemble de critères précis que l'entité responsable doit utiliser pour répertorier ces *systèmes électroniques BES* selon leur impact sur le *BES*. Les *systèmes électroniques BES* doivent être répertoriés et catégorisés selon leur impact, de sorte que les mesures appropriées puissent être appliquées, proportionnellement à leur impact. Ces catégories d'impact constitueront la base de l'application des exigences pertinentes des normes CIP-003 à CIP-011.

Justification de l'exigence E2

Les listes exigées par l'exigence E1 sont revues sur une base périodique pour s'assurer que tous les *systèmes électroniques BES* pertinents ont été correctement répertoriés et catégorisés. Toute erreur de catégorisation ou non-catégorisation d'un *système électronique BES* peut entraîner l'adoption de mesures de cybersécurité inadéquates ou l'absence de contrôles de cybersécurité, qui peuvent mener à une compromission ou à une mauvaise utilisation susceptible de nuire au fonctionnement en temps réel du *BES*. L'approbation par le *cadre supérieur CIP* assure une bonne supervision du processus par le personnel approprié de l'entité responsable.

Historique des versions

Version	Date	Intervention	Suivi des modifications
1	16 janvier 2006	E3.2 — Remplacement de « Control Center » par « control center » dans la version anglaise.	24 mars 2006
2	30 septembre 2009	Modifications visant à clarifier les exigences et à mettre les éléments de conformité en concordance avec les plus récentes directives sur l'établissement des éléments de conformité des normes. 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 « Responsabilité du contrôle de la conformité ».	
3	16 décembre 2009	Changement du numéro de version de -2 à -3. 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
5	26 novembre 2012	Approbation par le Conseil d'administration de la NERC.	Modification en coordination avec les autres normes CIP et révision du format selon le gabarit RBS.

Version	Date	Intervention	Suivi des modifications
5.1	30 septembre 2013	Remplacement de « Devices » par « Systems » dans une définition de la section Contexte.	Errata
5.1	22 novembre 2013	Ordonnance de la FERC approuvant la version CIP-002-5.1.	
5.1a	2 novembre 2016	Adoption par le Conseil d'administration de la NERC.	
5.1a	14 décembre 2016	Ordonnance de la FERC approuvant la version CIP-002-5.1a (dossier RD17-2-000).	

Addenda 1

Numéro et texte de l'exigence

CIP-002-5.1, exigence E1

E1. Chaque entité responsable doit mettre en œuvre un processus qui examine chacun des actifs suivants aux fins des alinéas 1.1 à 1.3 :

i. *centres de contrôle* et *centres de contrôle* de repli ;

ii. postes de transport ;

iii. ressources de production ;

iv. systèmes et installations essentiels à la remise en charge du réseau, y compris les *ressources à démarrage autonome* et les *chemins de démarrage* ainsi que les exigences relatives aux manœuvres initiales ;

v. *automatismes de réseau* qui contribuent à la fiabilité du *système de production-transport d'électricité* ; et

vi. pour les *distributeurs*, *systèmes de protection* indiqués à l'alinéa 4.2.1 de la section Applicabilité ci-dessus.

1.1 répertorier chacun des *systèmes électroniques BES* à impact élevé, selon la section 1 de l'annexe 1, s'il y en a, dans chaque actif ;

1.2 répertorier chacun des *systèmes électroniques BES* à impact moyen, selon la section 2 de l'annexe 1, s'il y en a, dans chaque actif ; et

1.3 répertorier chaque actif qui comporte un *système électronique BES* à impact faible, selon la section 3 de l'annexe 1, s'il y en a (une liste des *systèmes électroniques BES* à impact faible n'est pas exigée).

Annexe 1, critère 2.1

2. **Impact moyen (M**)

Chaque *système électronique BES,* non inclus dans la section 1 ci-dessus, associé à un des éléments suivants :

2.1 Production en service, pour chaque ensemble de groupes de production à une même centrale, dont la puissance active nominale nette totale la plus élevée des 12 mois civils précédents est de 1 500 MW ou plus dans une même *Interconnexion*. Pour chaque ensemble de groupes de production, les seuls *systèmes électroniques BES* qui répondent à ce critère sont les *systèmes électroniques BES* partagés qui pourraient, dans un délai de 15 minutes, avoir un impact négatif sur l'exploitation fiable de toute combinaison de groupes de production qui, ensemble, représentent 1 500 MW ou plus dans une même *Interconnexion*.

Questions

Energy Sector Security Consortium, Inc. (EnergySec) a présenté une demande d'interprétation (RFI) afin d'obtenir une clarification du critère 2.1 de l'annexe 1 de la norme de fiabilité CIP-002-5.1 relativement à l'expression « *systèmes électroniques BES* partagés ».

L'équipe chargée de rédiger l'interprétation a dégagé de la demande d'interprétation les questions suivantes :

1. L'expression « *systèmes électroniques BES* partagés » implique-t-elle que l'évaluation selon le critère 2.1 doit être faite individuellement pour chaque *système électronique BES* à une même centrale, ou collectivement pour les groupes de *systèmes électroniques BES* ?
2. L'expression « *systèmes électroniques BES* partagés » désigne-t-elle des *systèmes électroniques BES* distincts qui sont partagés entre plusieurs groupes de production, ou des groupes de *systèmes électroniques BES* qui pourraient collectivement avoir un impact sur plusieurs groupes de production ?
3. Si cette expression désigne des groupes de *systèmes électroniques BES* pris collectivement, quel critère doit-on appliquer pour déterminer quels *systèmes électroniques BES* doivent former un groupe aux fins d'une évaluation collective ?

Réponses

Question 1 : L'expression « *systèmes électroniques BES* partagés » implique-t-elle que l'évaluation selon le critère 2.1 doit être faite individuellement pour chaque *système électronique BES* à une même centrale, ou collectivement pour les groupes de *systèmes électroniques BES* ?

L'évaluation visant à déterminer si un *système électronique BES* est partagé doit être faite individuellement pour chaque *système électronique BES*. Il n'existe dans le texte de la norme CIP-002-5.1 aucune mention ni obligation de grouper les *systèmes électroniques BES*. L'alinéa 1.2 de l'exigence E1 stipule : « répertorier chacun des *systèmes électroniques BES* à impact moyen, selon la section 2 de l'annexe 1... ». Par ailleurs, le préambule de la section 2 de l'annexe 1 de la norme CIP-002-5.1 stipule : « chaque *système électronique BES*, non inclus dans la section 1 ci-dessus, associé à un des éléments suivants ». (soulignements ajoutés)

En outre, la section Contexte de la norme CIP-002-5.1 stipule : « Il est laissé à la discrétion de l'entité responsable de déterminer le niveau de granularité pour délimiter un *système électronique BES*, compte tenu des conditions de la définition de *système électronique BES* ». La section Contexte stipule également ce qui suit :

> « L'entité responsable devrait prendre en considération le contexte opérationnel et le cadre de gestion lorsqu'elle définit les limites d'un *système électronique BES*, de manière à maximiser l'efficience de son fonctionnement sécurisé. Définir des limites trop étroites pourrait entraîner des redondances dans les processus administratifs et les autorisations, tandis que définir des limites trop larges pourrait rendre le

fonctionnement sécurisé du *système électronique BES* difficile à surveiller et à évaluer. »

Question 2 : L'expression « *systèmes électroniques BES* partagés » désigne-t-elle des *systèmes électroniques BES* distincts qui sont partagés entre plusieurs groupes de production, ou des groupes de *systèmes électroniques BES* qui pourraient collectivement avoir un impact sur plusieurs groupes de production ?

L'expression « *systèmes électroniques BES* partagés » désigne des *systèmes électroniques BES* distincts qui sont partagés entre plusieurs groupes de production.

L'emploi du mot « partagé » est également clarifié dans le document de questions et réponses (FAQ) publié par la NERC afin d'encadrer la mise en œuvre des normes de fiabilité CIP. La réponse à la question 49 stipule ce qui suit :

> « Les *systèmes électroniques BES* partagés sont ceux qui sont associés à toute combinaison de groupes de production dans une même *Interconnexion*, comme il est indiqué aux critères 2.1 et 2.2 d'évaluation du degré d'impact de l'annexe 1 de la norme CIP-002-5.1. Pour le critère 2.1 : « *systèmes électroniques BES* partagés qui pourraient, dans un délai de 15 minutes, avoir un impact négatif sur l'exploitation fiable de toute combinaison de groupes de production qui, ensemble, représentent 1 500 MW ou plus dans une même *Interconnexion* ». Pour le critère 2.2 : « *systèmes électroniques BES* partagés qui pourraient, dans un délai de 15 minutes, avoir un impact négatif sur l'exploitation fiable de toute combinaison de ressources qui au total représentent 1 000 Mvar ou plus ». Se reporter également au document *Lesson Learned – CIP-002-5.1 Requirement R1: Impact Rating of Generation Resource Shared BES Cyber Systems* (Leçons à retenir – Exigence E1 de la norme CIP-002-5.1 – Évaluation du degré d'impact des *systèmes électroniques BES* partagés entre plusieurs ressources de production), qui donne de plus amples précisions ainsi que des exemples. »

Question 3 : Si cette expression désigne des groupes de *systèmes électroniques BES* pris collectivement, quel critère doit-on appliquer pour déterminer quels *systèmes électroniques BES* doivent former un groupe aux fins d'une évaluation collective ?

Cette expression désigne des *systèmes électroniques BES* pris individuellement.

Annexe QC-CIP-002-5.1a
Dispositions particulières de la norme CIP-002-5.1a applicables au Québec

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

A. Introduction

1. Titre : Cybersécurité — Catégorisation des systèmes électroniques BES

2. Numéro : CIP-002-5.1a

3. Objet : Aucune disposition particulière

4. Applicabilité :

Entités fonctionnelles

Aucune disposition particulière

Installations

La présente norme s'applique seulement aux installations du *réseau de transport principal* (RTP) et aux installations spécifiées pour le *distributeur*. Dans l'application de cette norme, toute référence aux termes « *système de production-transport d'électricité* » ou « BES » doit être remplacée par les termes « *réseau de transport principal* » ou « RTP » respectivement.

Exemptions additionnelles

Sont exemptés de l'application de la présente norme :

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

5. Date d'entrée en vigueur au Québec :

5.1. Adoption de la norme par la Régie de l'énergie : xx mois 20xx

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

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

1er janvier 2019

Les dates de mises en application de la norme sont les mêmes que celles de la version CIP-002-5.1 :

Pour les entités qui possèdent des actifs classés critiques aux fins des normes CIP (version 1) :

- 1er janvier 2019 pour les systèmes électroniques BES dont l'impact est « moyen » ou « élevé » ;

- 1er janvier 2019 pour les systèmes électroniques BES dont l'impact est « faible ».

Pour les entités qui ne possèdent ni des actifs critiques aux fins de normes CIP (version 1), ni des installations de production à vocation industrielle:

- 1er janvier 2019 pour les systèmes électroniques BES dont l'impact est « moyen » ou « élevé » ;
- 1er octobre 2019 pour les systèmes électroniques BES dont l'impact est « faible ».

Pour les entités qui possèdent des installations de production à vocation industrielle :

- 1er avril 2019 pour les systèmes électroniques BES dont l'impact est « moyen » ou « élevé » ;
- 1er avril 2020 pour les systèmes électroniques BES dont l'impact est « faible ».

6. Contexte : Aucune disposition particulière

B. Exigences et mesures

Aucune disposition particulière

C. Conformité

1. Processus de surveillance de la conformité

1.1. Responsable des mesures pour assurer la conformité

La Régie de l'énergie est responsable, au Québec, de la surveillance de l'application de la norme de fiabilité et de son annexe qu'elle adopte.

1.2. Conservation des pièces justificatives

Aucune disposition particulière

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

Aucune disposition particulière

1.4. Autres informations sur la conformité

Aucune disposition particulière

2. Tableau des éléments de conformité

Aucune disposition particulière

D. Différences régionales

Aucune disposition particulière

E. Interprétations

Aucune disposition particulière

F. Documents connexes

Aucune disposition particulière

CIP-002-5.1a — Annexe 1

Aucune disposition particulière

Principes directeurs et fondements techniques

Aucune disposition particulière

Raisonnement

Aucune disposition particulière

Historique des révisions

Révision	Date	Intervention	Suivi des modifications
0	xx mois 20xx	Nouvelle annexe.	Nouvelle

A. Introduction

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

2. Numéro : CIP-003-7

3. Objet : Définir des mécanismes de gestion de la sécurité cohérents et viables qui établissent les responsabilités et l'imputabilité à l'égard de la protection des *systèmes électroniques BES* contre les compromissions qui pourraient entraîner un fonctionnement incorrect ou des instabilités dans le *système de production-transport d'électricité* (*BES*).

4. Applicabilité :

4.1. Entités fonctionnelles : Dans le contexte des exigences de la présente norme, les entités fonctionnelles indiquées ci-après seront appelées collectivement les « entités responsables ». Dans le cas des exigences de cette norme qui visent une entité fonctionnelle particulière ou un sous-ensemble particulier d'entités fonctionnelles, la ou les entités fonctionnelles sont précisées explicitement.

4.1.1 ***Responsable de l'équilibrage***

4.1.2 ***Distributeur*** qui possède un ou plusieurs des systèmes, *installations* et équipements suivants pour la protection ou la remise en charge du *BES* :

4.1.2.1 Chaque système de délestage de *charge* en sous-fréquence (DSF) ou de délestage de *charge* en sous-tension (DST) qui :

4.1.2.1.1 fait partie d'un programme de délestage de *charge* visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou de l'*entité régionale* ; et

4.1.2.1.2 effectue du délestage automatique de *charge* de 300 MW ou plus par un système de commande commun détenu par l'entité responsable, sans intervention humaine.

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

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

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

4.1.3 ***Exploitant d'installation de production***

4.1.4 ***Propriétaire d'installation de production***

4.1.5 ***Coordonnateur des échanges*** **ou** ***responsable des échanges***

4.1.6 ***Coordonnateur de la fiabilité***

4.1.7 ***Exploitant de réseau de transport***

4.1.8 ***Propriétaire d'installation de transport***

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

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

4.2.1.1 Chaque système DSF ou DST qui :

4.2.1.1.1 fait partie d'un programme de délestage de *charge* visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou de l'*entité régionale* ; et

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

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

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

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

4.2.2 Entités responsables indiquées en 4.1, sauf les *distributeurs* :

Toutes les *installations* du *BES*.

4.2.3 Exemptions : Sont exemptés de la norme CIP-003-7 :

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-003-7.

6. Contexte :

La norme CIP-003 fait partie d'une série de normes CIP sur la cybersécurité qui exigent la détermination et la catégorisation initiales des *systèmes électroniques BES*. Ces normes exigent aussi 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 DSF et DST. Ce seuil particulier de 300 MW pour les systèmes DSF et DST provient de la version 1 des normes CIP sur la cybersécurité. Ce seuil demeure à 300 MW puisqu'il concerne spécifiquement les systèmes DST et DSF, qui constituent des efforts de dernier recours pour sauver le *BES*. Un examen des tolérances des systèmes DSF définies dans les normes de fiabilité régionales pour les exigences des programmes de DSF à ce jour indique que la valeur historique de 300 MW représente une valeur de seuil adéquate et raisonnable pour les tolérances d'exploitation admissibles des systèmes DSF.

B. Exigences et mesures

E1. Chaque entité responsable doit réexaminer et faire approuver par un *cadre supérieur CIP*, au moins une fois tous les 15 mois civils, une ou plusieurs politiques de cybersécurité documentées qui, collectivement, couvrent les thèmes suivants : *[Facteur de risque de non-conformité : moyen] [Horizon : planification de l'exploitation]*

1.1 Pour ses *systèmes électroniques BES* à impact élevé ou moyen, le cas échéant :

1.1.1. personnel et formation (CIP-004) ;

1.1.2. *périmètres de sécurité électronique* (CIP-005), y compris l'*accès distant interactif ;*

1.1.3. sécurité physique des *systèmes électroniques BES* (CIP-006) ;

1.1.4. gestion de la sécurité des systèmes (CIP-007) ;

1.1.5. déclaration des incidents et planification des mesures d'intervention (CIP-008) ;

1.1.6. plans de rétablissement des *systèmes électroniques BES* (CIP-009) ;

1.1.7. gestion des changements de configuration et analyses de vulnérabilité (CIP-010) ;

1.1.8. protection de l'information (CIP-011) ; et

1.1.9. déclaration 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 de surveillance de la conformité aux normes de fiabilité de la NERC.

1.2. Conservation des pièces justificatives

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

L'entité responsable doit conserver les données ou 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 et d'évaluation de la conformité

Audits de conformité

Déclarations sur la conformité

Contrôles ponctuels

Enquêtes de conformité

Déclarations de non-conformité

Plaintes

1.4. Autres informations sur la conformité

Aucune.

2. Tableau des éléments de conformité

Ex.	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-003-7)			
			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	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	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	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

Ex.	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-003-7)			
			VSL faible	**VSL modéré**	**VSL élevé**	**VSL critique**
			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 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	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 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*	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 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*	L'entité responsable n'a pas fait approuver par le *cadre 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

Ex.	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-003-7)			
			VSL faible	**VSL modéré**	**VSL élevé**	**VSL critique**
			les critères de la norme CIP-002, mais dans un délai de plus de 15 mois civils et d'au plus 16 mois civils suivant le réexamen précédent. (E1.2) 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)	*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 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)	*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 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)	actifs qui comportent des *systèmes électroniques BES* à impact faible selon les 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	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	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	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.

Ex.	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-003-7)			
			VSL faible	**VSL modéré**	**VSL élevé**	**VSL critique**
			conformément à la section 1 de l'annexe 1 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)	civils conformément à la section 1 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 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)	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 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	(E2)

Ex.	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-003-7)			
			VSL faible	**VSL modéré**	**VSL élevé**	**VSL critique**
			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 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	OU 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*	d'*incident de cybersécurité* au moins une fois tous les 36 mois civils conformément à la 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	

Ex.	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-003-7)			
			VSL faible	**VSL modéré**	**VSL élevé**	**VSL critique**
			L'entité responsable a documenté son ou ses plans 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)	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 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	malveillants à partir d'*actifs électroniques temporaires* gérés par l'entité responsable 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 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*,	

Ex.	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-003-7)			
			VSL faible	**VSL modéré**	**VSL élevé**	**VSL critique**
				risque lié à l'introduction de programmes malveillants à partir d'*actifs électroniques 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*	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 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	Niveaux de gravité de la non-conformité (CIP-003-7)			
			VSL faible	**VSL modéré**	**VSL élevé**	**VSL critique**
				électroniques temporaires et les *supports de stockage amovibles*, mais n'a pas mis en place de mesures 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	Niveaux de gravité de la non-conformité (CIP-003-7)			
			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.	
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.
7	19 avril 2018	Ordonnance de la FERC approuvant la norme CIP-003-7 (dossier RM17-11-000).	

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, 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 ;

5.3 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 à 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 à la section 5.2 : 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.

3. Exemples non limitatifs de pièces justificatives attestant la conformité à 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 à 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 la caractéristique *BES*, l'utilisation additionnelle du terme « *BES* » vise ici à renforcer la portée d'applicabilité pour ces *installations*, en particulier dans cette section sur l'applicabilité. Cela établit quels sont les *installations*, systèmes et équipements visés par les normes.

Exigence E1

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 à l'exigence E1 de la norme CIP-003-7.

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 003-7. 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-003-7, 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.

<u>Exemption de l'exigence de contrôle des accès électroniques</u>

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

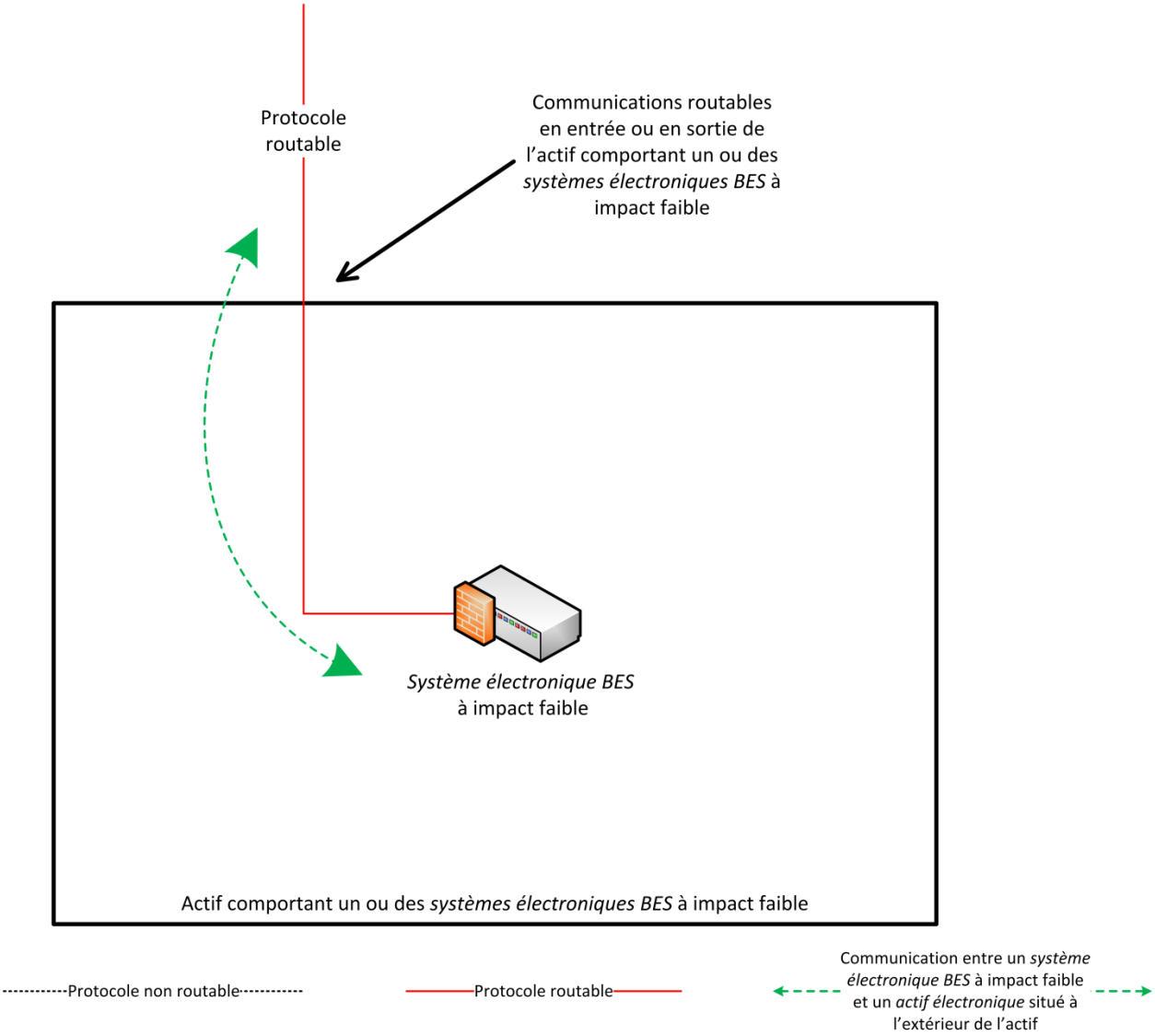
Les schémas des pages suivantes présentent des exemples conceptuels qui illustrent diverses situations de contrôle des accès électroniques. Quels que soient les concepts ou les configurations choisis par l'entité responsable, le but recherché est de réaliser l'objectif de sécurité suivant : autoriser 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.

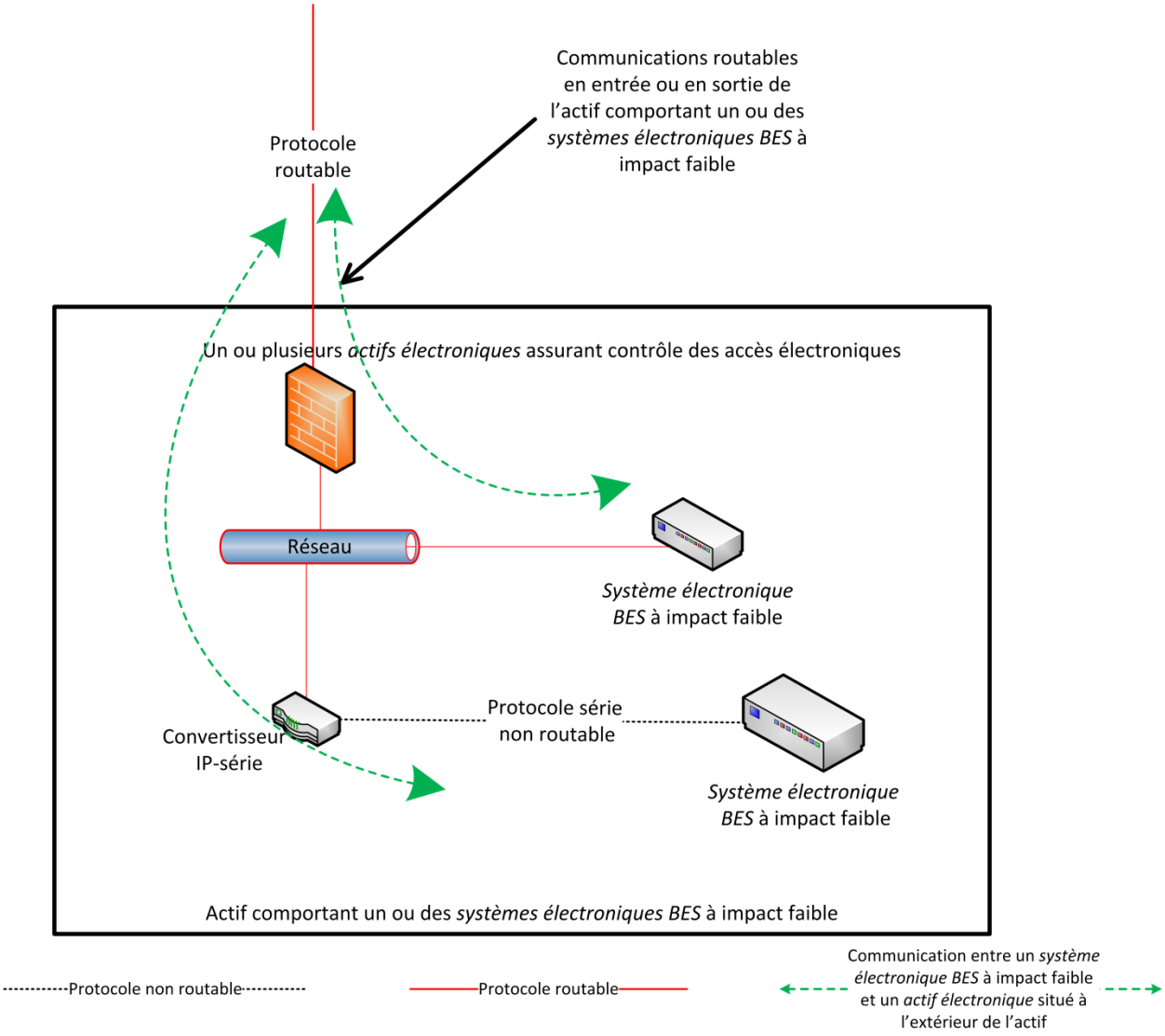


Modèle de référence 1

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.

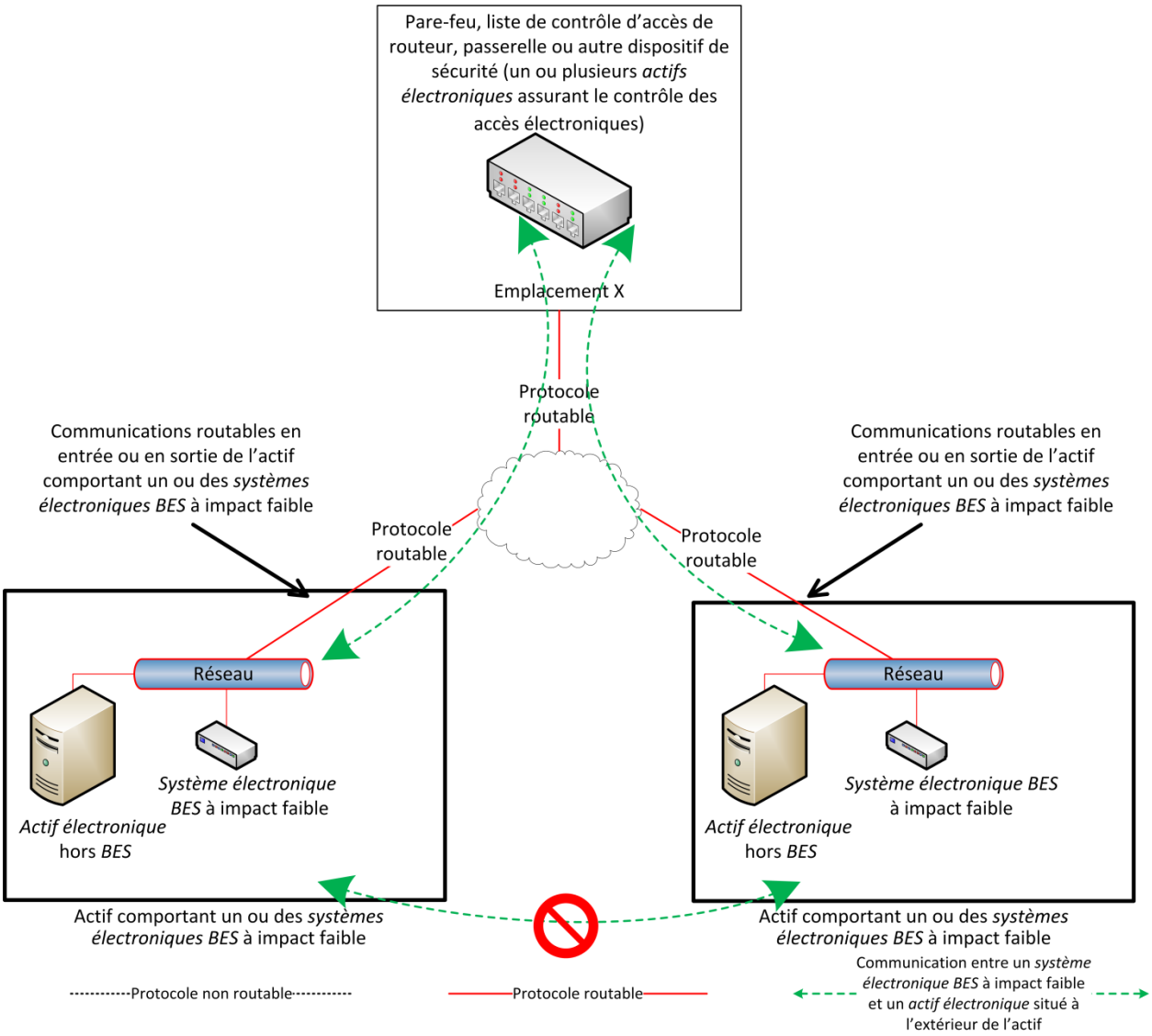


Modèle de référence 2

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.

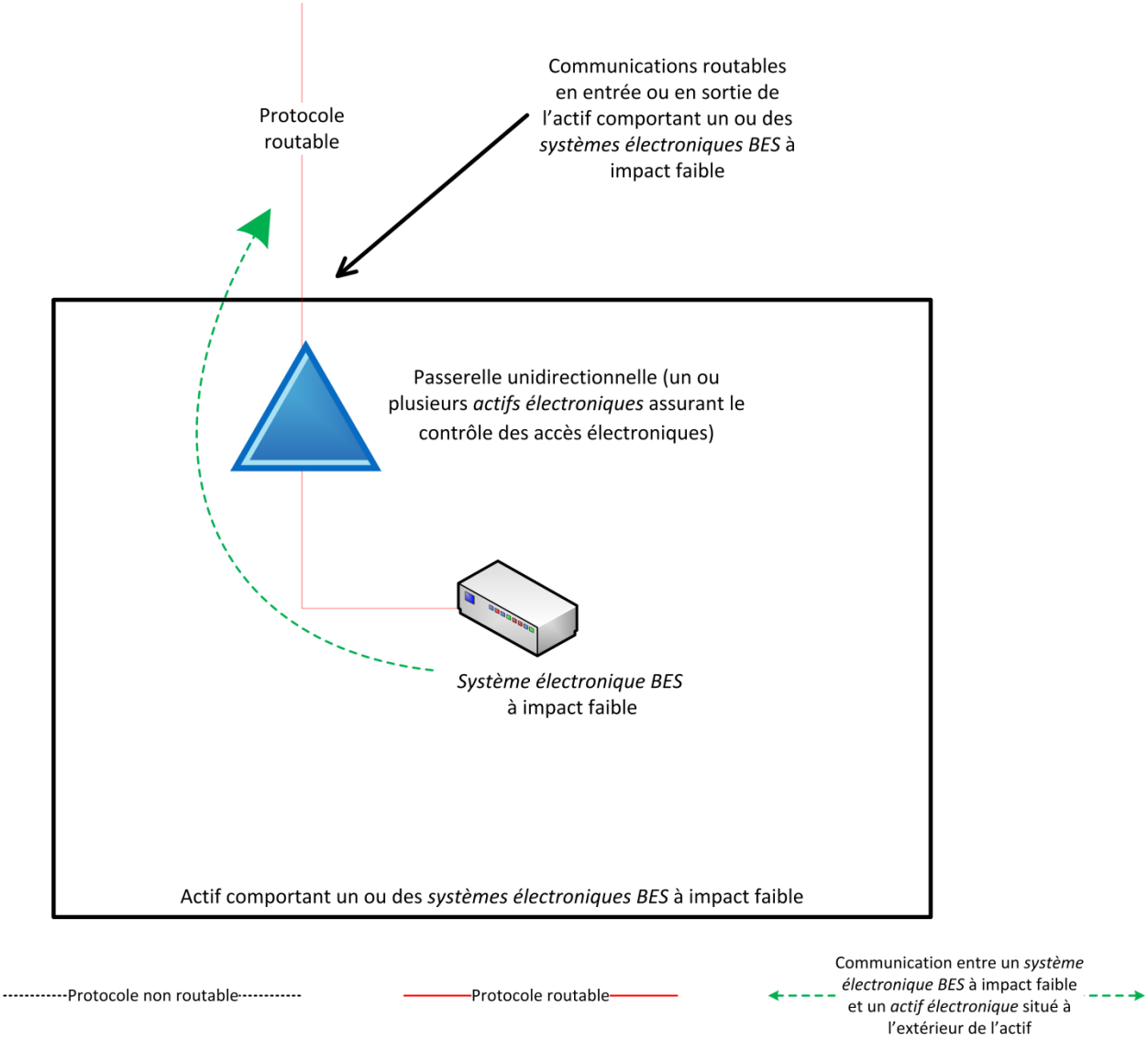


Modèle de référence 3

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.

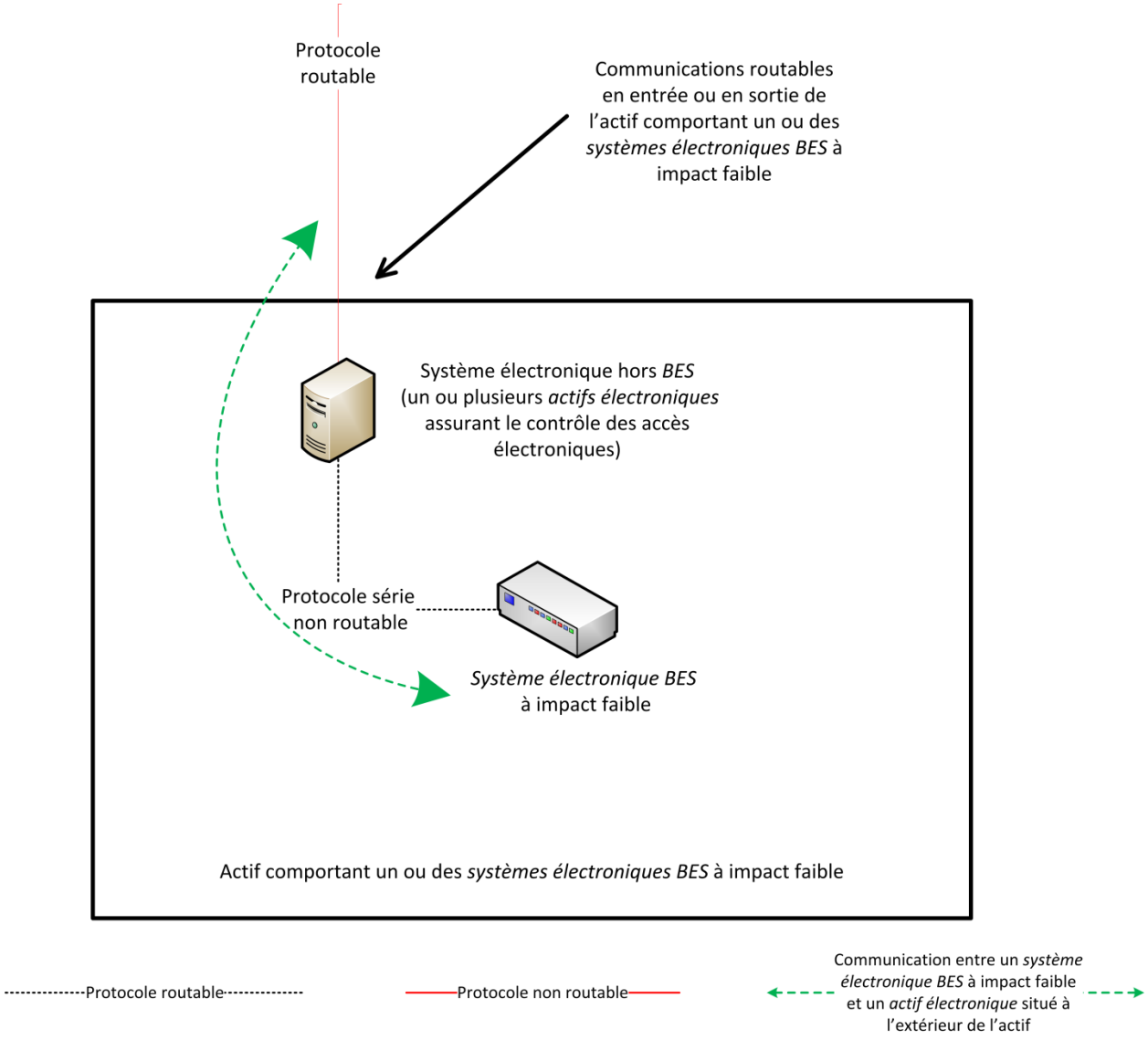


Modèle de référence 4

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.

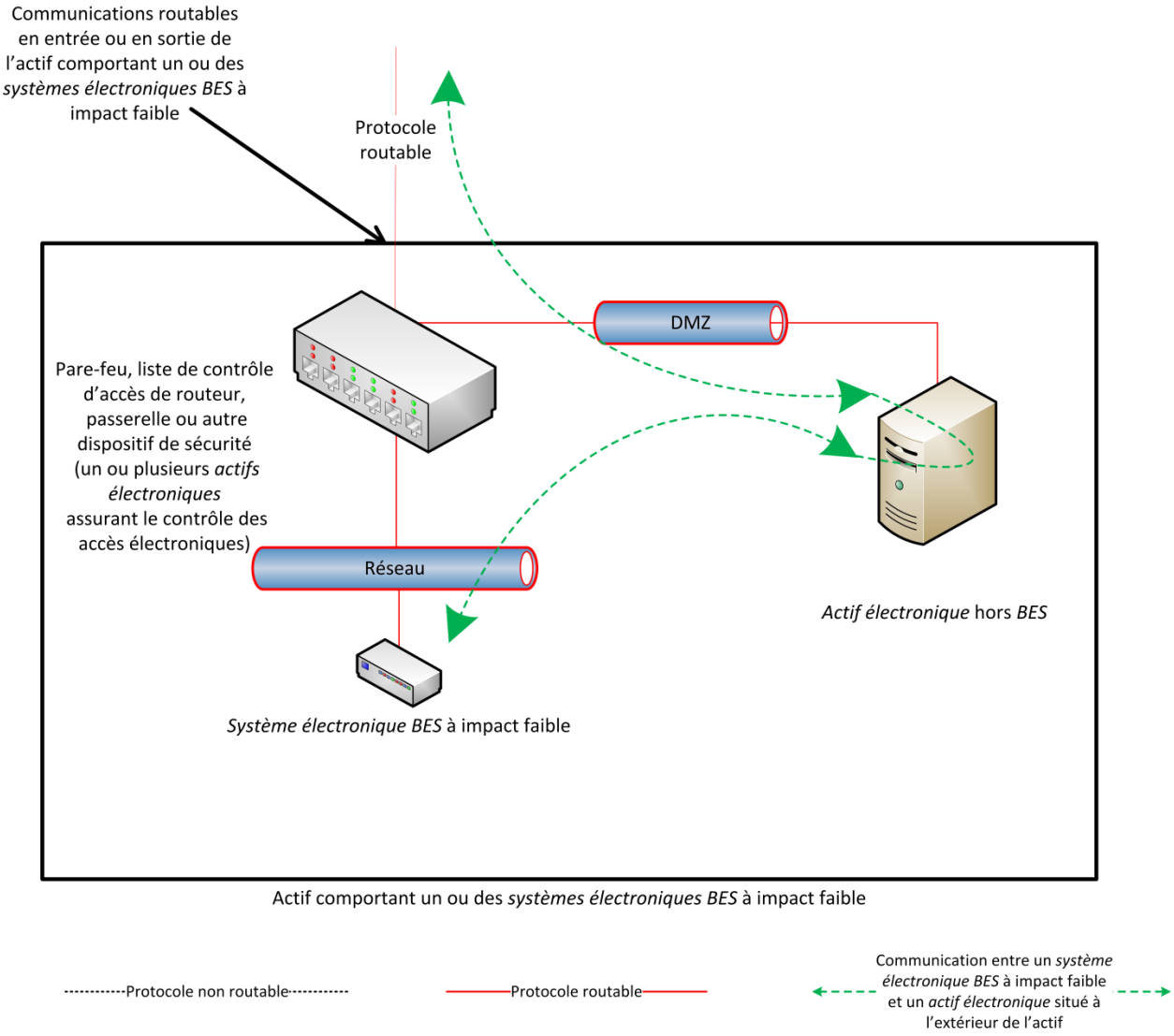


Modèle de référence 5

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.

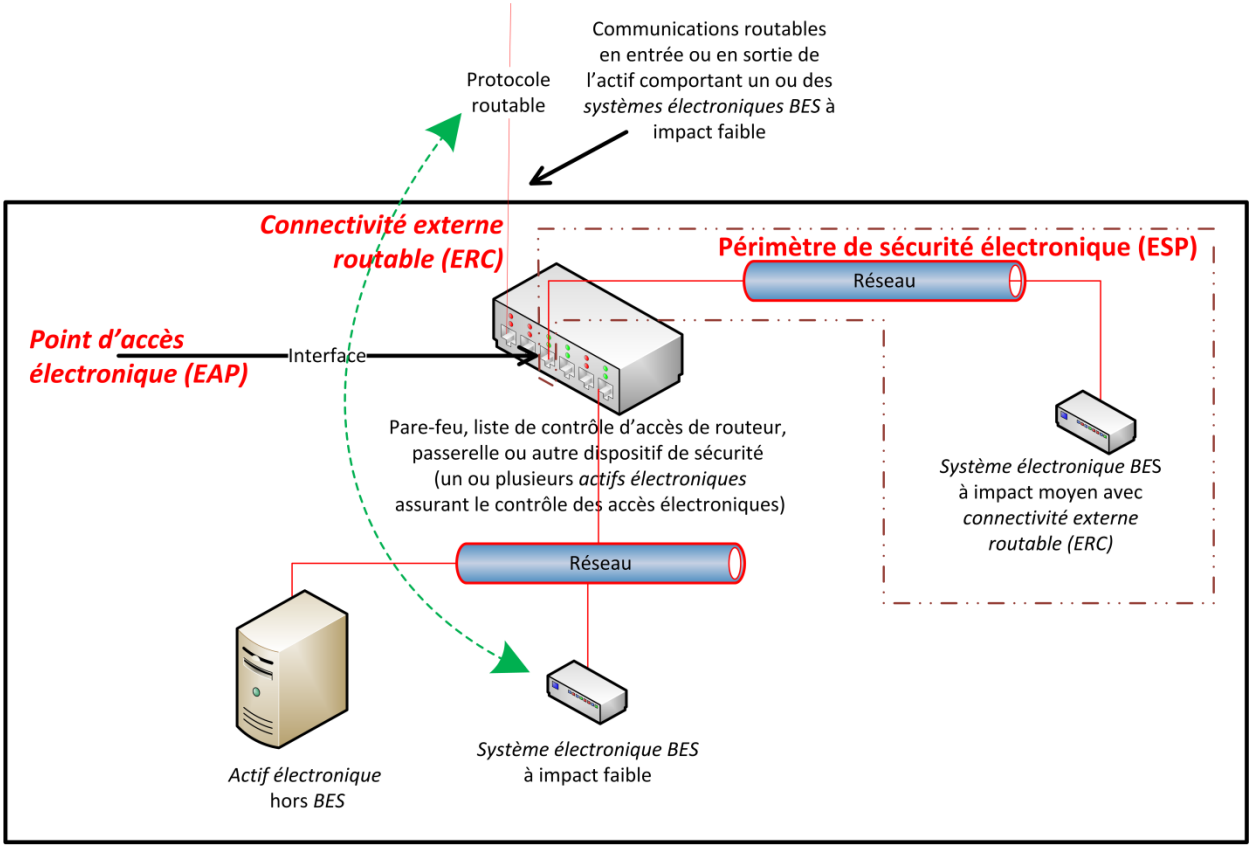


Modèle de référence 6

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

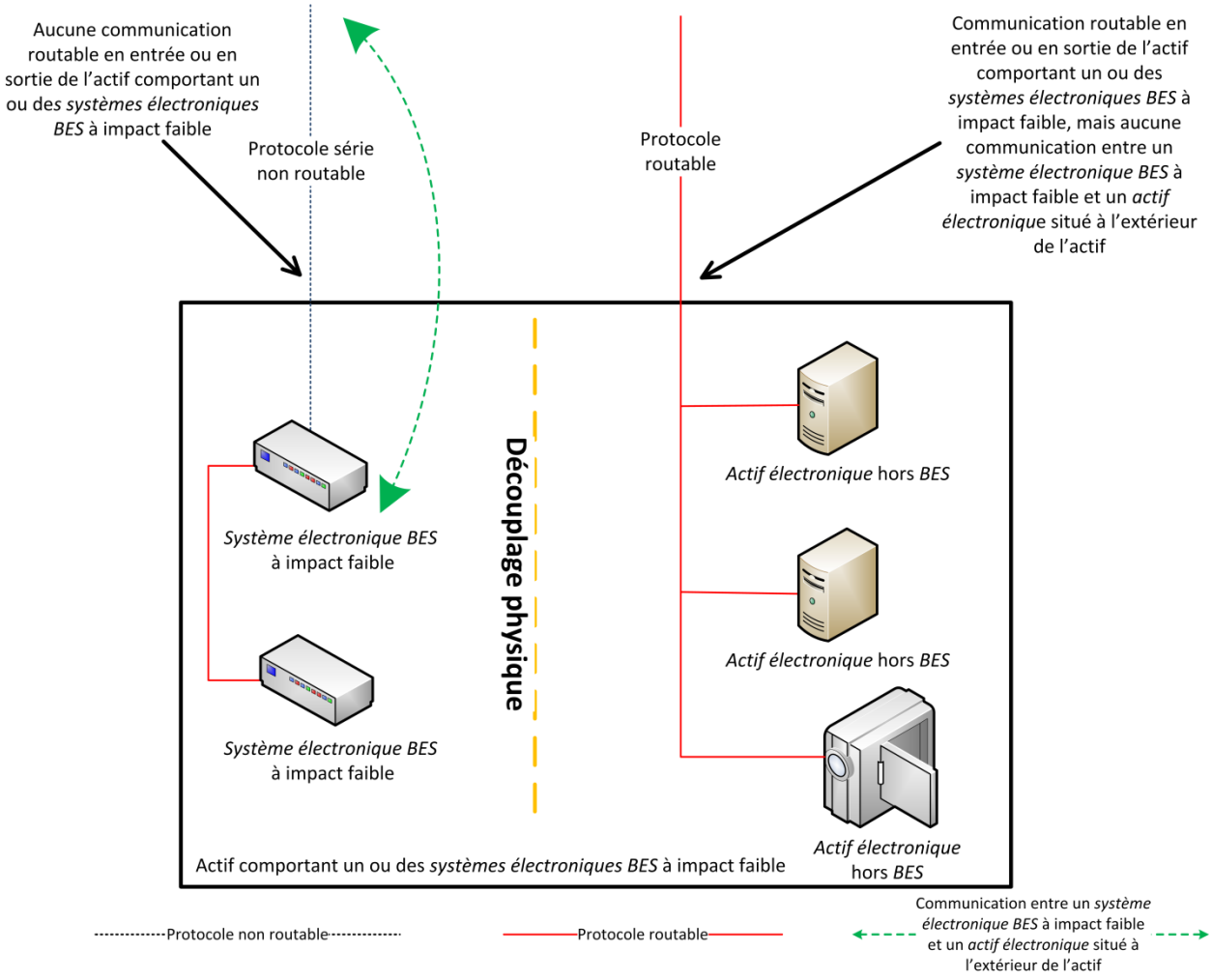
Modèle de référence 8 – Découplage physique et communication série non routable – Contrôle des accès électroniques non exigé

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.

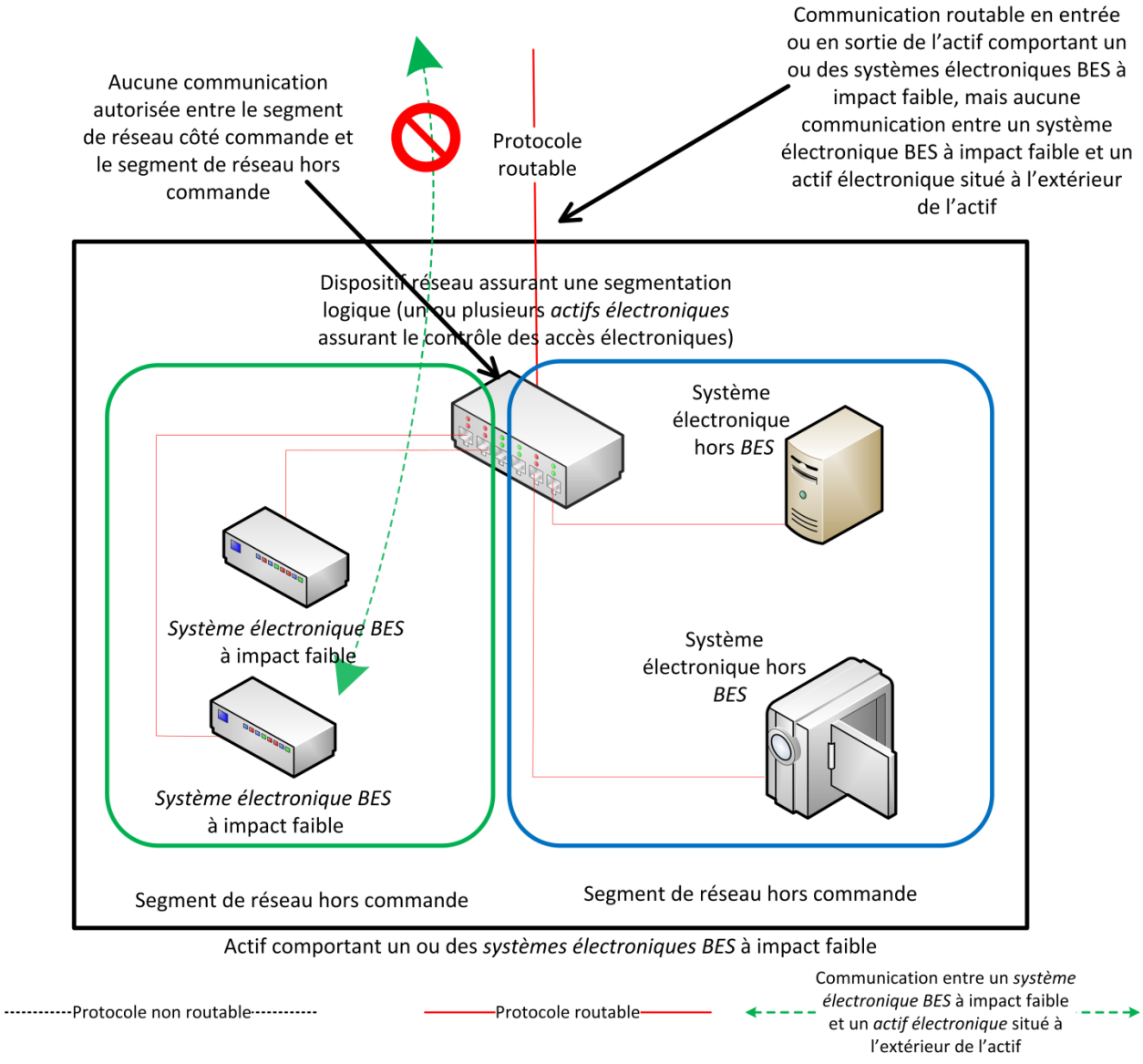
3) Une communication par protocole routable entre les *systèmes électroniques BES* à impact faible et d'autres *actifs électroniques*, par exemple entre les premier et deuxième *systèmes électroniques BES* à impact faible de la figure, ne nécessite pas de contrôle des accès électroniques pourvu que les 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

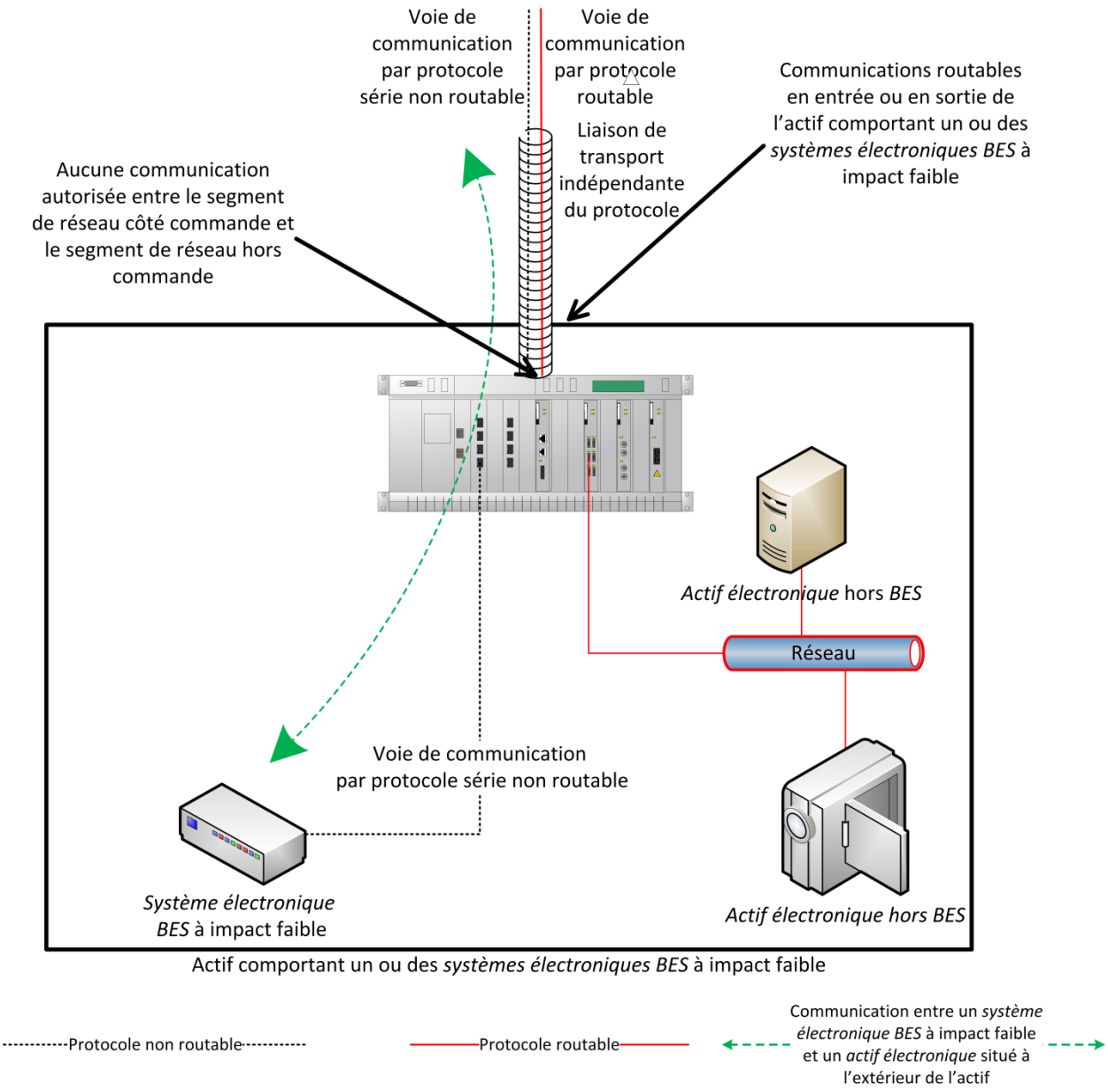
faible et un *actif électronique* situé à l'extérieur de l'actif. En outre, il n'existe aucun accès indirect parce que les *actifs électroniques* hors *BES* capables de communiquer avec l'extérieur de l'actif sont strictement empêchés de communiquer vers le ou les *systèmes électroniques BES* à impact 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.

Section 5.2 : 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.

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

- 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.

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-003-7 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-003-7, 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.

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

A. Introduction

1. Titre : Cybersécurité — Mécanismes de gestion de la sécurité

2. Numéro : CIP-003-7

3. Objet : Aucune disposition particulière

4. Applicabilité :

4.1. Entités Fonctionnelles

Aucune disposition particulière

4.2. Installations

La présente norme s'applique seulement aux installations du *réseau de transport principal* (RTP) et aux installations spécifiées pour le *distributeur*. Dans l'application de cette norme, toute référence aux termes « *système de production-transport d'électricité* » ou « BES » doit être remplacée par les termes « *réseau de transport principal* » ou « RTP » respectivement.

Exemptions additionnelles

Sont exemptés de l'application de la présente norme :

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

5. Date d'entrée en vigueur au Québec :

5.1. Adoption de la norme par la Régie de l'énergie : xx mois 20xx

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

5.3. Date d'entrée en vigueur de la norme et de l'annexe au Québec : 1er janvier 2020

Norme	Date de mise en application au Québec		
	Entités visées par la version 1 des normes CIP adoptées par la Régie	Entités exemptées de l'application de la version 1 des normes CIP en vertu des dispositions particulières associées à ces normes	Entités qui possèdent des installations de production à vocation industrielle
CIP-003-7	2020-01-01	2020-01-01	2020-04-01
CIP-003-7, E1 l'alinéa 1.2	2020-01-01	2020-01-01	2020-04-01
CIP-003-7, E2	2020-01-01	2020-01-01	2020-04-01
CIP-003-7, Annexe 1, Sect.1	2020-01-01	2020-01-01	2020-04-01
CIP-003-7, Annexe 1, Sect.2	2020-01-01	2020-01-01	2020-04-01
CIP-003-7, Annexe 1, Sect.3	2020-01-01	2020-01-01	2020-04-01
CIP-003-7, Annexe 1, Sect.4	2020-01-01	2020-01-01	2020-04-01
CIP-003-7, Annexe 1, Sect.5	2020-01-01	2020-01-01	2020-04-01

L'adoption de la présente norme doit coïncider avec la suspension de l'entrée en vigueur de l'Annexe 1, section 2 et 3 de la norme CIP-003-6.[1]

Les ajouts et modifications proposés au glossaire pour les termes suivants doivent être approuvés et en vigueur en même temps que la norme :[1]

- « *actif électronique temporaire* »;
- « *support de stockage amovible* ».

6. Contexte : Aucune disposition particulière

B. Exigences et mesures

Aucune disposition particulière

C. Conformité

1. Processus de surveillance de la conformité

1.1. Responsable des mesures pour assurer la conformité

[1] Cette section sera retirée suivant l'adoption de la norme par la Régie.

La Régie de l'énergie est responsable, au Québec, de la surveillance de l'application de la norme de fiabilité et de son annexe qu'elle adopte.

1.2. Conservation des pièces justificatives

Aucune disposition particulière

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

Aucune disposition particulière

1.4. Autres informations sur la conformité

Aucune disposition particulière

2. Tableau des éléments de conformité

Aucune disposition particulière

D. Différences régionales

Aucune disposition particulière

E. Interprétations

Aucune disposition particulière

F. Documents connexes

Aucune disposition particulière

Annexe 1

Aucune disposition particulière

Annexe 2

Aucune disposition particulière

Principes directeurs et fondements techniques

Aucune disposition particulière

Justification

Aucune disposition particulière

Historique des versions

Révision	Date	Intervention	Suivi des modifications
0	Xx mois 20xx	Nouvelle annexe.	Nouvelle