

A. Introduction

1. **Titre :** Cybersécurité – Mécanismes de gestion de la sécurité
2. **Numéro :** CIP-003-8
3. **Objet :** Définir des mécanismes de gestion de la sécurité cohérents et viables qui établissent les responsabilités et l'imputabilité à l'égard de la protection des *systèmes électroniques BES* contre les compromissions qui pourraient entraîner un fonctionnement incorrect ou des instabilités dans le *système de production-transport d'électricité (BES)*.
4. **Applicabilité :**
 - 4.1. **Entités fonctionnelles :** Dans le contexte de la présente norme, les entités fonctionnelles indiquées ci-après sont appelées collectivement « entités responsables ». Si certaines exigences visent plus spécifiquement une entité fonctionnelle ou un sous-ensemble d'entités fonctionnelles, la ou les entités fonctionnelles sont précisées explicitement.
 - 4.1.1. **Responsable de l'équilibrage**
 - 4.1.2. **Distributeur** qui possède un ou plusieurs des systèmes, *installations* et équipements suivants pour la protection ou la remise en charge du *BES* :
 - 4.1.2.1. Système de délestage de *charge* en sous-fréquence (DSF) ou en sous-tension (DST) qui :
 - 4.1.2.1.1. fait partie d'un programme de délestage de *charge* visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou de l'*entité régionale* ; et
 - 4.1.2.1.2. effectue des délestages automatiques de *charge* de 300 MW ou plus sous la commande d'un système commun détenu par l'entité responsable, sans intervention humaine.
 - 4.1.2.2. *Automatisme de réseau (RAS)* visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou de l'*entité régionale*.
 - 4.1.2.3. *Système de protection* de réseau de *transport* (à l'exclusion des systèmes de DSF et de DST) visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou de l'*entité régionale*.
 - 4.1.2.4. *Chemin de démarrage* et groupe d'*éléments* respectant les exigences relatives aux manœuvres initiales depuis une *ressource à démarrage autonome* jusqu'au premier point de raccordement, inclusivement, d'alimentation des services auxiliaires du ou des prochains groupes de production à démarrer.
 - 4.1.3. **Exploitant d'installation de production**
 - 4.1.4. **Propriétaire d'installation de production**
 - 4.1.5. **Coordonnateur de la fiabilité**
 - 4.1.6. **Exploitant de réseau de transport**
 - 4.1.7. **Propriétaire d'installation de transport**

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

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

4.2.1.1. Système de DSF ou de DST qui :

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

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

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

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

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

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

Toutes les *installations* du *BES*.

4.2.3. Exemptions : Sont exemptés de la norme CIP-003-8 :

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

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

4.2.3.3. Les systèmes, structures et composants régis par la U.S. Nuclear Regulatory Commission en vertu d'un plan de cybersécurité, conformément au règlement CFR 10, section 73.54.

4.2.3.4. Dans le cas des *distributeurs*, les systèmes et les équipements non mentionnés à la section 4.2.1 ci-dessus.

5. Dates d'entrée en vigueur :

Voir le plan de mise en œuvre de la norme CIP-003-8.

6. Contexte :

La norme CIP-003 fait partie d'une série de normes CIP sur la cybersécurité qui exigent l'inventaire et la catégorisation initiales des *systèmes électroniques BES* ainsi que des mesures organisationnelles, opérationnelles et administratives pour atténuer les risques aux *systèmes électroniques BES*.

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

L'expression « processus documenté » désigne un ensemble de consignes spécifiques à l'entité responsable et visant à produire un résultat particulier. Cette expression n'implique pas de structure de nommage ou d'approbation au-delà de la formulation des exigences. Une entité doit inclure tout ce qu'elle juge nécessaire dans ses processus documentés, mais en s'assurant de bien couvrir les exigences pertinentes.

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

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

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

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

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

Plusieurs références de la section Applicabilité utilisent un seuil de 300 MW pour les systèmes de DSF et de DST. Ce seuil particulier de 300 MW pour les systèmes de DSF et de DST provient de la version 1 des normes CIP sur la cybersécurité. Ce seuil demeure à 300 MW puisqu'il concerne spécifiquement les systèmes de DST et de DSF, qui constituent des efforts de dernier recours pour sauver le *BES*. Un examen des tolérances des systèmes de DSF définies dans les normes de fiabilité régionales pour les exigences des programmes de DSF à ce jour indique que

la valeur historique de 300 MW représente une valeur de seuil adéquate et raisonnable pour les tolérances d'exploitation admissibles des systèmes de DSF.

B. Exigences et mesures

E1. Chaque entité responsable doit réexaminer et faire approuver par un *cadre supérieur CIP*, au moins une fois tous les 15 mois civils, une ou plusieurs politiques de cybersécurité documentées qui, collectivement, couvrent les thèmes suivants :

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

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

1.1.1. personnel et formation (CIP-004) ;

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

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

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

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

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

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

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

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

1.2. Pour ses actifs qui comportent des *systèmes électroniques BES* à impact faible selon les critères de la norme CIP-002, le cas échéant :

1.2.1. sensibilisation à la cybersécurité ;

1.2.2. mesures de sécurité physique ;

1.2.3. contrôle des accès électroniques ;

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

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

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

M1. Exemples non limitatifs de pièces justificatives : documents de politique ; historique de révisions, dossiers d'examen ou preuves de flux de travail provenant d'un système de gestion documentaire qui attestent le réexamen de chaque politique de cybersécurité au moins une fois tous les 15 mois civils ; et approbation documentée de chaque politique de cybersécurité par le *cadre supérieur CIP*.

E2. Chaque entité responsable qui détient au moins un actif comportant des *systèmes électroniques BES* à impact faible, selon les critères de la norme CIP-002, doit mettre en œuvre pour ses *systèmes électroniques BES* à impact faible un ou plusieurs plans de cybersécurité documentés comprenant toutes les sections de l'annexe 1.

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

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

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

C. Conformité

1. Processus de surveillance de la conformité

1.1. Responsable des mesures pour assurer la conformité

Selon la définition des règles de procédure de la NERC, le terme « *responsable des mesures pour assurer la conformité* » (*CEA*) désigne la NERC ou l'*entité régionale* dans leurs rôles respectifs visant à surveiller et à assurer la conformité avec les normes de fiabilité de la NERC.

1.2. Conservation des pièces justificatives

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

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

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

1.3. Processus de surveillance de la conformité et d'application des normes

Audits de conformité

Déclarations sur la conformité

Contrôles ponctuels

Enquêtes de conformité

Déclarations de non-conformité

Plaintes

1.4. Autres informations sur la conformité

Aucune.

Niveau de gravité de la non-conformité (VSL)

Ex.	Horizon	VRF	Niveau de gravité de la non-conformité (CIP-003-8)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
E1.	Planification de l'exploitation	Moyen	<p>L'entité responsable a documenté et mis en œuvre une ou plusieurs politiques de cybersécurité pour ses <i>systèmes électroniques BES</i> à impact élevé et moyen, mais en omettant l'un des neuf thèmes indiqués à l'exigence E1. (E1.1)</p> <p>OU</p> <p>L'entité responsable a terminé le réexamen de sa ou ses politiques de cybersécurité documentées pour ses <i>systèmes électroniques BES</i> à impact élevé et moyen selon l'exigence E1, mais dans un délai de plus de 15 mois civils et d'au plus 16 mois civils suivant le réexamen précédent. (E1.1)</p> <p>OU</p> <p>L'entité responsable a fait approuver par le <i>cadre supérieur CIP</i> sa ou ses politiques de cybersécurité documentées pour ses <i>systèmes électroniques</i></p>	<p>L'entité responsable a documenté et mis en œuvre une ou plusieurs politiques de cybersécurité pour ses <i>systèmes électroniques BES</i> à impact élevé et moyen, mais en omettant deux des neuf thèmes indiqués à l'exigence E1. (E1.1)</p> <p>OU</p> <p>L'entité responsable a terminé le réexamen de sa ou ses politiques de cybersécurité documentées pour ses <i>systèmes électroniques BES</i> à impact élevé et moyen selon l'exigence E1, mais dans un délai de plus de 16 mois civils et d'au plus 17 mois civils suivant le réexamen précédent. (E1.1)</p> <p>OU</p> <p>L'entité responsable a fait approuver par le <i>cadre supérieur CIP</i> sa ou ses politiques de cybersécurité documentées pour ses <i>systèmes électroniques</i></p>	<p>L'entité responsable a documenté et mis en œuvre une ou plusieurs politiques de cybersécurité pour ses <i>systèmes électroniques BES</i> à impact élevé et moyen, mais en omettant trois des neuf thèmes indiqués à l'exigence E1. (E1.1)</p> <p>OU</p> <p>L'entité responsable a terminé le réexamen de sa ou ses politiques de cybersécurité documentées pour ses <i>systèmes électroniques BES</i> à impact élevé et moyen selon l'exigence E1, mais dans un délai de plus de 17 mois civils et d'au plus 18 mois civils suivant le réexamen précédent. (E1.1)</p> <p>OU</p> <p>L'entité responsable a fait approuver par le <i>cadre supérieur CIP</i> sa ou ses politiques de cybersécurité documentées pour ses <i>systèmes électroniques</i></p>	<p>L'entité responsable a documenté et mis en œuvre une ou plusieurs politiques de cybersécurité pour ses <i>systèmes électroniques BES</i> à impact élevé et moyen, mais en omettant au moins quatre des neuf thèmes indiqués à l'exigence E1. (E1.1)</p> <p>OU</p> <p>L'entité responsable n'avait aucune politique de cybersécurité documentée pour ses <i>systèmes électroniques BES</i> à impact élevé et moyen, comme le prescrit l'exigence E1. (E1.1)</p> <p>OU</p> <p>L'entité responsable n'a pas terminé le réexamen de sa ou ses politiques de cybersécurité selon l'exigence E1 dans un délai de 18 mois civils suivant le réexamen précédent. (E1)</p> <p>OU</p> <p>L'entité responsable n'a pas fait approuver par le <i>cadre</i></p>

Ex.	Horizon	VRF	Niveau de gravité de la non-conformité (CIP-003-8)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
			<p><i>BES</i> à impact élevé et moyen selon l'exigence E1, mais dans un délai de plus de 15 mois civils et d'au plus 16 mois civils suivant l'approbation précédente. (E1.1)</p> <p>OU</p> <p>L'entité responsable a documenté une ou plusieurs politiques de cybersécurité pour ses actifs qui comportent des <i>systèmes électroniques BES</i> à impact faible selon les critères de la norme CIP-002, mais en omettant un des six thèmes indiqués à l'exigence E1. (E1.2)</p> <p>OU</p> <p>L'entité responsable a terminé le réexamen, selon l'exigence E1, de sa ou ses politiques de cybersécurité documentées pour ses actifs qui comportent des <i>systèmes électroniques BES</i> à impact faible selon les critères de la norme CIP-002, mais dans un délai de plus de 15 mois civils et d'au plus 16 mois civils</p>	<p><i>BES</i> à impact élevé et moyen selon l'exigence E1, mais dans un délai de plus de 16 mois civils et d'au plus 17 mois civils suivant l'approbation précédente. (E1.1)</p> <p>OU</p> <p>L'entité responsable a documenté une ou plusieurs politiques de cybersécurité pour ses actifs qui comportent des <i>systèmes électroniques BES</i> à impact faible selon les critères de la norme CIP-002, mais en omettant deux des six thèmes indiqués à l'exigence E1. (E1.2)</p> <p>OU</p> <p>L'entité responsable a terminé le réexamen, selon l'exigence E1, de sa ou ses politiques de cybersécurité documentées pour ses actifs qui comportent des <i>systèmes électroniques BES</i> à impact faible selon les critères de la norme CIP-002, mais dans un délai de plus de 16 mois civils et</p>	<p><i>BES</i> à impact élevé et moyen selon l'exigence E1, mais dans un délai de plus de 17 mois civils et d'au plus 18 mois civils suivant l'approbation précédente. (E1)</p> <p>OU</p> <p>L'entité responsable a documenté une ou plusieurs politiques de cybersécurité pour ses actifs qui comportent des <i>systèmes électroniques BES</i> à impact faible selon les critères de la norme CIP-002, mais en omettant trois des six thèmes indiqués à l'exigence E1. (E1.2)</p> <p>OU</p> <p>L'entité responsable a terminé le réexamen, selon l'exigence E1, de sa ou ses politiques de cybersécurité documentées pour ses actifs qui comportent des <i>systèmes électroniques BES</i> à impact faible selon les critères de la norme CIP-002, mais dans un délai de plus de 17 mois civils et</p>	<p><i>supérieur CIP</i> sa ou ses politiques de cybersécurité documentées pour ses <i>systèmes électroniques BES</i> à impact élevé et moyen selon l'exigence E1 dans un délai de 18 mois civils suivant l'approbation précédente. (E1.1)</p> <p>OU</p> <p>L'entité responsable a documenté une ou plusieurs politiques de cybersécurité pour ses actifs qui comportent des <i>systèmes électroniques BES</i> à impact faible selon les critères de la norme CIP-002, mais en omettant au moins quatre des six thèmes indiqués à l'exigence E1. (E1.2)</p> <p>OU</p> <p>L'entité responsable n'avait aucune politique de cybersécurité documentée, selon l'exigence E1, pour ses actifs qui comportent des <i>systèmes électroniques BES</i> à impact faible selon les</p>

Ex.	Horizon	VRF	Niveau de gravité de la non-conformité (CIP-003-8)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
			<p>suivant le réexamen précédent. (E1.2)</p> <p>OU</p> <p>L'entité responsable a fait approuver par le <i>cadre supérieur CIP</i>, selon l'exigence E1, sa ou ses politiques de cybersécurité documentées pour ses actifs qui comportent des <i>systèmes électroniques BES</i> à impact faible selon les critères de la norme CIP-002, mais dans un délai de plus de 15 mois civils et d'au plus 16 mois civils suivant l'approbation précédente. (E1.2)</p>	<p>d'au plus 17 mois civils suivant le réexamen précédent. (E1.2)</p> <p>OU</p> <p>L'entité responsable a fait approuver par le <i>cadre supérieur CIP</i>, selon l'exigence E1, sa ou ses politiques de cybersécurité documentées pour ses actifs qui comportent des <i>systèmes électroniques BES</i> à impact faible selon les critères de la norme CIP-002, mais dans un délai de plus de 16 mois civils et d'au plus 17 mois civils suivant l'approbation précédente. (E1.2)</p>	<p>d'au plus 18 mois civils suivant le réexamen précédent. (E1.2)</p> <p>OU</p> <p>L'entité responsable a fait approuver par le <i>cadre supérieur CIP</i>, selon l'exigence E1, sa ou ses politiques de cybersécurité documentées pour ses actifs qui comportent des <i>systèmes électroniques BES</i> à impact faible selon les critères de la norme CIP-002, mais dans un délai de plus de 17 mois civils et d'au plus 18 mois civils suivant l'approbation précédente. (E1.2)</p>	<p>critères de la norme CIP-002. (E1.2)</p> <p>OU</p> <p>L'entité responsable n'a pas fait approuver par le <i>cadre supérieur CIP</i>, selon l'exigence E1, sa ou ses politiques de cybersécurité documentées pour ses actifs qui comportent des <i>systèmes électroniques BES</i> à impact faible selon les critères de la norme CIP-002 dans un délai de 18 mois civils suivant l'approbation précédente. (E1.2)</p>
E2.	Planification de l'exploitation	Faible	<p>L'entité responsable a documenté son ou ses plans de cybersécurité pour ses actifs comportant des <i>systèmes électroniques BES</i> à impact faible, mais n'a pas documenté son plan de sensibilisation à la cybersécurité conformément à la section 1 de l'annexe 1</p>	<p>L'entité responsable a documenté son ou ses plans de cybersécurité pour ses actifs comportant des <i>systèmes électroniques BES</i> à impact faible, mais n'a pas fait de rappel des pratiques de cybersécurité au moins une fois tous les 15 mois civils conformément à la section 1 de l'annexe 1</p>	<p>L'entité responsable a documenté le contrôle des accès physiques pour ses actifs comportant des <i>systèmes électroniques BES</i> à impact faible, mais n'a pas mis en place les mesures de sécurité physique conformément à la section 2 de l'annexe 1 portant sur l'exigence E2. (E2)</p>	<p>L'entité responsable n'a pas documenté et mis en œuvre un ou plusieurs plans de cybersécurité pour ses actifs comportant des <i>systèmes électroniques BES</i> à impact faible conformément à l'annexe 1 portant sur l'exigence E2. (E2)</p>

Ex.	Horizon	VRF	Niveau de gravité de la non-conformité (CIP-003-8)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
			<p>portant sur l'exigence E2. (E2)</p> <p>OU</p> <p>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)</p> <p>OU</p> <p>L'entité responsable a documenté son ou ses plans de cybersécurité pour ses actifs comportant des <i>systèmes électroniques BES</i> à impact faible, mais n'a pas documenté un ou plusieurs plans d'intervention en cas d'<i>incident de cybersécurité</i> conformément à la section 4 de l'annexe 1 portant sur l'exigence E2. (E2)</p> <p>OU</p>	<p>portant sur l'exigence E2. (E2)</p> <p>OU</p> <p>L'entité responsable a documenté son ou ses plans de cybersécurité pour ses actifs comportant des <i>systèmes électroniques BES</i> à impact faible, mais n'a pas documenté de mesures de sécurité physique conformément à la section 2 de l'annexe 1 portant sur l'exigence E2. (E2)</p> <p>OU</p> <p>L'entité responsable a documenté son ou ses plans de cybersécurité pour ses actifs comportant des <i>systèmes électroniques BES</i> à impact faible, mais n'a pas documenté de mesures de contrôle des accès électroniques conformément à la section 3 de l'annexe 1 portant sur l'exigence E2. (E2)</p> <p>OU</p>	<p>OU</p> <p>L'entité responsable a documenté son ou ses plans de cybersécurité pour le contrôle des accès électroniques à ses actifs comportant des <i>systèmes électroniques BES</i> 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)</p> <p>OU</p> <p>L'entité responsable a documenté un ou plusieurs plans d'intervention en cas d'<i>incident de cybersécurité</i> dans le cadre de son ou ses plans de cybersécurité pour ses actifs comportant des <i>systèmes électroniques BES</i> à impact faible, mais n'a pas mis à l'essai chaque plan d'intervention en cas d'<i>incident de cybersécurité</i> au moins une fois tous les 36 mois civils conformément à la</p>	

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

Ex.	Horizon	VRF	Niveau de gravité de la non-conformité (CIP-003-8)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
			<p>concernant les <i>actifs électroniques temporaires</i>, mais n'a pas documenté les mesures applicables aux <i>supports de stockage amovibles</i> conformément à la section 5.3 de l'annexe 1 portant sur l'exigence E2. (E2)</p>	<p>portant sur l'exigence E2. (E2) OU L'entité responsable a documenté son ou ses plans de cybersécurité pour ses actifs comportant des <i>systèmes électroniques BES</i> à impact faible, mais n'a pas documenté le processus consistant à déterminer si un <i>incident de cybersécurité</i> constaté est un <i>incident de cybersécurité à déclarer</i>, 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 <i>actifs électroniques temporaires</i> et les <i>supports de stockage amovibles</i>, mais n'a pas documenté de mesures pour atténuer le risque lié à l'introduction de programmes malveillants à partir d'<i>actifs électroniques</i></p>	<p>l'annexe 1 portant sur l'exigence E2. (E2) OU L'entité responsable a documenté son ou ses plans pour les <i>actifs électroniques temporaires</i> et les <i>supports de stockage amovibles</i>, mais n'a pas mis en place de mesures pour atténuer le risque lié à l'introduction de programmes malveillants à partir d'<i>actifs électroniques temporaires</i> 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 <i>actifs électroniques temporaires</i> et les <i>supports de stockage amovibles</i>, mais n'a pas mis en place de mesures pour neutraliser la menace d'un programme malveillant détecté sur un <i>support de stockage amovible</i> avant de</p>	

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

Ex.	Horizon	VRF	Niveau de gravité de la non-conformité (CIP-003-8)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
				applicables aux <i>supports de stockage amovibles</i> 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 <i>cadre supérieur CIP</i> , mais a documenté un changement concernant celui-ci dans un délai de plus de 30 jours civils et de moins de 40 jours civils suivant ce changement. (E3)	L'entité responsable a désigné nominativement un <i>cadre supérieur CIP</i> , mais a documenté un changement concernant celui-ci dans un délai de plus de 40 jours civils et de moins de 50 jours civils suivant ce changement. (E3).	L'entité responsable a désigné nominativement un <i>cadre supérieur CIP</i> , mais a documenté un changement concernant celui-ci dans un délai de plus de 50 jours civils et de moins de 60 jours civils suivant ce changement. (E3).	L'entité responsable n'a pas désigné nominativement un <i>cadre supérieur CIP</i> . OU L'entité responsable a désigné nominativement un <i>cadre supérieur CIP</i> , mais n'a pas documenté un changement concernant celui-ci dans un délai de 60 jours civils suivant ce changement. (E3)

Ex.	Horizon	VRF	Niveau de gravité de la non-conformité (CIP-003-8)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
E4.	Planification de l'exploitation	Faible	L'entité responsable a désigné un déléataire 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 déléataire 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 déléataire 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 <i>cadre supérieur CIP</i> . (E4) OU L'entité responsable a désigné un déléataire 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	<p>Modifications visant à clarifier les exigences et à mettre les éléments de conformité en concordance avec les plus récentes directives sur l'établissement des éléments de conformité des normes.</p> <p>Suppression de la mention sur la prise en compte des considérations d'affaires.</p> <p>Remplacement de l'organisation régionale de fiabilité par l'<i>entité régionale</i> comme entité responsable.</p> <p>Reformulation de la date d'entrée en vigueur.</p> <p>Remplacement de « <i>responsable de la surveillance de la conformité</i> » par « <i>responsable des mesures pour assurer la conformité</i> ».</p>	
3	16 décembre 2009	<p>Changement du numéro de version de -2 à -3.</p> <p>Dans l'exigence E1.6, suppression de la phrase concernant le retrait du service d'un composant ou d'un système aux fins d'essais, en réponse à l'ordonnance de la FERC du 30 septembre 2009.</p>	
3	16 décembre 2009	Approbation par le Conseil d'administration de la NERC.	
3	31 mars 2010	Approbation par la FERC.	

Version	Date	Intervention	Suivi des modifications
4	24 janvier 2011	Approbation par le Conseil d'administration de la NERC.	
5	26 novembre 2012	Adoption par le Conseil d'administration de la NERC.	Modification en coordination avec les autres normes CIP et révision du format selon le modèle RBS.
5	22 novembre 2013	Ordonnance de la FERC approuvant la norme CIP-003-5.	
6	13 novembre 2014	Adoption par le Conseil d'administration de la NERC.	Mise en œuvre de deux prescriptions de l'ordonnance 791 de la FERC concernant l'obligation de « détecter, évaluer et corriger » ainsi que les réseaux de communication
6	12 février 2015	Adoption par le Conseil d'administration de la NERC.	Remplacement de la version adoptée par le Conseil le 13 novembre 2014. La version à jour met en œuvre des prescriptions en instance de l'ordonnance 791 relativement aux actifs temporaires et aux <i>systèmes électroniques BES</i> 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 <i>LERC</i> et 2) les actifs temporaires.

Version	Date	Intervention	Suivi des modifications
7	19 avril 2018	Ordonnance de la FERC approuvant la norme CIP-003-7 (dossier RM17-11-000).	
8	9 mai 2019	Adoption par le Conseil d'administration de la NERC.	Suppression des références aux plans de défense. Changements en réponse aux prescriptions de l'ordonnance 843 de la FERC concernant l'atténuation des risques liés aux programmes malveillants.
8	31 juillet 2019	Ordonnance de la FERC approuvant la norme CIP-003-8 (dossier RD19-5-000).	

Annexe 1

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

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

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

- Section 1.** Sensibilisation à la cybersécurité : Chaque entité responsable doit rappeler, au moins une fois tous les 15 mois civils, les pratiques de cybersécurité (lesquelles peuvent comprendre des pratiques de sécurité physiques connexes).
- Section 2.** Mesures de sécurité physique : Chaque entité responsable doit contrôler l'accès physique, d'après les besoins qu'elle détermine elle-même, 1) à l'actif ou aux emplacements des *systèmes électroniques BES* à impact faible à l'intérieur de l'actif, et 2) à tout *actif électronique* qu'elle décide d'affecter, conformément à la section 3.1, au contrôle des accès électroniques.
- Section 3.** Contrôle des accès électroniques : Pour chaque actif comportant un ou des *systèmes électroniques BES* à impact faible selon les critères de la norme CIP-002, l'entité responsable doit mettre en place un contrôle des accès électroniques qui :
- 3.1** autorisent uniquement les accès entrants et sortants nécessaires, selon l'évaluation de l'entité responsable, pour toute communication :
 - i. entre un ou des *systèmes électroniques BES* à impact faible et tout *actif électronique* situé à l'extérieur de l'actif comportant un ou des *systèmes électroniques BES* à impact faible ;
 - ii. assurée par un protocole routable en entrée ou en sortie de l'actif comportant le ou les *systèmes électroniques BES* à impact faible ; et
 - iii. ne servant pas à des fonctions de commande ou de protection à délai critique entre des dispositifs électroniques intelligents (par exemple, des communications utilisant le protocole R-GOOSE de la norme CEI TR-61850-90-5) ;
 - 3.2** authentifient toute *connectivité par lien commuté* donnant accès à des *systèmes électroniques BES* à impact faible, selon les capacités de l'*actif électronique*.
- Section 4.** Intervention en cas d'incident de cybersécurité : Chaque entité responsable doit avoir un ou plusieurs plans d'intervention en cas d'*incident de cybersécurité*, par actif ou par groupe d'actifs, qui doivent comprendre :
- 4.1** la détection et le classement des *incidents de cybersécurité*, ainsi que les mesures d'intervention ;
 - 4.2** le processus consistant à déterminer si un *incident de cybersécurité* détecté est un *incident de cybersécurité à déclarer*, puis à en aviser l'Electricity Information Sharing and Analysis Center (E-ISAC), à moins que la loi ne l'interdise ;

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

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

- 5.1 pour tout *actif électronique temporaire* géré par l'entité responsable, le recours à un ou plusieurs des moyens suivants, utilisés en permanence ou à la demande (selon les capacités de l'*actif électronique temporaire*) :
 - logiciel antivirus, avec mises à jour manuelles ou systématiques des signatures ou des séquences de code ;
 - liste blanche d'applications ; ou
 - autres moyens d'atténuer le risque lié à l'introduction de programmes malveillants ;
- 5.2 pour tout *actif électronique temporaire* géré par une tierce partie autre que l'entité responsable :
 - 5.2.1 l'application d'une ou de plusieurs des mesures suivantes avant de connecter l'*actif électronique temporaire* à un *système électronique BES* à impact faible (selon les capacités de l'*actif électronique temporaire*) :
 - examen du degré de maintien à jour de l'antivirus ;
 - examen de la procédure de mise à jour de l'antivirus adoptée par la tierce partie ;
 - examen de l'utilisation par la tierce partie de listes blanches d'applications ;
 - examen de l'utilisation de systèmes d'exploitation et de logiciels exécutables uniquement à partir de supports non inscriptibles ;

- examen des mesures de renforcement du système d'exploitation adoptées par la tierce partie ; ou
 - autres moyens d'atténuation du risque lié à l'introduction de programmes malveillants ;
- 5.2.2** pour toute méthode utilisée conformément à la section 5.2.1, les entités responsables doivent déterminer si des mesures d'atténuation supplémentaires sont nécessaires, et les mettre en œuvre avant de connecter l'*actif électronique temporaire* ;
- 5.3** pour les *supports de stockage amovibles*, le recours à chacun des moyens suivants :
- 5.3.1** mesures permettant de détecter les programmes malveillants sur les *supports de stockage amovibles* au moyen d'un *actif électronique* autre qu'un *système électronique BES* ; et
- 5.3.2** mesures permettant de neutraliser la menace d'un programme malveillant détecté sur un *support de stockage amovible* avant de connecter ce support à un *système électronique BES* à impact faible.

Annexe 2

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

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

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

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

- documentation des mécanismes de contrôle d'accès (carte d'accès, serrures, sécurisation de périmètre, etc.), des mesures de surveillance (systèmes d'alarme, surveillance humaine, etc.) ou d'autres mesures de sécurité physique de nature opérationnelle, administrative ou technique pour le contrôle de l'accès physique :
 - a. à l'actif, s'il y a lieu, ou aux emplacements de *système électronique BES* à impact faible à l'intérieur de l'actif ; et
 - b. à tout *actif électronique* désigné par l'entité responsable comme assurant un contrôle des accès électroniques selon la section 3.1 de l'annexe 1, s'il y a lieu.

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

1. documentation attestant qu'à chaque actif ou groupe d'actifs comportant des *systèmes électroniques BES* à impact faible, toute communication routable entre un ou plusieurs de ces *systèmes électroniques BES* à impact faible et un ou des *actifs électroniques* à l'extérieur de l'actif en question est limitée par un contrôle des accès électroniques aux seuls accès électroniques entrants et sortants que l'entité responsable juge nécessaires, sauf si l'entité peut démontrer qu'il s'agit d'une communication utilisée pour des fonctions de commande ou de protection à délai critique entre des dispositifs électroniques intelligents. Exemples non limitatifs de pièces justificatives : schémas montrant le contrôle des communications entrantes et sortantes entre le ou les *systèmes électroniques BES* à impact faible et un ou des *actifs électroniques* situés à l'extérieur de l'actif comportant ce ou ces *systèmes électroniques BES*, ou des listes de contrôle des accès électroniques mises en œuvre (contrôles d'accès par adresse IP, par ports ou par service, passerelles unidirectionnelles, etc.) ;
2. documentation du mécanisme d'authentification de la *connectivité par lien commuté* (appels sortants limités à un numéro préprogrammé pour la transmission de données, modems à fonction de rappel, modems télécommandés par le *centre de contrôle* ou la salle de commande, contrôle d'accès dans le *système électronique BES*, etc.).

Section 4. Intervention en cas d'incident de cybersécurité : Exemples non limitatifs de pièces justificatives pour la section 4 : documents datés (politiques, procédures, processus, etc.)

d'un ou de plusieurs plans d'intervention en cas d'*incident de cybersécurité* établis par actif ou par groupe d'actifs, qui comprennent les actions suivantes :

1. détecter les *incidents de cybersécurité*, les classer et y répondre ; déterminer si un *incident de cybersécurité* détecté est un *incident de cybersécurité à déclarer* et aviser l'Electricity Information Sharing and Analysis Center (E-ISAC) ;
2. établir et documenter les rôles et responsabilités des groupes ou des personnes chargés d'intervenir en cas d'*incident de cybersécurité* (déclenchement, documentation, surveillance, déclaration, etc.) ;
3. gérer les *incidents de cybersécurité* (confinement, élimination, reprise après incident ou résolution de l'incident, etc.) ;
4. mettre à l'essai le ou les plans, avec documents datés attestant qu'un essai a été fait au moins une fois tous les 36 mois civils ; et
5. mettre à jour au besoin les plans d'intervention en cas d'*incident de cybersécurité* dans les 180 jours civils suivant la mise à l'essai ou suivant un *incident de cybersécurité à déclarer* réel.

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

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

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

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

Principes directeurs et fondements techniques

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

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

La section 4.1. Entités fonctionnelles 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'en ce qui concerne les *distributeurs*, la section 4.1. limite l'applicabilité à ceux qui détiennent certains types de systèmes et d'équipements énumérés à la section 4.2.

La section 4.2. *Installations* définit la portée des *installations*, systèmes et équipements détenus par l'entité responsable désignée à la section 4.1. qui est visée par les exigences de la norme. Outre l'ensemble des *installations* du *BES*, des *centres de contrôle* et des autres systèmes et équipements, la liste comprend l'ensemble des systèmes et équipements détenus par les *distributeurs*. Bien que le terme « *installations* » dans le glossaire de la NERC comprenne déjà l'appartenance au *BES*, l'utilisation additionnelle du terme « *BES* » vise ici à renforcer la portée d'applicabilité pour ces *installations*, en particulier dans cette section sur l'applicabilité. Cela établit quels sont les *installations*, systèmes et équipements visés par les normes.

Exigence E1

Lors de l'élaboration des politiques prescrites à l'exigence E1, le nombre de politiques et leur contenu doivent être guidés par la structure de gestion de l'entité responsable et par son contexte opérationnel. Ces politiques peuvent être intégrées à un programme général de sécurité de l'information pour l'ensemble de l'organisation, ou encore à des programmes particuliers. L'entité responsable a le choix d'élaborer une politique de cybersécurité monolithique qui englobe les thèmes prescrits, mais elle peut aussi créer une politique globale de haut niveau et confier les détails à des documents de niveau inférieur dans la hiérarchie documentaire. Dans le cas d'une politique globale de haut niveau, l'entité responsable devrait fournir la politique globale ainsi que les documents complémentaires afin de démontrer la conformité avec l'exigence E1 de la norme CIP-003-8.

Si une entité responsable détient des *systèmes électroniques BES* à impact élevé ou moyen, la ou les politiques de cybersécurité doivent couvrir les neuf thèmes prescrits à l'alinéa 1.1 de l'exigence E1 de la norme CIP 003-8. Si une entité responsable a répertorié, selon les critères de la norme CIP-002, des actifs comportant des *systèmes électroniques BES* à impact faible, la ou les politiques de cybersécurité doivent couvrir les six thèmes prescrits à l'alinéa 1.2 de l'exigence E1.

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

La mise en œuvre de la politique de cybersécurité n'est pas traitée explicitement dans l'exigence E1 de la norme CIP-003-8, car on considère qu'elle se manifesterait 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 antimaliçieux avant l'exécution de l'*accès distant interactif*
- Tenue à jour des correctifs pour les systèmes d'exploitation et pour les applications qui exécutent l'*accès distant interactif*
- Désactivation des postes de travail VPN avec séparation des flux (*split tunneling*) ou à double résidence (*dual-homed*) avant l'exécution de l'*accès distant interactif*
- Pour les fournisseurs, les contractuels ou les consultants, le recours à des clauses contractuelles qui exigent le respect des mesures de contrôle d'*accès distant interactif* de l'entité responsable

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

- Stratégie de protection des *actifs électroniques* contre les accès physiques non autorisés
- Méthodes acceptables de contrôle des accès physiques
- Surveillance et consignation des accès physiques

1.1.4 Gestion de la sécurité des systèmes (CIP-007)

- Stratégies de renforcement des systèmes
- Méthodes acceptables d'authentification et de contrôle d'accès
- Politiques sur les mots de passe comprenant longueur, complexité, mise en application et prévention des attaques exhaustives
- Surveillance et consignation des activités des *systèmes électroniques BES*

1.1.5 Déclaration des incidents et planification des mesures d'intervention (CIP-008)

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

- Obligations de signaler les *incidents de cybersécurité*
- 1.1.6 Plans de rétablissement des *systèmes électroniques BES* (CIP-009)
 - Disponibilité des composants de rechange
 - Disponibilité des sauvegardes système
- 1.1.7 Gestion des changements de configuration et analyses de vulnérabilité (CIP-010)
 - Demandes de changement
 - Approbation des changements
 - Processus de réparation
- 1.1.8 Protection de l'information (CIP-011)
 - Méthodes de contrôle d'accès à l'information
 - Notification des divulgations non autorisées
 - Accès à l'information selon le principe du besoin de savoir
- 1.1.9 Déclaration des *circonstances CIP exceptionnelles* et mesures d'intervention
 - Processus de recours à des procédures spéciales en cas de *circonstance CIP exceptionnelle*
 - Processus de tolérance des dérogations qui n'enfreignent pas les exigences CIP

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

- 1.2.1 Sensibilisation à la cybersécurité
 - Mesures de sensibilisation à la sécurité
 - Détermination des groupes visés par les mesures de sensibilisation à la cybersécurité
- 1.2.2 Mesures de sécurité physique
 - Approches acceptables pour la sélection des mesures de sécurité physique
- 1.2.3 Contrôle des accès électroniques
 - Approches acceptables pour la sélection des moyens de contrôle des accès électroniques
- 1.2.4 Intervention en cas d'*incident de cybersécurité*
 - Détection des *incidents de cybersécurité*
 - Notifications appropriées en cas de découverte d'un incident
 - Obligations de signaler les *incidents de cybersécurité*
- 1.2.5 Atténuation des risques liés à l'introduction de programmes malveillants à partir d'*actifs électroniques temporaires* ou de *supports de stockage amovibles*
 - Utilisation acceptable des *actifs électroniques temporaires* et des *supports de stockage amovibles*

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

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

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

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

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

Exigence E2

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

Exigence E2, annexe 1

Comme il est indiqué, l'annexe 1 présente les sections à inclure dans tout plan de cybersécurité. Il s'agit de donner aux entités qui ont une combinaison de *systèmes électroniques BES* à impact faible, moyen et élevé la possibilité, si elles le souhaitent, d'appliquer à leurs *systèmes électroniques BES* à impact faible (ou à une partie de ceux-ci) les programmes qu'elles ont établis pour les *systèmes électroniques BES* à impact moyen ou élevé, plutôt que de devoir gérer deux programmes différents. Les plans de cybersécurité établis selon l'exigence E2 amènent les entités responsables à documenter la manière dont elles abordent les différents thèmes présentés. Les plans de cybersécurité peuvent renvoyer à d'autres politiques et procédures qui montrent de quelle manière l'entité responsable entend répondre à chacun des thèmes ; ou encore, l'entité responsable peut élaborer des plans de cybersécurité très complets qui contiennent tous les détails des moyens mis en œuvre. Pour respecter l'exigence, il faut que le plan de cybersécurité contienne (textuellement ou par renvoi) suffisamment de détails quant aux moyens adoptés pour répondre à chacun des thèmes.

Des précisions et éclaircissements pour chacun des thèmes de l'annexe 1 sont présentés ci-après.

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

Le programme de sensibilisation à la cybersécurité oblige les entités à rappeler les bonnes pratiques de cybersécurité à leur personnel au moins une fois tous les 15 mois civils. L'entité est libre de choisir les thèmes à couvrir et la manière de communiquer les rappels sur ces thèmes. Quant aux pièces justificatives attestant la conformité, l'entité responsable doit pouvoir présenter le matériel de sensibilisation utilisé, selon la ou les méthodes de communication employées (affiches, courriels, sujets abordés aux réunions de service, etc.). L'intention de l'équipe de rédaction n'est pas d'obliger les entités

responsables à tenir des listes de destinataires ni à confirmer la réception par le personnel du matériel de sensibilisation.

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

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

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

L'entité responsable est libre de choisir les méthodes utilisées pour réaliser l'objectif de contrôle des accès physiques 1) aux actifs comportant des *systèmes électroniques BES* à impact faible, ou encore aux *systèmes électroniques BES* à impact faible eux-mêmes, et 2) à tout *actif électronique* affecté par l'entité responsable, le cas échéant, au contrôle des accès électroniques. L'entité responsable peut utiliser une ou plusieurs mesures de contrôle d'accès, mesures de surveillance ou autres mesures de sécurité physique de nature opérationnelle, administrative ou technique. Les entités peuvent appliquer des mesures de contrôle d'accès physique à des périmètres étendus (clôtures avec barrières verrouillées, gardiens, politiques d'accès aux sites, etc.) ou encore à des zones plus circonscrites où sont situés les *systèmes électroniques BES* à impact faible, comme les salles de commande ou les *centres de contrôle*.

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

La surveillance comme mesure de sécurité physique peut servir de complément ou de solution de rechange au contrôle d'accès physique. Exemples non limitatifs de mesures de surveillance : 1) systèmes d'alarme sensibles au mouvement ou à l'entrée dans la zone contrôlée ou 2) surveillance humaine de la zone contrôlée. La surveillance n'oblige pas nécessairement à tenir des registres, mais pourrait comprendre la détection qu'un accès physique a eu lieu ou été tenté (alarme de porte, surveillance humaine, etc.). L'intention de l'équipe de rédaction n'est pas de rendre nécessaire une surveillance pour chaque *système électronique BES* à impact faible, mais plutôt une surveillance au niveau approprié pour réaliser l'objectif de sécurité en matière de contrôle d'accès physique.

Il n'est pas exigé d'avoir des programmes d'autorisation des utilisateurs et des listes d'utilisateurs autorisés à un accès physique, bien que ces mesures soient à envisager pour réaliser l'objectif de sécurité.

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

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

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

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

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

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

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

Exemption de l'exigence de contrôle des accès électroniques

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

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

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

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

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

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

Détermination des contrôles des accès électroniques

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

Schémas conceptuels

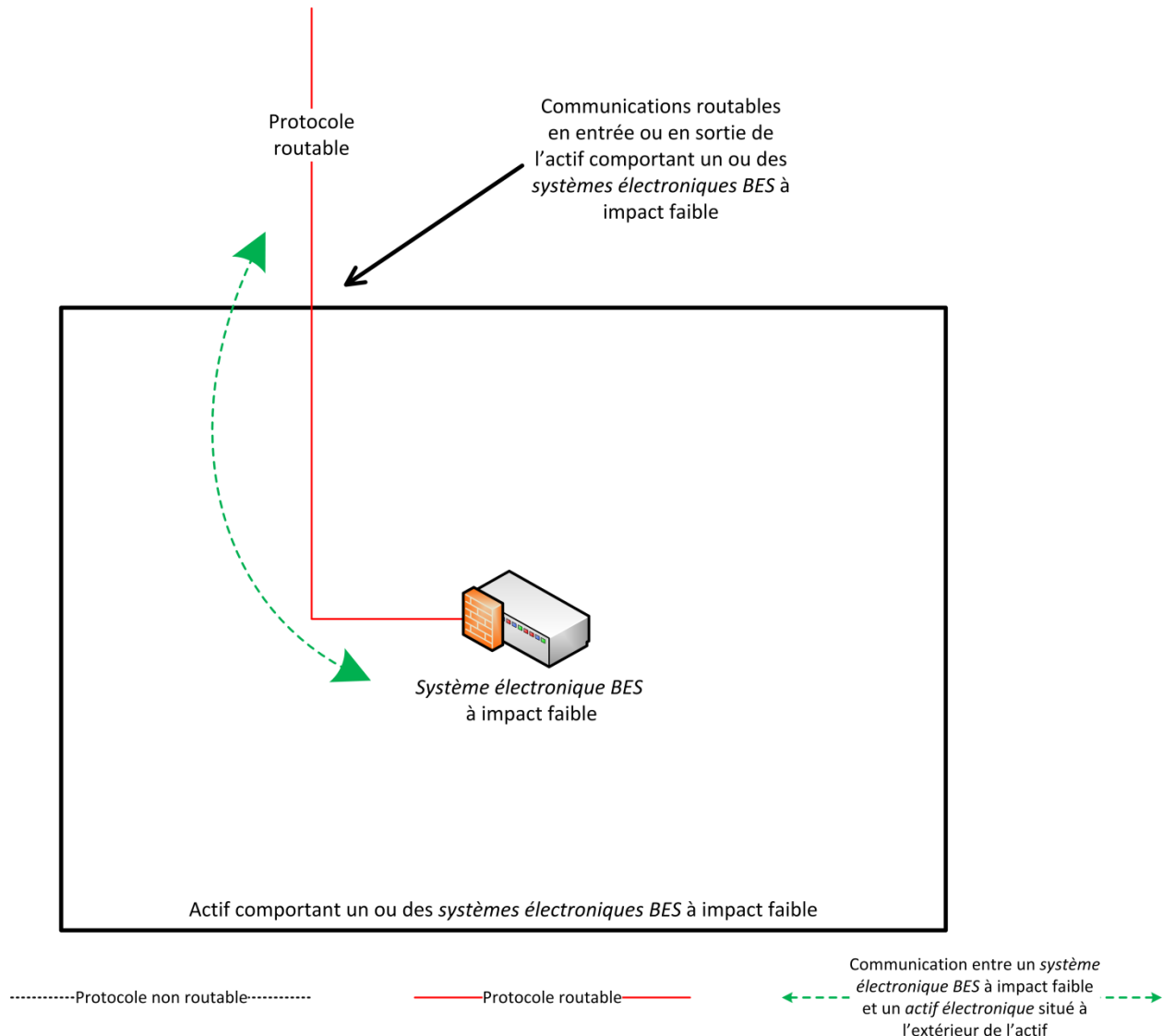
Les schémas des pages suivantes présentent des exemples conceptuels qui illustrent diverses situations de contrôle des accès électroniques. Quels que soient les concepts ou les configurations choisis par l'entité responsable, le but recherché est de réaliser l'objectif de sécurité suivant : autoriser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

REMARQUES :

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

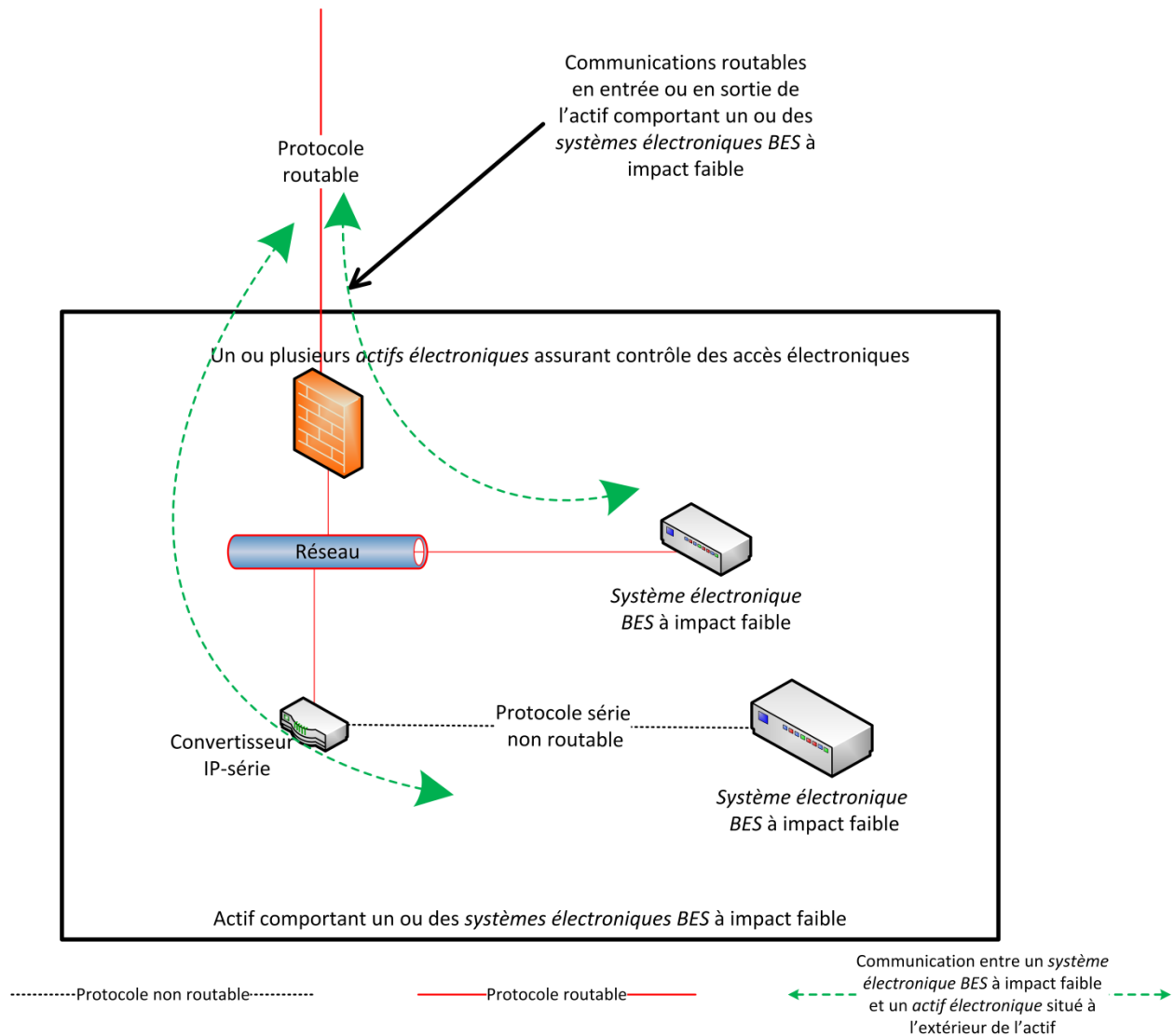
Modèle de référence 1 – Autorisations d'accès entrant et sortant sur hôte

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



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

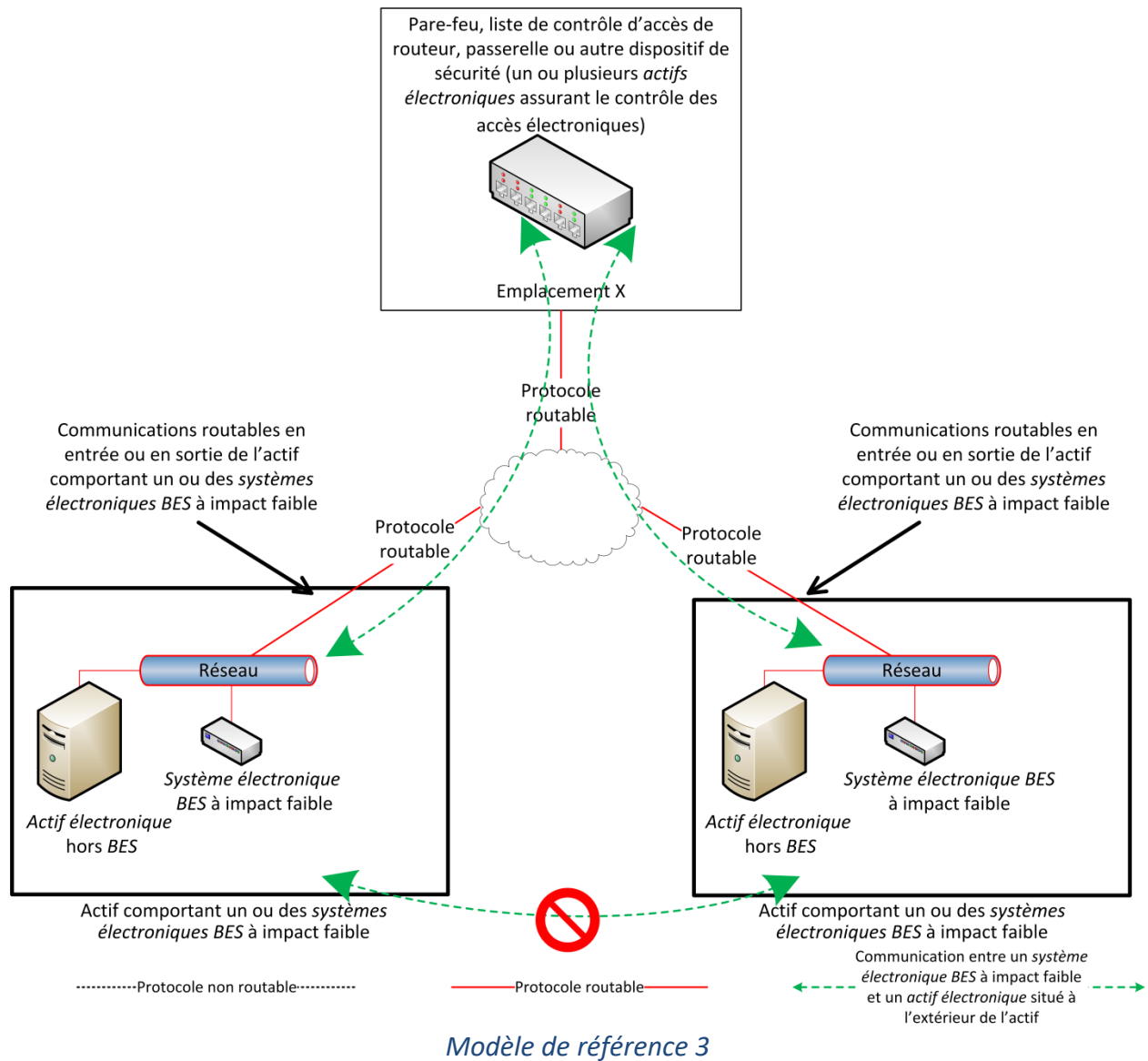
L'entité responsable peut opter pour un dispositif de sécurité qui autorise uniquement les accès électroniques entrants et sortants nécessaires pour le ou les *systèmes électroniques BES* à impact faible situés dans l'actif comportant ce ou ces *systèmes électroniques BES* à impact faible. Dans cet exemple, 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

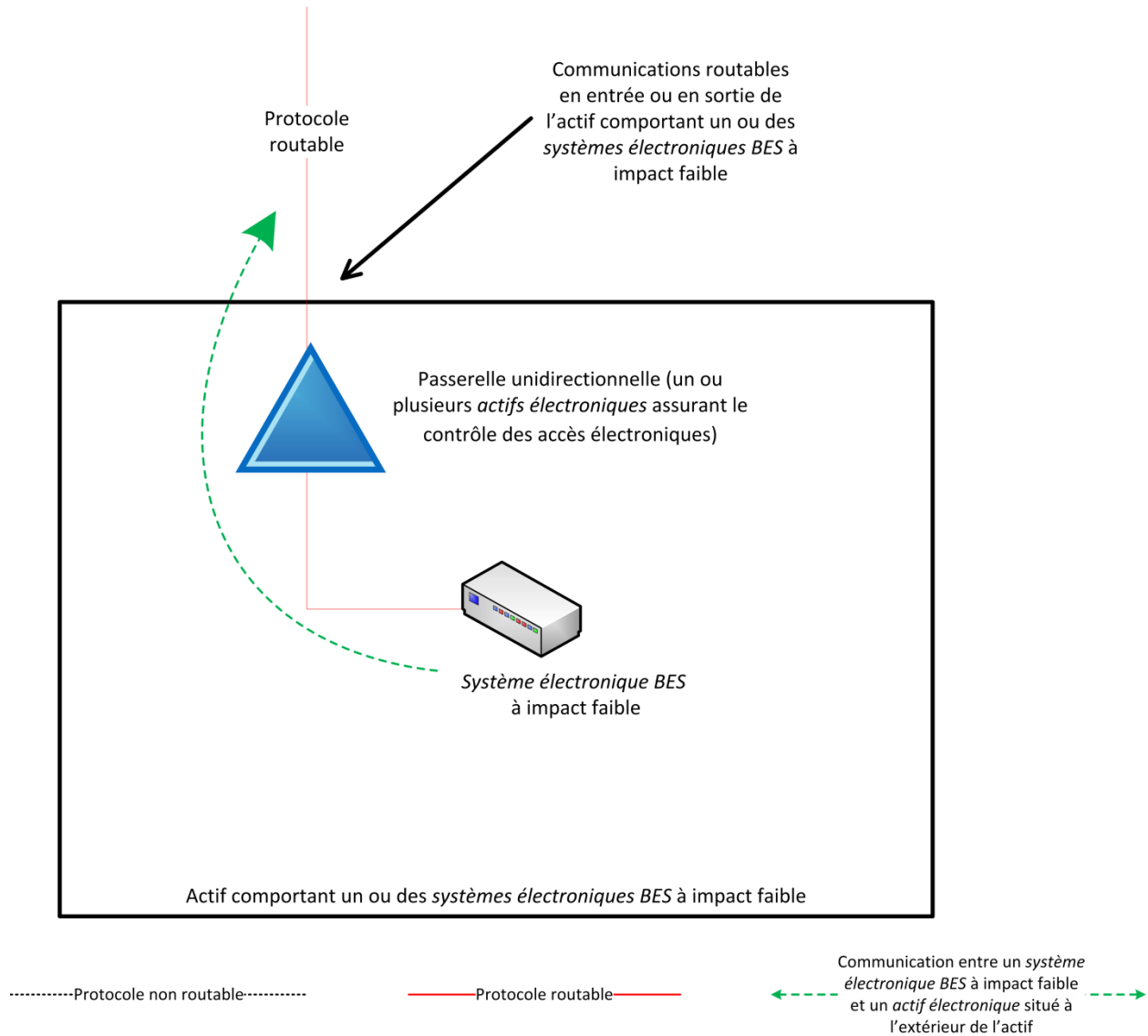
Modèle de référence 3 – Autorisations d'accès entrant et sortant par dispositif réseau centralisé

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 4 – Passerelle unidirectionnelle

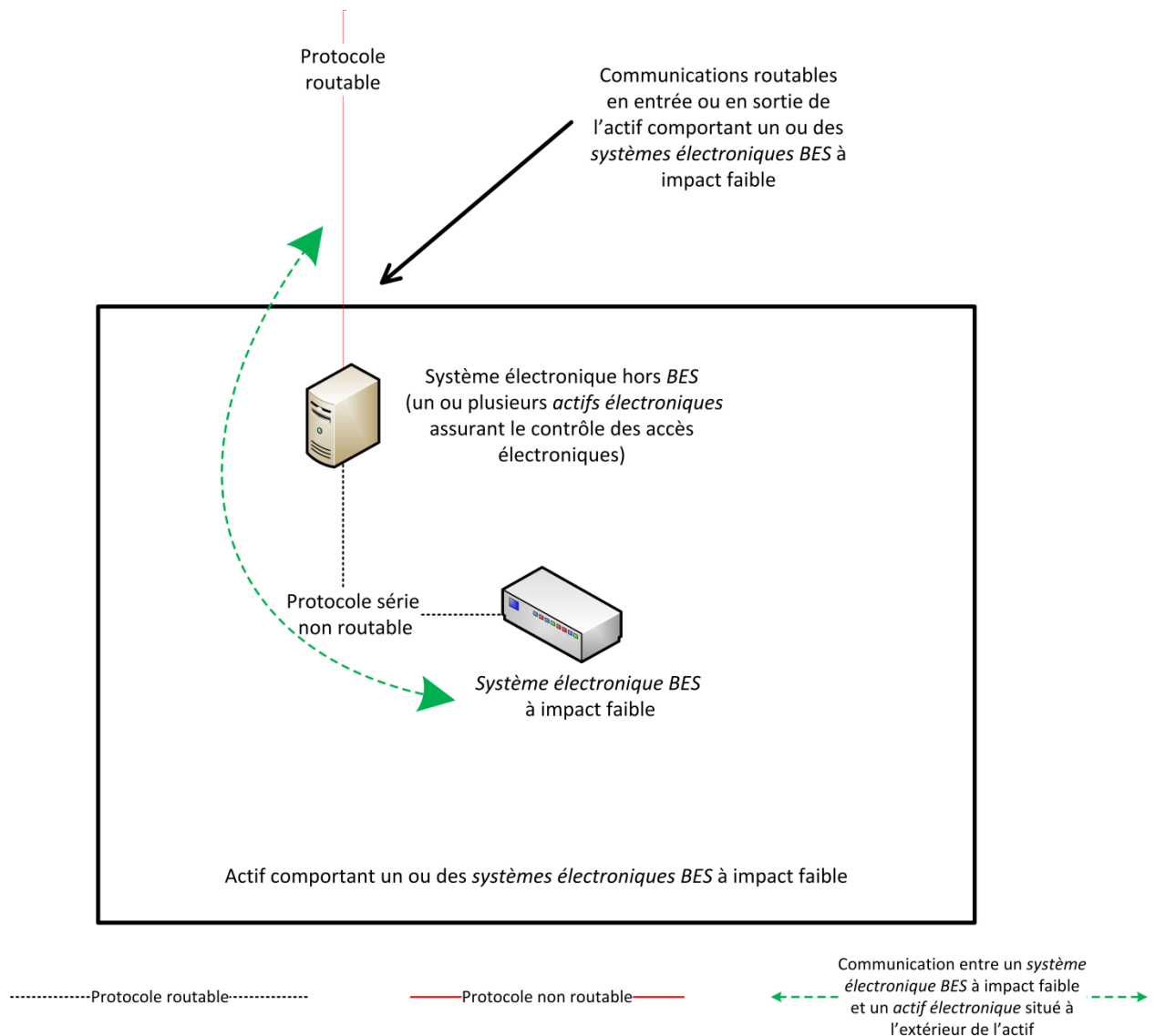
L'entité responsable peut choisir d'utiliser une passerelle unidirectionnelle pour le contrôle des accès électroniques. Le ou les *systèmes électroniques BES* à impact faible ne sont pas accessibles (les données ne peuvent pas les atteindre) au moyen de la communication par protocole routable en entrée 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.

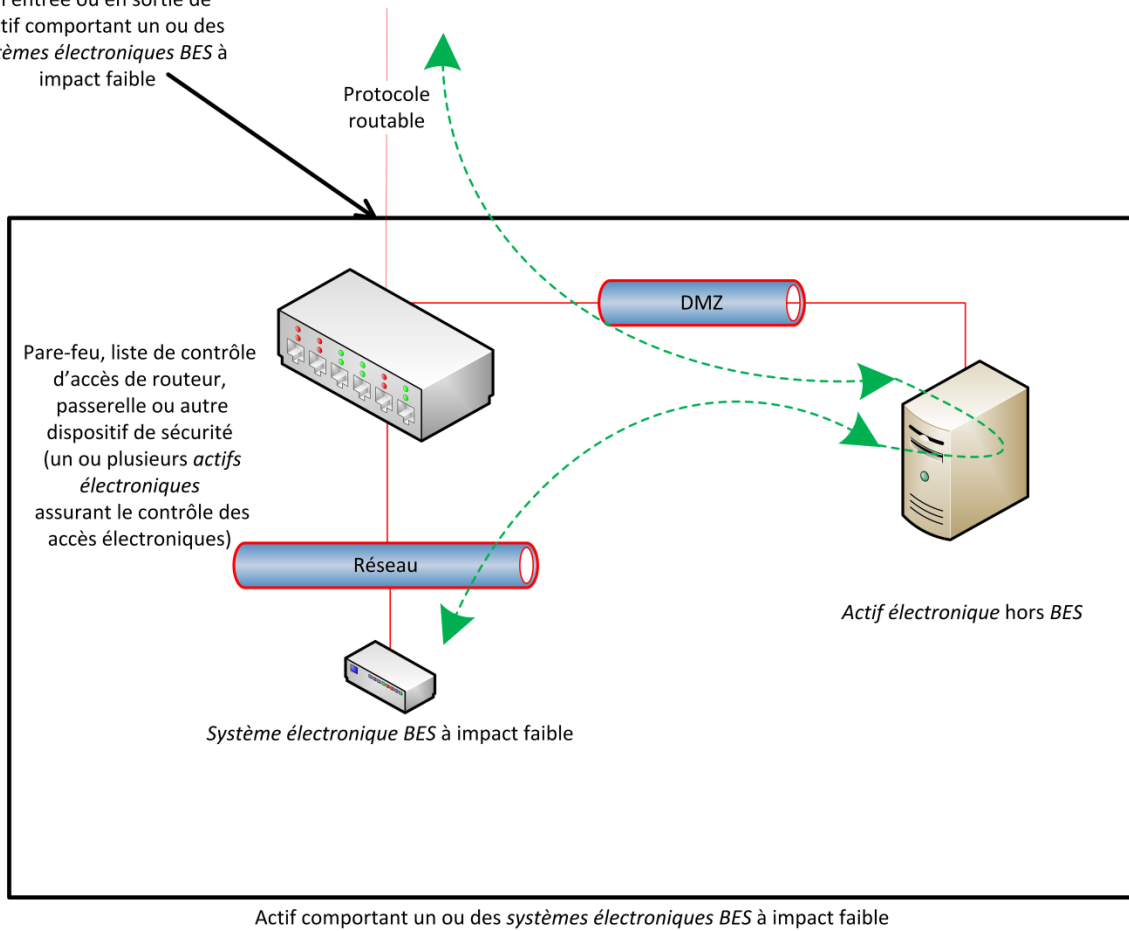


Modèle de référence 5

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.

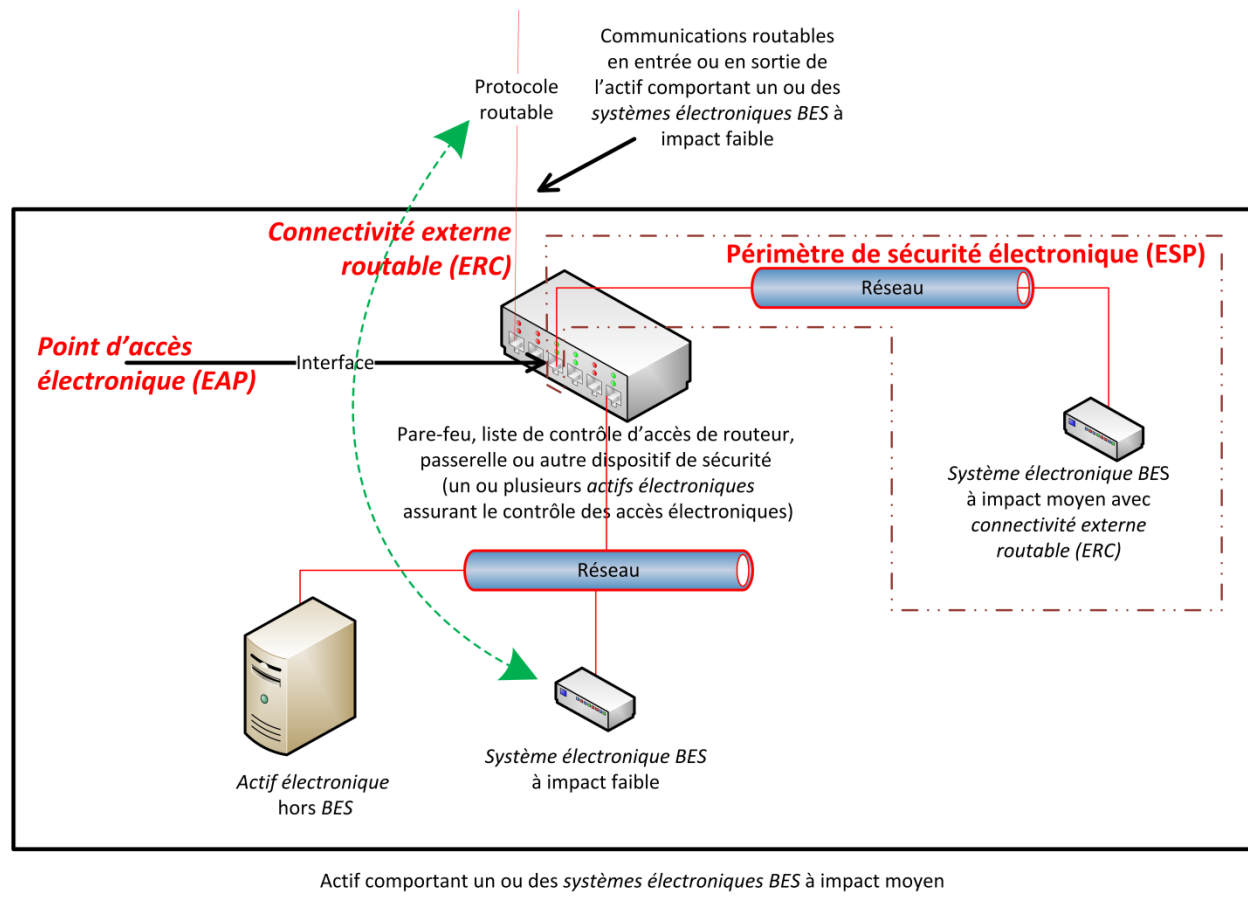
Communications routables en entrée ou en sortie de l'actif comportant un ou des *systèmes électroniques BES* à impact faible



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.

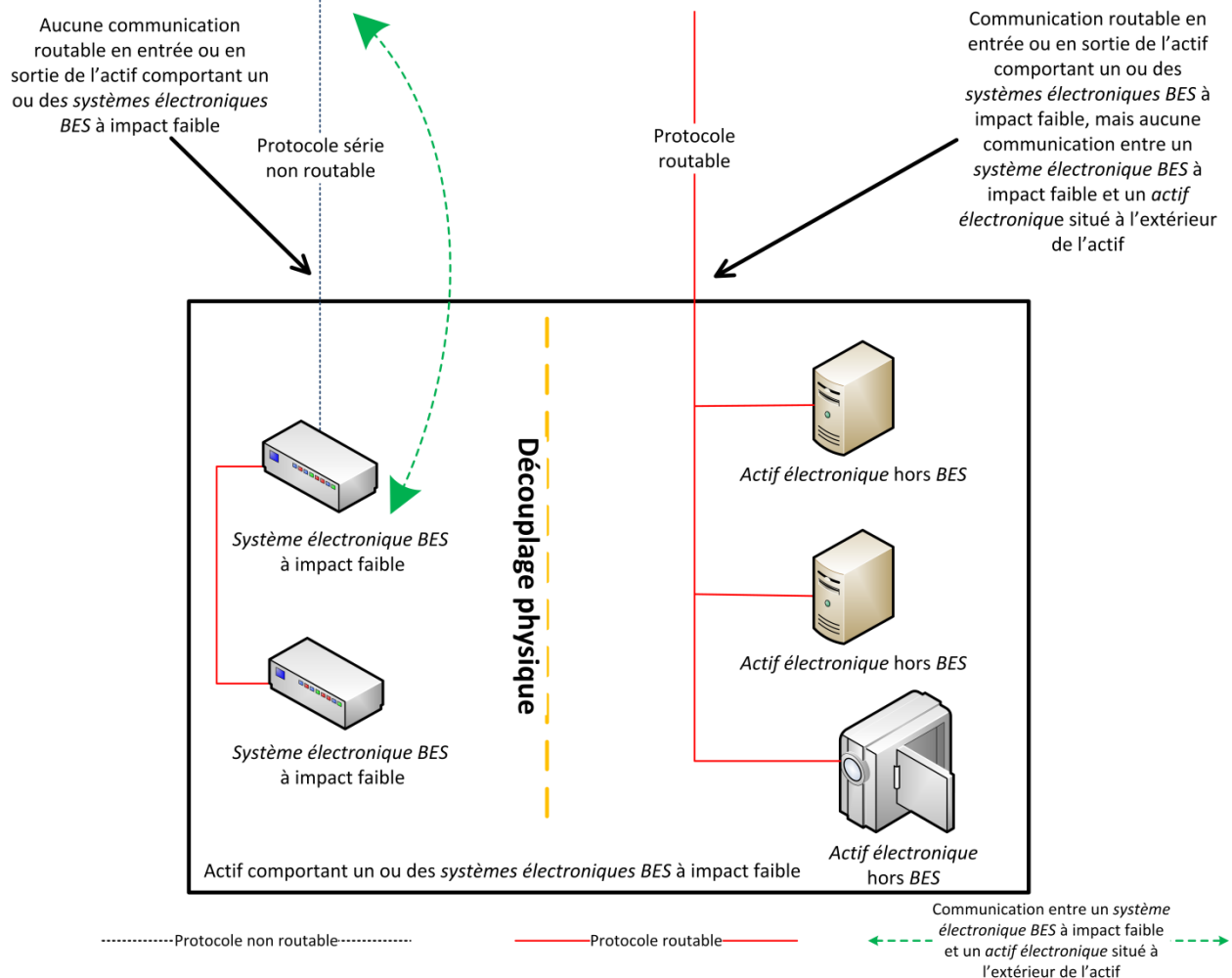


Modèle de référence 7

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 :

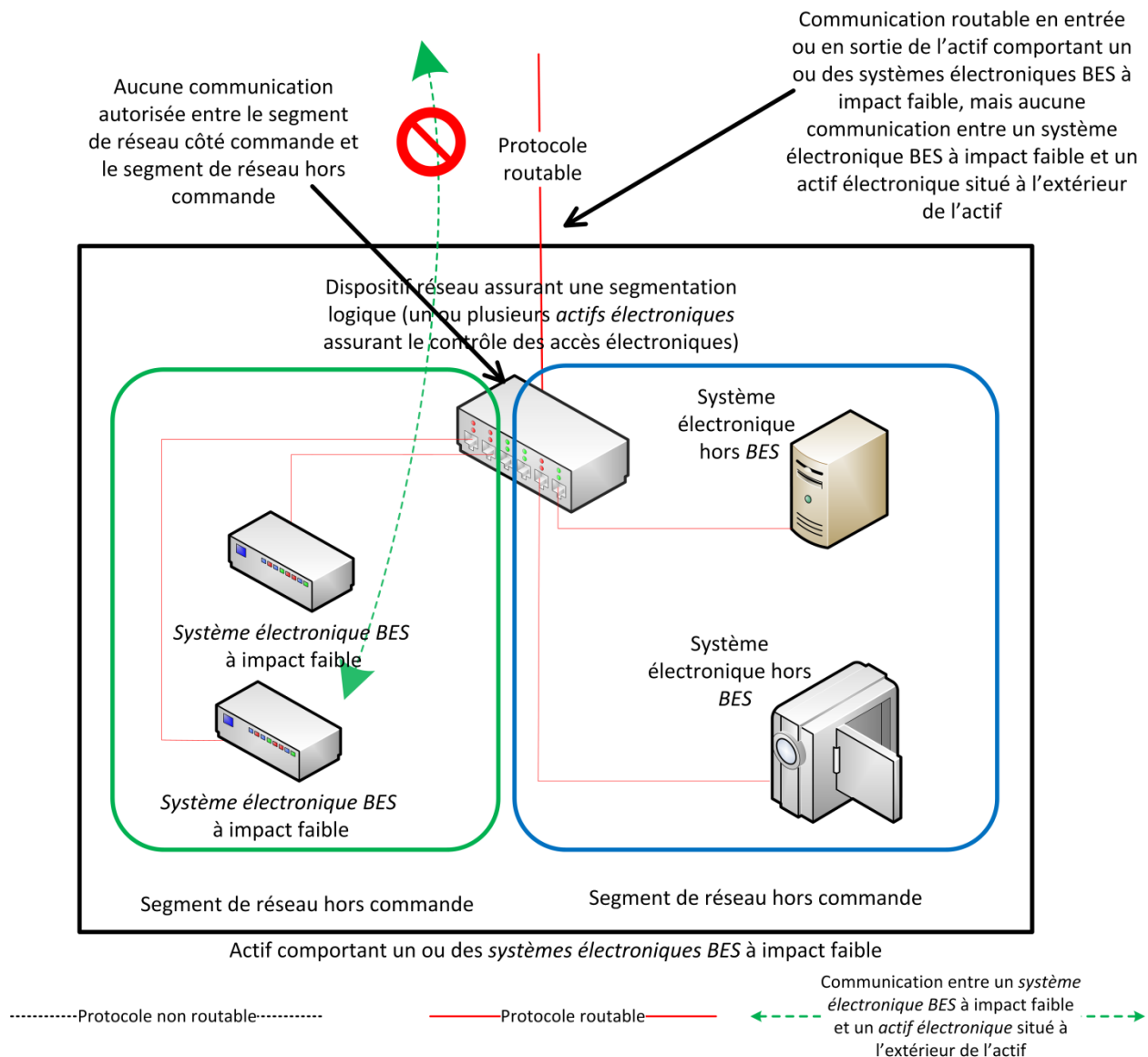
- 1) Étant donné le découplage physique (communément appelé « *air gap* » en anglais) du ou des *systèmes électroniques BES* à impact faible par rapport aux communications entrantes ou sortantes par protocole routable de l'actif comportant le ou les *systèmes électroniques BES* à impact faible, le contrôle 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

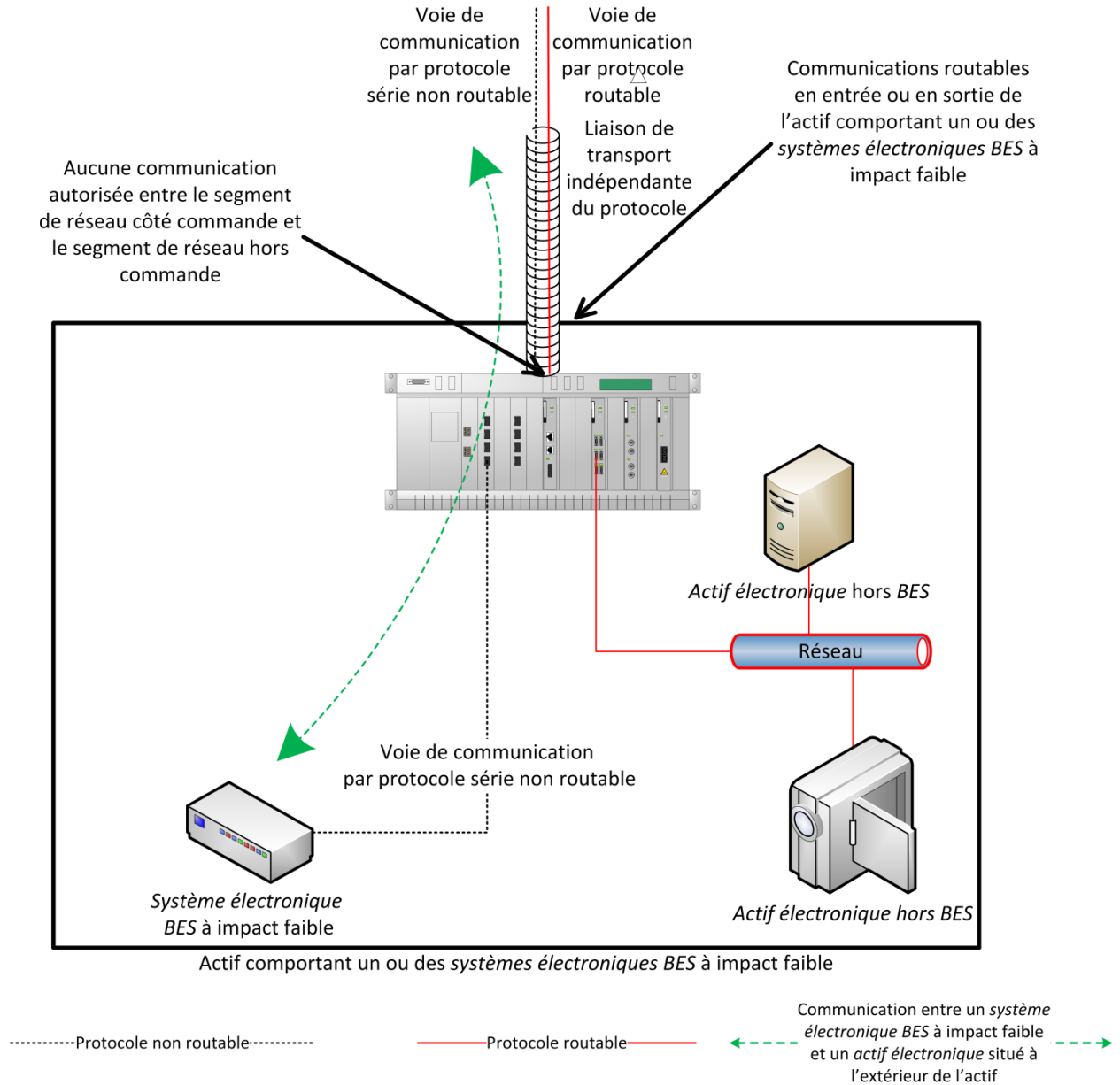
Dans ce modèle de référence, les critères de la section 3.1 de l'annexe 1 concernant l'obligation de contrôler les accès électroniques ne sont pas remplis. L'entité responsable a isolé logiquement le ou les *systèmes électroniques BES* à impact faible par rapport aux communications entrantes ou sortantes 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 2014¹). Ces clauses d'approvisionnement peuvent aider à harmoniser les actions de l'entité responsable et des tierces parties chargées du soutien des *systèmes électroniques BES* et des *actifs électroniques BES*. Les attributs du programme de protection des infrastructures essentielles (CIP), y compris les rôles et responsabilités, les contrôles d'accès, la surveillance, la journalisation, la gestion des vulnérabilités et celle des correctifs logiciels ainsi que les interventions en cas d'incident et la récupération des sauvegardes, peuvent faire partie des prestations confiées à une tierce partie. Les entités pourront s'inspirer des chapitres *General Cybersecurity Procurement Language* et *The Supplier's Life Cycle Security Program* du document précité pour la rédaction des ententes-cadres de services, des contrats et des processus et contrôles du programme CIP.

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

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

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

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

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

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

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

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

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

Exigence E3

L'esprit de l'exigence E3 de la norme CIP-003-8 reste pratiquement inchangé par rapport aux versions antérieures de la norme. La description spécifique du *cadre supérieur CIP* est maintenant comprise dans les termes définis, ce qui évite de l'expliquer dans le texte de la norme de fiabilité et de devoir créer des renvois à la norme dans d'autres documents. Le *cadre supérieur CIP* est appelé à jouer un rôle clé pour assurer la planification stratégique appropriée, la sensibilisation des dirigeants et du conseil d'administration ainsi que la gouvernance générale du programme.

Exigence E4

Comme l'indique la justification de l'exigence E4 de la norme CIP-003-8, cette exigence vise à démontrer une chaîne d'autorité et d'imputabilité claire en matière de sécurité. L'intention de l'équipe de rédaction (SDT) était de ne pas imposer une structure organisationnelle particulière ; elle laisse plutôt à l'entité responsable une ample marge de manœuvre pour adapter cette exigence à sa structure organisationnelle existante. Une entité responsable peut satisfaire à cette exigence au moyen d'un seul ou de plusieurs documents de délégation. L'entité responsable peut aussi déléguer les pouvoirs de délégation eux-mêmes pour augmenter la souplesse de mise en œuvre dans son organisation. Dans un tel cas, les délégations peuvent être dispersées dans de multiples documents, pourvu que l'ensemble de ces documents décrive une chaîne d'autorité claire qui remonte au *cadre supérieur CIP*. De plus, le *cadre supérieur CIP* pourrait aussi choisir de ne déléguer aucun pouvoir et de respecter cette exigence sans recourir à des documents de délégation.

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

Justification

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

Justification de l'exigence E1

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

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

Justification de l'exigence E2

En réponse à l'ordonnance 791 de la FERC, l'exigence E2 demande aux entités d'élaborer et de mettre en œuvre des plans de cybersécurité afin d'atteindre des objectifs précis en matière de mécanismes de sécurité pour leurs actifs comportant un ou des *systèmes électroniques BES* à impact faible. Les plans de cybersécurité couvrent cinq thèmes : 1) la sensibilisation à la cybersécurité ; 2) les mesures de sécurité physique ; 3) le contrôle des accès électroniques ; 4) l'intervention en cas d'*incident de cybersécurité* ; et 5) l'atténuation des risques liés à l'introduction de programmes malveillants à partir d'*actifs électroniques temporaires* ou de *supports de stockage amovibles*. Ces plans, combinés aux politiques de cybersécurité spécifiées à l'alinéa 1.2 de l'exigence E1, présentent un cadre pour la mise en place de mesures opérationnelles, administratives et techniques visant les *systèmes électroniques BES* à impact faible.

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

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

Justification des modifications aux sections 2 et 3 de l'annexe 1 (exigence E2) :

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

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

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

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

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

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

L'exigence E2 demande aux entités d'élaborer et de mettre en œuvre un ou des plans de cybersécurité afin de réaliser des objectifs de sécurité précis pour leurs actifs comportant un ou des *systèmes électroniques BES* à impact faible. Au paragraphe 32 de son ordonnance 822, la FERC demande à la NERC de « ...rendre obligatoires des mesures de protection visant les actifs temporaires utilisés avec les *systèmes électroniques BES* à impact faible, d'après le risque pour la fiabilité du *système de production-transport d'électricité* ». Les actifs temporaires sont des vecteurs potentiels d'introduction de programmes malveillants dans les *systèmes électroniques BES* à impact faible. La section 5 de l'annexe 1 vise à combattre le risque de contamination du *BES* par des maliciels propagés par l'entremise de *systèmes électroniques BES* à impact faible, en demandant aux entités d'élaborer et de mettre en œuvre un ou des plans à cette fin. Ces plans de cybersécurité, combinés aux politiques de cybersécurité spécifiées à l'alinéa 1.2 de l'exigence E1, présentent un cadre pour la mise en place de mesures opérationnelles, administratives et techniques visant les *systèmes électroniques BES* à impact faible.

Justification de l'exigence E3

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

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

Justification de l'exigence E4

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

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

Annexe CIP-003-8-QC-1
Dispositions particulières applicables au Québec visant la norme
CIP-003-8 — Cybersécurité — Mécanismes de gestion de la sécurité

La présente annexe établit les dispositions particulières d'application au Québec de la norme qu'elle vise. Les dispositions de la norme visée et de l'annexe doivent obligatoirement être lues conjointement pour fins de compréhension et d'interprétation. En cas de divergence entre la norme visée et l'annexe, l'annexe a préséance.

A. Introduction

- 1. Titre :** Aucune disposition particulière
- 2. Numéro :** Aucune disposition particulière
- 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 : 10 septembre 2020
- 5.2.** Adoption de l'annexe par la Régie de l'énergie : 10 septembre 2020
- 5.3.** Date d'entrée en vigueur de la norme et de l'annexe au Québec : 1^{er} octobre 2021

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

Annexe CIP-003-8-QC-1
Dispositions particulières applicables au Québec visant la norme
CIP-003-8 — Cybersécurité — Mécanismes de gestion de la sécurité

Au Québec, le terme *responsable des mesures pour assurer la conformité* désigne la Régie de l'énergie dans le rôle visant à surveiller la conformité à la norme de fiabilité visée et à la présente annexe, et à assurer l'application de celles-ci.

1.2. Conservation des pièces justificatives

Aucune disposition particulière

1.3. Processus de surveillance de la conformité et d'application des normes

La Régie de l'énergie établit les processus de surveillance qui servent à évaluer les données ou l'information afin de déterminer la conformité ou la non-conformité avec la norme de fiabilité visée et avec la présente annexe.

1.4. Autres informations sur la conformité

Aucune disposition particulière

2. Niveau de gravité de la non-conformité (VSL)

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

Historique des révisions

Version	Date	Intervention	Suivi des modifications
1	10 septembre 2020	Nouvelle annexe.	Nouvelle
2	16 octobre 2020	Améliorations de forme	Révision