Normes de fiabilité de la NERC
en suivi des modifications

A. Introduction

1. Titre : Cybersécurité — Catégorisation des systèmes électroniques BES

2. Numéro : CIP-002-5.1a

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

4. Applicabilité :

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

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

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

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

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

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

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

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

4.1.2.4. Chaque *chemin de démarrage* et groupe d'*éléments* respectant les exigences relatives aux manœuvres initiales depuis une *ressource à démarrage autonome* jusqu'au premier point de raccordement,

inclusivement, d'alimentation des services auxiliaires du ou des prochains groupes de production à démarrer.

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

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

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

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

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

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

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

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

4.2.1.1. Chaque système ~~de~~ DSF ou ~~de~~ DST qui :

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

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

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

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

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

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

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

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

4.2.3.2. les *actifs électroniques* associés aux réseaux de communication et aux liaisons d'échange de données entre des *périmètres de sécurité* ~~*électroniques*~~*électronique* distincts ;

4.2.3.3. les systèmes, structures et ~~composantes~~composants régis par la U.S. Nuclear Regulatory Commission en vertu d'un plan de cybersécurité ~~conforme à la norme~~, conformément au règlement CFR 10, section~~-~~ 73.54 ;

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

5. Dates d'entrée en vigueur :

1. **24 mois minimum** – La norme~~-~~ CIP-002-5.~~1~~1a entrera en vigueur soit le 1er juillet 2015, soit le premier jour civil du neuvième trimestre civil suivant l'entrée en vigueur de l'ordonnance d'approbation réglementaire appropriée, selon le délai le plus long.

2. Dans les ~~juridictions~~territoires où aucune approbation réglementaire n'est requise, la norme~~-~~ CIP-002-5.~~1~~1a entrera en vigueur le premier jour du neuvième trimestre civil suivant l'approbation par le Conseil d'administration, ou selon les modalités d'approbation prévues par la loi pour les organismes gouvernementaux chargés de la fiabilité électrique (ERO).

6. Contexte :

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

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

Plusieurs références de la section Applicabilité et les critères de l'annexe~~-~~ 1 de la norme~~-~~ CIP-002 utilisent un seuil de 300 MW pour les systèmes DSF et DST. Ce seuil particulier de 300 MW pour les systèmes DSF et DST provient de la version 1 des normes CIP sur la cybersécurité. Ce seuil demeure à 300 MW puisqu'il concerne spécifiquement les systèmes DST et DSF, qui constituent des efforts de dernier recours

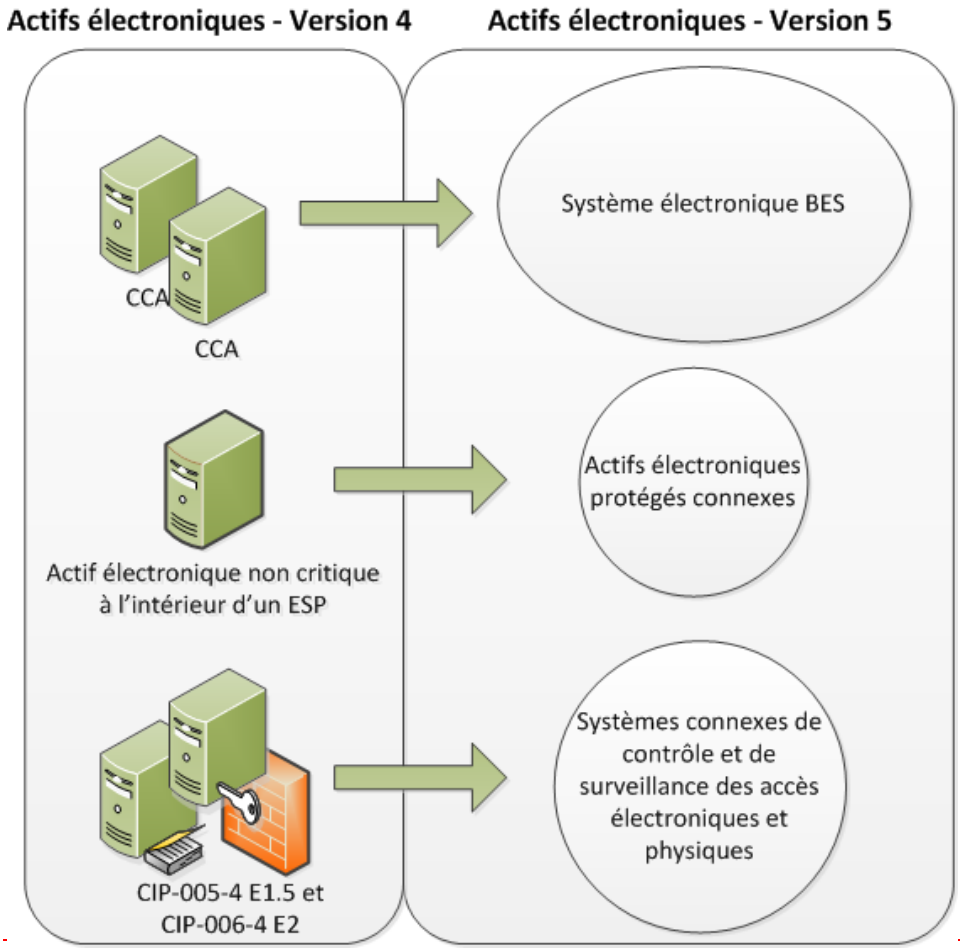
pour sauver le *système de production-transport d'électricité*. Un examen des tolérances ~~de~~des systèmes DSF définies dans les normes de fiabilité régionales pour les exigences des programmes ~~de~~ DSF à ce jour indique que la valeur historique de 300 MW représente une valeur de seuil adéquate et raisonnable pour les tolérances d'exploitation admissibles des systèmes DSF.

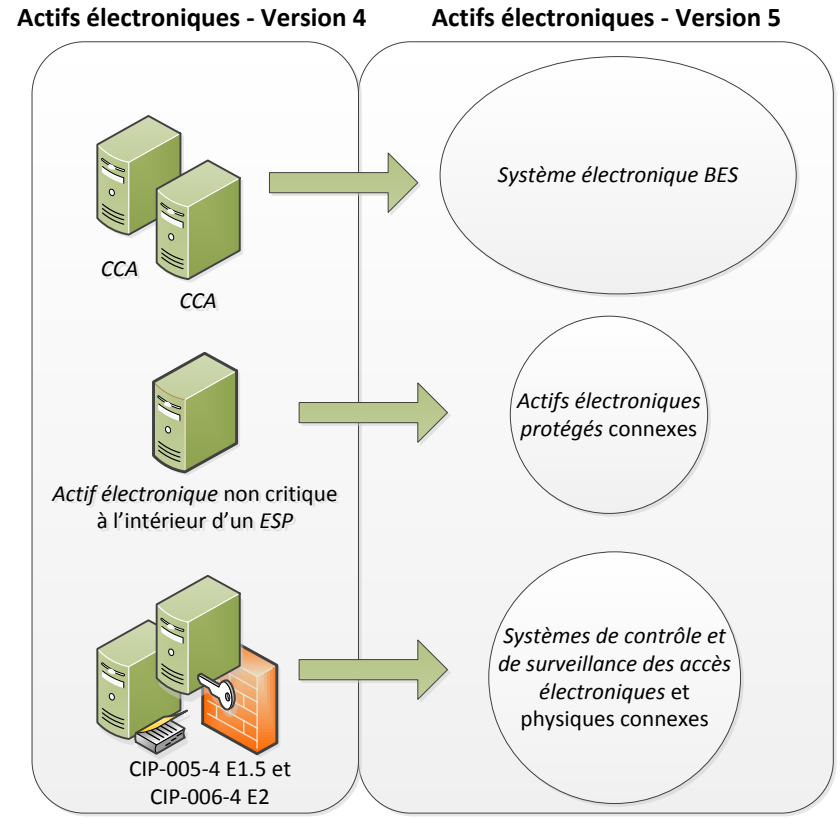
Systèmes électroniques BES

Mis en fo

Mis en fo
0,55", Par

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





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

Une autre raison d'utiliser le terme « *système électronique BES* » est de fournir un niveau pratique auquel une entité responsable peut organiser la mise en œuvre documentée des exigences et des pièces justificatives de conformité. Les entités responsables peuvent utiliser le concept bien développé de plan de sécurité pour chaque *système électronique BES* afin de documenter les programmes, processus et plans en place visant à se conformer aux exigences de sécurité.

Il est laissé à la discrétion de l'entité responsable de déterminer le niveau de granularité pour délimiter un *système électronique BES*, compte tenu des ~~conditions~~éléments de la définition de *système électronique BES*. Par exemple, l'entité responsable pourrait choisir de considérer l'ensemble d'un système de commande de

centrale comme un seul *système électronique BES*, ou choisir de considérer certaines parties de ce système comme des *systèmes électroniques BES* distincts. L'entité responsable devrait prendre en considération le contexte opérationnel et le cadre de gestion lorsqu'elle définit les limites d'un *système électronique BES*, de manière à maximiser l'efficience de son fonctionnement sécurisé. Définir des limites trop étroites pourrait entraîner des redondances dans les processus administratifs et les autorisations, tandis que définir des limites trop larges pourrait rendre le fonctionnement sécurisé du *système électronique BES* difficile à surveiller et à évaluer.

Exploitation fiable du *BES*

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

Exploitation en temps réel

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

Critères de catégorisation

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

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

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

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

- ***Systèmes de contrôle ou de surveillance des accès électroniques* (*EACMS*)** – Exemples : *points d'accès électroniques*, *systèmes intermédiaires*, serveurs d'authentification (serveurs Radius, serveurs Active Directory, autorités de certification, etc.), systèmes de surveillance des événements de sécurité et systèmes de détection des intrusions.
- ***Systèmes de contrôle des accès physiques* (*PACS*)** – Exemples : serveurs d'authentification et systèmes d'accès à carte ou à porte-nom.
- ***Actifs électroniques protégés* (*PCA*)** – Exemples, dans la mesure où ils se trouvent à l'intérieur de l'ESP : serveurs de fichiers, serveurs FTP, serveurs de temps, commutateurs ~~LAN~~de réseau local, imprimantes réseau, enregistreurs numériques de défauts et systèmes de surveillance des émissions.

B. Exigences et mesures

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

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

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

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

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

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

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

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

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

M2. Les pièces justificatives acceptables comprennent, ~~mais~~ sans s'y limiter, des documents électroniques ou papier datés ~~pour démontrer~~attestant que l'entité responsable a passé en revue et mis à jour, lorsque nécessaire, les identifications exigées selon l'exigence- E1 et ses alinéas, et qu'elle a fait approuver par son *cadre supérieur CIP* ou son délégué les ~~identifications exigées~~répertoires établis selon l'exigence- E1 et ses alinéas au moins une fois tous les 15- mois civils, même si aucun élément n'a été ~~identifié~~répertorié selon l'exigence- E1 et ses alinéas, conformément à l'exigence- E2.

C. Conformité

1. Processus de surveillance de la conformité

1.1. Responsable des mesures pour assurer la conformité

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

Mis en fo
Mis en fo
Mis en fo
Mis en fo
Mis en fo
Mis en fo

1.2. Conservation des pièces justificatives

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

Mis en fo

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

Mis en fo

- 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.

Mis en fo

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

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

1.4. Autres informations sur la conformité

- ~~Aucun~~

- Aucune

2. Tableau des éléments de conformité

~~E#E~~x.	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-002-5.1)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
E1	**Planification de l'exploitation**	**Élevé**	Pour les entités responsables qui ont plus de 40- actifs *BES* au total à l'exigence- E1, ~~cinq pour cent~~5 % ou moins des actifs *BES* n'ont pas été ~~considérés conformément à~~examinés selon l'exigence- E1~~;~~. OU Pour les entités responsables qui ont 40- actifs *BES* au total ou moins, ~~2~~ deux actifs *BES* ou moins à l'exigence- E1 n'ont pas été ~~considérés conformément à~~examinés selon l'exigence- E1~~;~~. OU Pour les entités responsables qui ont	Pour les entités responsables qui ont plus de 40- actifs *BES* au total à l'exigence- E1, plus de ~~cinq pour cent,~~5 %, mais au plus 10~~ pour cent~~ % des actifs *BES* n'ont pas été ~~considérés conformément à~~examinés selon l'exigence- E1~~;~~. OU Pour les entités responsables qui ont 40- actifs *BES* au total ou moins, plus de deux, mais au plus quatre actifs *BES* à l'exigence- E1 n'ont pas été ~~considérés conformément à~~examinés selon l'exigence- E1~~;~~.	Pour les entités responsables qui ont plus de 40- actifs *BES* au total à l'exigence- E1, plus de 10~~ pour cent,~~ %, mais au plus 15~~ pour cent~~ % des actifs *BES* n'ont pas été ~~considérés conformément à~~examinés selon l'exigence- E1~~;~~. OU Pour les entités responsables qui ont 40- actifs *BES* au total ou moins, plus de quatre, mais au plus six actifs *BES* à l'exigence- E1 n'ont pas été ~~considérés conformément à~~examinés selon l'exigence- E1~~;~~. OU	Pour les entités responsables qui ont plus de 40- actifs *BES* au total à l'exigence- E1, plus de 15~~ pour cent~~ % des actifs *BES* n'ont pas été ~~considérés conformément à~~examinés selon l'exigence- E1~~;~~. OU Pour les entités responsables qui ont 40- actifs *BES* au total ou moins, plus de six actifs *BES* à l'exigence- E1 n'ont pas été ~~considérés conformément à~~examinés selon l'exigence- E1~~;~~. OU Pour les entités responsables qui ont

Mis en fo
Mis en fo
Mis en fo
Mis en fo
Mis en fo
Mis en fo
Mis en fo
Mis en fo
Mis en fo
Mis en fo
Mis en fo
Mis en fo
Mis en fo
Mis en fo

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

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

~~E#E~~x.	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-002-5.1)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
			ou moyen ou moins n'ont pas été ~~identifiés~~répertoriés.	100- *systèmes électroniques BES* ~~d'impact~~à impact élevé ou moyen ou moins au total, plus de cinq, mais au plus 10- *systèmes électroniques BES* ~~d'impact~~à impact élevé ou moyen ou moins n'ont pas été ~~identifiés~~répertoriés.	~~d'impact~~à impact élevé ou moyen ou moins au total, plus de 10, mais au plus 15- *systèmes électroniques BES* ~~d'impact~~à impact élevé ou moyen ou moins n'ont pas été ~~identifiés~~répertoriés.	*électroniques BES* ~~d'impact~~à impact élevé ou moyen ~~ou moins~~ n'ont pas été ~~identifiés~~répertoriés.
E2	**Planification de l'exploitation**	**Faible**	L'entité responsable n'a pas ~~complété~~effectué son passage en revue et sa mise à jour ~~pour l'identification exigée en~~ des répertoires établis selon E1 ~~à l'intérieur de~~dans les 15- mois civils, mais ~~en~~l'a fait au plus dans les 16- mois civils, du passage en revue précédent. (E2.1) OU	L'entité responsable n'a pas ~~complété~~effectué son passage en revue et sa mise à jour ~~pour l'identification exigée en~~ des répertoires établis selon E1 ~~à l'intérieur de~~dans les 16- mois civils, mais ~~en~~l'a fait au plus dans les 17- mois civils, du passage en revue précédent. (E2.1) OU	L'entité responsable n'a pas ~~complété~~effectué son passage en revue et sa mise à jour ~~pour l'identification exigée en~~ des répertoires établis selon E1 ~~à l'intérieur de~~dans les 17- mois civils, mais ~~en~~l'a fait au plus dans les 18- mois civils, du passage en revue précédent. (E2.1) OU	L'entité responsable n'a pas ~~complété~~effectué son passage en revue et sa mise à jour ~~pour l'identification exigée en~~ des répertoires établis selon E1 ~~à l'intérieur de~~dans les 18- mois civils du passage en revue précédent. (E2.1) OU L'entité responsable n'a pas ~~complété son~~

~~E#E~~ x.	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-002-5.1)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
			L'entité responsable n'a pas ~~complété son approbation des identifications exigées en~~ obtenu l'approbation des répertoires établis selon E1 par le *cadre supérieur CIP* ou son délégué conformément à l'exigence- E2 ~~à l'intérieur de~~dans les 15- mois civils, mais ~~en~~l'a fait au plus dans les 16- mois civils de l'approbation précédente. (E2.2)	L'entité responsable n'a pas ~~complété son approbation des identifications exigées en~~ obtenu l'approbation des répertoires établis selon E1 par le *cadre supérieur CIP* ou son délégué conformément à l'exigence- E2 ~~à l'intérieur de~~dans les 16- mois civils, mais l'a fait en au plus dans les 17- mois civils de l'approbation précédente. (E2.2)	L'entité responsable n'a pas ~~complété son approbation des identifications exigées en~~ obtenu l'approbation des répertoires établis selon E1 par le *cadre supérieur CIP* ou son délégué conformément à l'exigence- E2 ~~à l'intérieur de~~dans les 17- mois civils, mais l'a fait en au plus dans les 18- mois civils de l'approbation précédente. (E2.2)	~~approbation des identifications exigées en~~ obtenu l'approbation des répertoires établis selon E1 par le *cadre supérieur CIP* ou son délégué conformément à l'exigence- E2 ~~à l'intérieur de~~dans les 18- mois civils de l'approbation précédente. (E2.2)

D. Différences régionales

Aucune.

E. Interprétations

Aucune.

F. Documents connexes

Aucun.

Mis en fo
Non Gras

Mis en fo

CIP-~~-~~002-~~-~~5.~~1~~1a – Annexe-~~ ~~1

Mis en fo

Critères de degré d'impact

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

1. Impact élevé (H)

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

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

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

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

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

2. Impact moyen (M)

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

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

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

Mis en fo

Mis en fo

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

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

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

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

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

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

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

2.8. *Installations* de *transport*, y compris les *installations* de raccordement de la production, qui fournissent le raccordement de la production nécessaire pour

raccorder la sortie du groupe de production aux *réseaux* de *transport* et qui, si elles étaient détruites, ~~endommagées~~dégradées, mal utilisées ou autrement rendues indisponibles, entraîneraient la perte d'*installations* de production ~~identifiées~~répertoriées par un *propriétaire d'installation de production* en vertu du critère 2.1 ou 2.3 de l'annexe 1.

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

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

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

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

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

3. Impact faible (L)

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

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

3.2. ~~Postes~~postes de transport ;

Mis en fo
Non Gras

3.3. ~~Ressources~~ressources de production ;

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

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

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

Principes directeurs et fondements techniques

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

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

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

La section ~~«~~ 4.2~~-~~. Installations~~»~~ définit la portée des *installations*, systèmes et équipements détenus par l'entité responsable ~~qualifié~~désignée à la section~~-~~ 4.1~~,~~., qui est visée par les exigences de la norme. Outre l'ensemble des *installations* du *BES*, des *centres de contrôle* et des autres systèmes et équipements, la liste comprend l'ensemble des systèmes et équipements visés détenus par les *distributeurs*. Bien que le terme « *installations* » ~~du~~dans le glossaire de la NERC comprenne déjà la caractéristique *BES*, l'utilisation additionnelle du terme « *BES* » vise ici à renforcer la portée d'applicabilité pour ces *installations*, en particulier dans cette section sur l'applicabilité. Cela établit quels sont les *installations*, systèmes et équipements visés par les normes. Cette section est particulièrement importante dans la norme CIP~~-~~-002~~-~~-5.~~1~~1a et délimite l'ensemble des *installations*, systèmes et équipements auxquels s'appliquent les critères de l'annexe~~-~~ 1. C'est important, car cela détermine les *installations*, systèmes et équipements qui sont classés dans la catégorie Impact faible, après filtrage de ceux qui répondent aux critères des catégories Impact élevé et Impact moyen.

Dans le but ~~d'identifier~~de répertorier les groupes d'*installations*, de systèmes et d'équipements (par leur emplacement ou autrement), l'entité responsable ~~identifie~~examine les actifs de la façon décrite à l'exigence E1 de la norme CIP-002-5.~~1. Ceci est une~~1a. Il s'agit d'une démarche familière pour les entités responsables qui ont à se conformer aux versions 1, 2, 3 et 4 des normes CIP pour les *actifs critiques*. Comme dans les versions 1, 2, 3 et 4, les entités responsables peuvent utiliser des postes, des centrales et des *centres de contrôle* ~~à des emplacements uniques~~dans un même emplacement pour désigner ces groupes d'*installations*, de systèmes et d'équipements.

CIP-002-5.~~1~~1a

La norme CIP-002-5.~~1~~1a stipule que les entités responsables ~~concernées~~visées doivent catégoriser leurs *systèmes électroniques BES* et les *actifs électroniques BES* connexes selon les critères de l'annexe 1. Un *actif électronique BES* inclut dans sa définition~~,~~ : « s'il était ~~rendu~~

~~indisponible,~~ endommagé, ~~ou~~ mal utilisé ~~, aurait~~ou rendu indisponible entraînerait, dans les 15 minutes~~.~~ […] un impact négatif sur […] l'exploitation fiable du *BES* ».

Ce qui suit donne des indications qu'une entité responsable peut utiliser pour ~~identifier~~désigner les *systèmes électroniques BES* qui seraient ~~dans la portée.~~visés. Le concept de ~~fonction~~service de fiabilité du *BES* est utile à cet égard, car il offre à l'entité responsable une méthode définie pour déterminer les *systèmes électroniques BES* auxquels s'applique la norme CIP-002-5.~~1~~1a. Ce concept établit une liste de ~~fonctions~~services de fiabilité du *BES*. Ces ~~fonctions~~services comprennent :

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

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

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

Coordination entre les entités	X	X	X	X		X	X

Réponse dynamique

~~La fonction~~Le service de réponse dynamique comprend les actions effectuées par des *éléments* ~~BES~~ ou des sous-systèmes du *BES* qui sont lancés automatiquement pour amorcer une réponse à une condition du *BES*. Ces actions sont lancées par un seul élément~~, un~~ ou dispositif de commande~~,~~ ou par une combinaison de ~~ces~~tels éléments ou dispositifs agissant de concert pour effectuer une action ou pour engendrer une condition en réponse à l'action ou à la condition initiale. Les types de réponses dynamiques qui peuvent être considérés comme ayant un impact potentiel sur le *BES* sont les suivants :

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

Équilibre production-charge

~~La fonction~~Le service d'équilibre production-charge comprend les activités, actions et conditions nécessaires pour surveiller et ~~contrôler~~régler la production et la charge dans

Mis en fo

Mis en fo

Mis en fo

Mis en fo

l'horizon de planification de l'exploitation et en temps réel. Les aspects de la fonction d'équilibre production-charge comprennent ce qui suit, mais n'y sont pas limités :

- Calcul de l'*écart de réglage de la zone* (*ACE*)
  - Sources de données sur le terrain (transits d'interconnexion en temps réel, sources de fréquence, écart de temps, etc.) (TO et TOP)
  - Logiciels utilisés pour effectuer les calculs (BA)
- ~~Réponse à~~Gestion de la demande
  - Capacité de détecter les besoins de modulation de la charge (BA)
  - Capacité de moduler la charge (TOP et DP)
- Délestages de *charge* commandés manuellement
  - Capacité de détecter les besoins de modulation de la charge (BA)
  - Capacité de moduler la charge (TOP et DP)
- Réserve arrêtée (réserve pour contingence)
  - Connaissance de l'état de marche, de la capacité, du taux de rampe et du temps de démarrage des groupes (GO et BA)
  - Démarrage des groupes de production et fourniture de l'énergie (GOP)

~~Contrôle~~Régulation de la fréquence (puissance active)

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

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

Mis en fo
Mis en fo
Paragraph
Mis en fo
Mis en fo
Mis en fo
Mis en fo

~~Contrôle~~Régulation de la tension (puissance réactive)

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

- Régulation automatique de la tension (AVR)
  - Capteurs, système de commande de stator et rétroaction (GO)
- Ressources capacitives
  - État, commande (manuelle ou automatique) et rétroaction (TOP, TO et DP)
- Ressources inductives (changeurs de prises de transformateur ou bobines d'inductance)
  - État, commande (manuelle ou automatique) et rétroaction (TOP, TO et DP)
- Compensateurs statiques (SVC)
  - État, calculs, commande (manuelle ou automatique) et rétroaction (TOP, TO et DP)

Gestion des contraintes

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

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

Surveillance et contrôle

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

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

Remise en charge du *BES*

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

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

Connaissance de la situation

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

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

Coordination entre les entités

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

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

- Directives d'exploitation (TOP, RC et BA)

Applicabilité aux distributeurs

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

Exigence E1

L'exigence E1 met en ~~oeuvre~~œuvre une méthode de catégorisation des *systèmes électroniques BES* selon leur impact sur le *BES*. Dans l'équation traditionnelle d'évaluation du risque, cette méthode réduit la mesure du risque à l'évaluation de l'impact (la conséquence), en supposant un indice de vulnérabilité de 1 (les systèmes sont présumés vulnérables) et une probabilité de menace de 1 (probabilité de 100 %). Les critères de l'annexe 1 ~~expriment~~permettent de mesurer le degré d'impact des actifs *BES* desservis par les *systèmes électroniques BES*.

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

Annexe 1

Application générale

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

- Lorsque l'équipe de rédaction utilise le terme « *installations* », les entités responsables disposent d'une certaine latitude pour déterminer les *installations* concernées. Le terme « *installation* » est défini dans le glossaire de la NERC comme un « ensemble d'équipements électriques qui fonctionnent comme un seul *élément* du *système de production-transport d'électricité* (exemples : ligne, groupe de production, compensateur shunt, transformateur, etc.). » Dans la plupart des cas, les critères ~~référent~~se rapportent à un groupe d'*installations* dans un emplacement donné qui contribue à l'exploitation fiable du *BES*. Par exemple, pour les actifs de *transport*, le poste peut être désigné comme le groupe d'*installations*. Cependant, dans un poste qui comprend à la fois de l'équipement utilisé pour l'exploitation du *BES* et de l'équipement utilisé seulement pour les ~~opérations~~activités de distribution, il peut être préférable pour l'entité responsable de considérer seulement le groupe

Mis en fo
Ne pas aju
latin et asi
l'espace en
asiatiques

Mis en fo

Mis en fo

Mis en fo

Mis en fo

Mis en fo

d'*installations* utilisé pour l'exploitation du *BES*. Dans ce cas, l'entité responsable peut désigner le groupe d'*installations* par son emplacement, avec des ~~restrictions~~indications pour cibler le groupe d'*installations* qui contribue à l'exploitation fiable du *BES*, comme étant les *installations* qui sont visées par les critères de catégorisation des *systèmes électroniques BES*. Les *installations* de production sont ~~discutées~~traitées séparément à la section Production ci-après. Dans la norme CIP-002-5.~~1~~1a, ces groupes d'*installations*, de systèmes et d'équipements sont parfois appelés « actifs *BES* ». Par exemple, un actif *BES* ~~identifié~~répertorié peut être un poste, une centrale de production ou un *centre de contrôle* nommé. Les entités responsables disposent d'une souplesse dans la manière de grouper les *installations*, systèmes et équipements à un emplacement donné.

- Dans certains cas, un *système électronique BES* peut être catégorisé ~~par le respect de~~parce qu'il répond à plusieurs critères. Dans de tels cas, l'entité responsable peut choisir de documenter tous les critères qui mènent à la catégorisation. Cela évitera une catégorisation incorrecte lorsqu'il ~~ne répond plus~~cesse de répondre à l'un des critères, mais qu'il répond encore à un autre.
- Il est recommandé que chaque *système électronique BES* soit ~~inventorié~~répertorié par une seule entité responsable. En cas de propriété commune, il est conseillé aux entités responsables propriétaires de s'entendre formellement sur la désignation ~~de l'entité~~d'une entité responsable à titre de responsable de la conformité aux normes.

Impact élevé (H)

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

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

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

Impact moyen (M)

Production

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

- Le critère 2.1 désigne comme étant à Impact moyen les *systèmes électroniques BES* qui influent sur des ressources de production dont la capacité en *puissance active nette* est supérieure à 1 500 MW. Le critère de 1 500 MW est partiellement tiré des exigences de *réserve pour contingence* de la norme BAL-002 de la NERC, dont l'objet est de « ~~s'assurer~~faire en sorte que le *responsable de l'équilibrage* ~~peut utiliser~~soit en mesure d'utiliser sa *réserve pour contingence* afin d'équilibrer les ressources et la demande, et de rétablir la fréquence de l'*Interconnexion* ~~dans les~~à l'intérieur des limites ~~établies après~~définies suivant une *perturbation à déclarer* ». En particulier, elle exige qu'« ~~au~~Au minimum, le *responsable de l'équilibrage* ou le *groupe de partage des réserves* doit disposer d'une *réserve pour contingence* suffisante afin de se ~~protéger~~prémunir contre la contingence simple la plus grave. » L'équipe de rédaction a utilisé 1 500 MW comme chiffre provenant des *réserves pour contingence* les plus importantes exploitées par divers BA dans toutes les régions.

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

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

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

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

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

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

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

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

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

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

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

Transport

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

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

Mis en fo

Mis en fo
solidaires

Mis en fo

Mis en fo

installations. La valeur de 1 000 Mvar utilisée dans ce critère est une valeur jugée raisonnable pour déterminer la criticité de l'impact.

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

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

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

  - exclut les installations radiales qui ~~fournirait~~fourniraient du ~~support~~soutien pour une seule installation de production ;
  - spécifie le raccordement à au moins trois postes de transport pour s'assurer que le degré d'impact soit approprié.

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

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

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

- 765- kV –> 3- 000- MVA

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

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

- Les lignes à dérivations multiples sont ~~considérées~~censées représenter une seule valeur pondérée par ligne et influent sur le nombre de raccordements à d'autres postes. Ainsi, une seule ligne à 230 kV à dérivations multiples entre trois postes de *transport* représenterait une valeur pondérée totale de 700 et ~~raccorde~~raccorderait des *installations* de *transport* d'un seul poste à deux autres postes de *transport*.

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

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

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

Mis en fo

Mis en fo

Mis en fo

Mis en fo
0,75", Inte

de moins de 200 kV ou de 500 kV et plus dans le tableau des valeurs pour la contribution à la valeur combinée de 3 000.

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

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

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

- Le critère~~.~~ 2.8 désigne comme ~~Impact~~« à impact moyen » les *systèmes électroniques BES* qui ont un impact sur les *installations* de *transport* nécessaires pour des installations de production qui respectent les conditions du critère 2.1 (*installations* de production avec une ~~sortie~~puissance de plus de 1 500 MW) et 2.3 (*installations* de production généralement désignées comme indispensables à la fiabilité de la zone étendue dans l'horizon de planification). L'entité responsable peut demander une déclaration formelle du propriétaire d'installation de production quant à la qualification des *installations* de production raccordées à ses réseaux de *transport*.

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

- Le critère 2.10 désigne comme ~~Impact~~« à impact moyen » les *systèmes électroniques BES* pour les systèmes ou *éléments* qui effectuent, sans intervention humaine, un délestage de charge automatique de 300 MW ou plus. ~~Le~~La SDT a passé un temps considérable à discuter de la formulation du critère 2.10, et choisi le mot « chaque » pour indiquer que le critère s'applique à un système ou une *installation* distincte. Dans la rédaction de ce critère, l'équipe de rédaction a cherché à inclure seulement les systèmes qui ne nécessitent pas d'intervention humaine, et a ciblé en particulier les *installations* et les systèmes de délestage de charge en sous-fréquence (DSF) et les systèmes et les *éléments* de délestage

Mis en fo
Mis en fo
Italique
Mis en fo
Mis en fo
Mis en fo
Mis en fo
Mis en fo
Mis en fo
Mis en fo

de charge en sous-tension (DST) qui seraient visés par une exigence de délestage de charge régionale visant à prévenir un *impact négatif sur la fiabilité*. Ceux-ci comprennent les systèmes automatisés DSF et DST capables de délester 300 MW de charge ou plus. Il est à noter que les systèmes qui ont besoin d'une intervention humaine pour leur armement, mais qui une fois armés se déclenchent automatiquement, doivent être considérés comme ne nécessitant pas d'intervention humaine et devraient être désignés comme ~~Impact~~« à impact moyen~~.~~ ». Le seuil de 300 MW a été défini comme la valeur de charge totale en MW la plus élevée, définie selon les normes de délestage de charge régionales pertinentes, pour les 12 mois précédents ~~pour~~afin de tenir compte des fluctuations saisonnières.

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

Mis en fo

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

Mis en fo

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

- Le critère 2.12 catégorise comme ~~Impact~~« à impact moyen » les *systèmes électroniques BES* utilisés par et dans les *centres de contrôle* et les centres informatiques connexes qui s'acquittent des obligations fonctionnelles d'un *exploitant de réseau de transport* et qui n'ont pas déjà été catégorisés comme ~~Impact~~« à impact élevé~~.~~ ».
- Le critère 2.13 catégorise comme ~~Impact~~« à impact moyen » les *centres de contrôle* de BA qui « contrôlent » une production de 1 500 MW ou plus dans une même *Interconnexion*. Le seuil de 1 500 MW est cohérent avec le degré d'impact et le raisonnement indiqué pour le critère 2.1.

Impact faible (L)

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

Installations de remise en charge

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

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

  En réponse à ces considérations, l'équipe de rédaction a recatégorisé les actifs de remise en charge, comme les *ressources à démarrage autonome* et les *chemins de démarrage*, les faisant passer de la catégorie Impact moyen (comme c'était le cas dans les premières versions de travail) à la catégorie Impact faible. Cela ne libère pas les propriétaires de ces actifs de toute responsabilité, comme cela aurait été le cas dans les versions 1 à 4 de la norme CIP-002 (puisque seuls les *actifs électroniques* à connectivité routable qui sont essentiels aux actifs de remise en charge sont inclus dans ces versions). En vertu de la catégorisation Impact faible, ces actifs seront protégés dans les domaines de sensibilisation à la cybersécurité, de contrôle des accès physiques et de contrôle des accès électroniques, et seront soumis à des obligations quant aux interventions en cas d'incident. Il s'agit néanmoins, en fin de compte, d'un gain net pour la fiabilité du *BES*, puisque beaucoup de ces actifs ne répondent pas aux critères d'inclusion des versions 1 à 4.

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

  Les *systèmes électroniques BES* pour les ressources de production qui ont été désignées comme *ressources à démarrage autonome* dans le plan de remise en charge de l'*exploitant de réseau de transport* tombent par défaut dans la catégorie Impact faible. La

Mis en fo
Mis en fo
Mis en fo

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

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

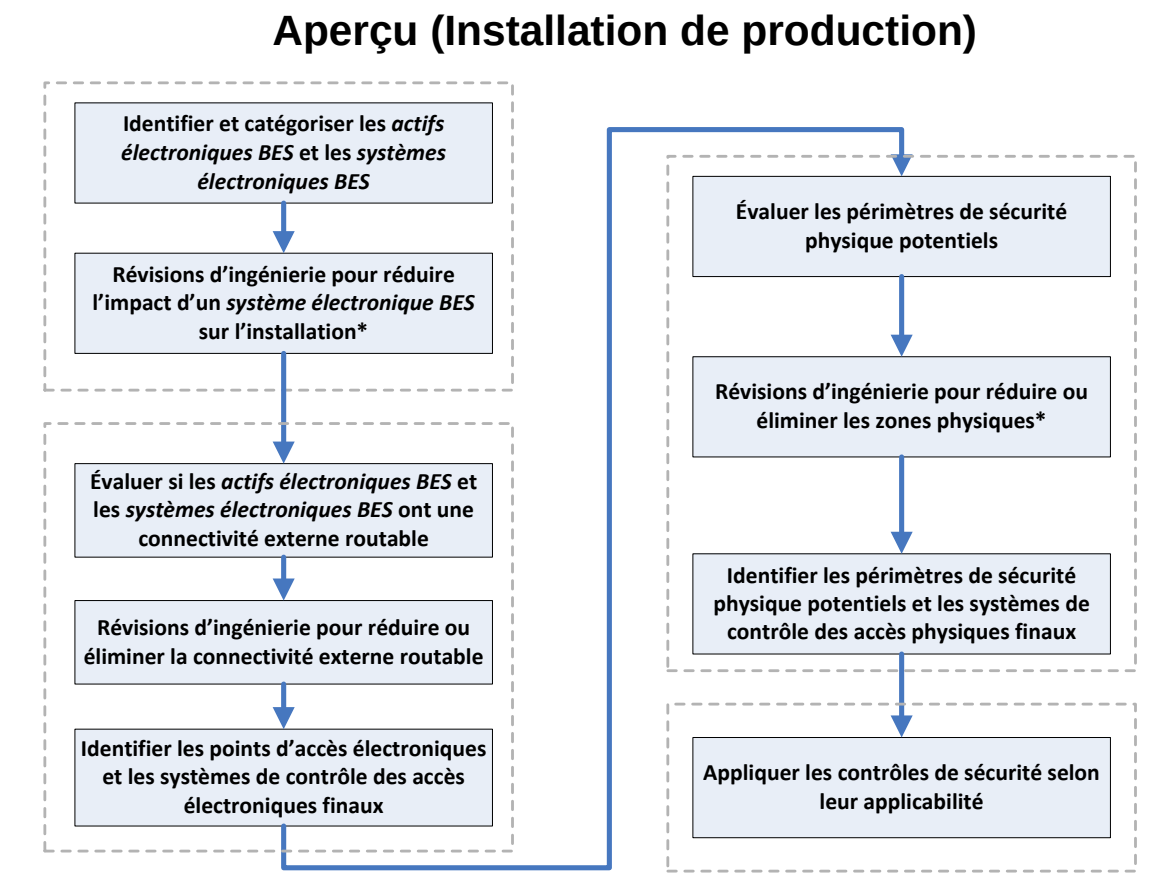
Mis en fo

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

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

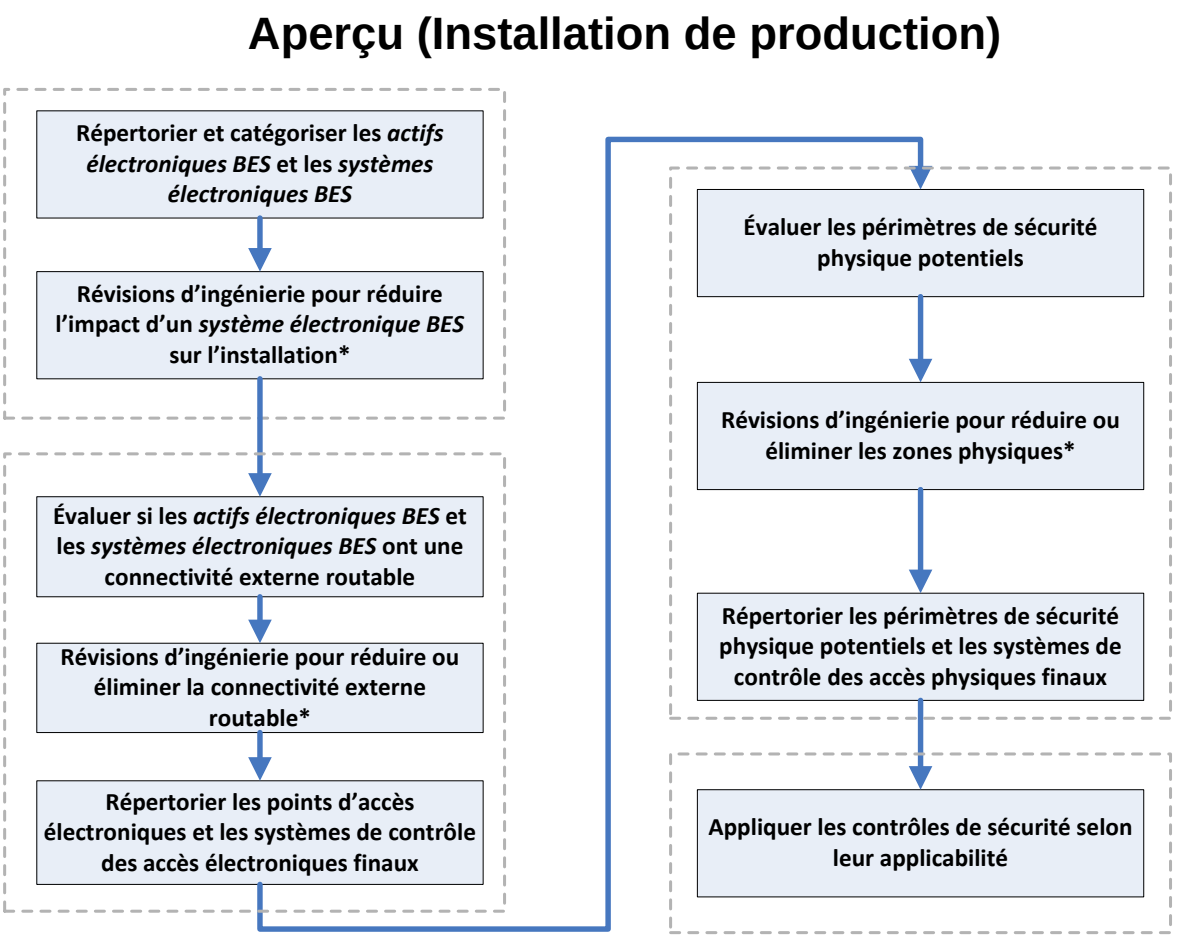
Cas d'utilisation : déroulement du processus CIP

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



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

~~**Raisonnement**~~



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

Justification

Pendant l'élaboration de cette norme, ~~les références aux versions antérieures~~ des ~~normes CIP et le raisonnement derrière les exigences et leurs~~zones de texte ont été incorporées à celle-ci pour exposer la justification de ses diverses parties~~ étaient intégrés à même la norme. Sur approbation du BOT, cette information~~. Après l'approbation par le Conseil d'administration, le contenu de ces zones de texte a été ~~déplacée à la présente section~~transféré ci-après.

~~**Raisonnement pour E1 :**~~

Justification de l'exigence E1

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

Mis en fo

~~**Raisonnement pour E2 :**~~

Justification de l'exigence E2

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

Mis en fo

Mis en fo

Historique des versions

Version	Date	Intervention	Suivi des modifications
1	16- janvier 2006	E3.2 — Remplacement de « Control Center » par « control center » dans la version anglaise.	24 mars 2006
2	30- septembre 2009	Modifications visant à clarifier les exigences et à mettre les éléments de conformité en concordance avec les plus récentes directives sur l'établissement des éléments de conformité des normes. Suppression de la mention sur la prise en compte des considérations d'affaires. Remplacement de l'organisation régionale de fiabilité par l'*entité régionale* comme entité responsable. Reformulation de la date d'entrée en vigueur. Remplacement de « Responsabilité de la surveillance de la conformité » par « ~~responsable deas mesures pour assurer~~Responsabilité du contrôle de la conformité ».	
3	16- décembre 2009	Changement du numéro de version de -2 à -3. Approbation par le Conseil d'administration de la NERC.	Mise à jour
3	31- mars 2010	Approbation par la FERC.	
4	30- décembre 2010	Ajout de critères précis pour l'identification des actifs critiques.	Mise à jour
4	24- janvier 2011	Approbation par le Conseil d'administration de la NERC.	Mise à jour

Mis en fo

Version	Date	Intervention	Suivi des modifications
5	26- novembre 2012	Approbation par le Conseil d'administration de la NERC.	~~Modifiée~~Modification en coordination avec les autres normes CIP et révision du format selon le gabarit RBS.
5.1	30- septembre 2013	Remplacement de « Devices » par « Systems » dans une définition de la section ~~«~~ Contexte ~~».~~.	Errata
5.1	22- novembre 2013	~~Émission d'une ordonnance~~Ordonnance de la FERC approuvant la version CIP-002-5.1. ~~(L'ordonnance entre en vigueur le 3 février 2014)~~	
5.1a	2 novembre 2016	Adoption par le Conseil d'administration de la NERC.	
5.1a	14 décembre 2016	Ordonnance de la FERC approuvant la version CIP-002-5.1a (dossier RD17-2-000).	

Mis en fo
pt, Gras

Mis en fo

Addenda 1

Numéro et texte de l'exigence

CIP-002-5.1, exigence E1

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

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

ii. postes de transport ;

iii. ressources de production ;

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

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

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

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

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

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

Annexe 1, critère 2.1

2. **Impact moyen (M)**

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

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

Mis en fo
pt, Gras

Questions

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

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

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

Réponses

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

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

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

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

Mis en fo
pt, Gras

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

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

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

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

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

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

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

Mis en fo
Roman

Mis en fo

A. Introduction

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

2. Numéro : CIP-003-~~6~~7

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

4. Applicabilité :

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

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

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

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

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

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

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

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

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

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

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

Mis en fo
Mis en fo

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

4.1.6 ***Coordonnateur de la fiabilité***

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

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

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

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

4.2.1.1 Chaque système ~~de~~ DSF ou ~~de~~ DST qui :

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

Mis en fo

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

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

Mis en fo

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

Mis en fo

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

Mis en fo
Automatiq

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

Toutes les *installations* du *BES*.

4.2.3 Exemptions : Sont exemptés de la norme CIP-003-~~6~~7 :

4.2.3.1 les *actifs électroniques* aux *installations* réglementées par la Commission canadienne de sûreté nucléaire ;

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

4.2.3.3 les systèmes, structures et composants régis par la U.S. Nuclear Regulatory Commission en vertu d'un plan de cybersécurité ~~conforme~~, 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-~~6~~7.

6. Contexte :

La norme CIP-003 fait partie d'une série de normes CIP sur la cybersécurité qui exigent la détermination et la catégorisation initiales des *systèmes électroniques BES*. Ces normes exigent aussi ~~un niveau minimal de~~des mesures organisationnelles, opérationnelles et administratives pour ~~réduire~~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 ~~à la section Exigences~~dans les exigences et les mesures sous forme de liste à puces sont liés par l'opérateur « ou », et les éléments présentés sous forme de liste numérotée sont liés par l'opérateur « et ».

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

B. Exigences et mesures

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

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

1.1.1. personnel et formation (CIP-004) ;

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

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

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

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

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

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

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

1.1.9. déclaration ~~et réponse aux~~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 ~~pour toute *connectivité externe routable à impact faible (LERC)* et la *connectivité par lien commuté* ; et~~ ;

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

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

~~1.2.4.~~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 ~~conformes à~~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 ~~identification~~désignation distincte des *systèmes électroniques BES* à impact faible ou de leurs *actifs électroniques BES* n'est pas exigé. Des listes d'utilisateurs autorisés ne sont pas exigées.

M2. Les pièces justificatives doivent comporter chacun des plans de cybersécurité qui, collectivement, couvrent toutes les sections de l'annexe 1 ; d'autres pièces justificatives doivent attester la mise en œuvre des plans de cybersécurité. L'annexe 2 présente d'autres exemples de pièces justificatives pour chacune des sections de l'annexe 1.

E3. Chaque entité responsable doit désigner nominativement un *cadre supérieur CIP* et documenter tout changement dans un délai de 30 jours civils suivant le changement. *[Facteur de risque de non-conformité : moyen] [Horizon : planification de l'exploitation]*

M3. Exemple non limitatif de pièce justificative : document daté et approuvé par un haut dirigeant indiquant le nom de la personne désignée comme *cadre supérieur CIP*.

E4. L'entité responsable doit mettre en œuvre un processus documenté de délégation de pouvoirs, sauf en l'absence de toute délégation. Dans les cas permis par les normes CIP, le *cadre supérieur CIP* peut déléguer ses pouvoirs relatifs à certains actes à un ou plusieurs délégataires. Ces délégations doivent être documentées, et comprendre notamment le nom ou le titre du délégataire, les actes délégués et la date de la délégation ; être approuvées par le *cadre supérieur CIP* ; et être mises à jour dans un délai de 30 jours suivant tout changement à la délégation. Il n'est pas nécessaire de réaffirmer les changements de délégation en cas de changement de délégant. *[Facteur de risque de non-conformité : faible] [Horizon : planification de l'exploitation]*

M4. Exemple non limitatif de pièce justificative : document daté et approuvé par le *cadre supérieur CIP* indiquant la ou les personnes (nom ou titre) auxquelles est délégué le pouvoir d'approuver ou d'autoriser des actions décrites explicitement.

C. Conformité

1. Processus de surveillance de la conformité

1.1. Responsable des mesures pour assurer la conformité

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

1.2. Conservation des pièces justificatives

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

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

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

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

Audits de conformité

Déclarations sur la conformité

Contrôles ponctuels

Enquêtes de conformité

Déclarations de non-conformité

Plaintes

1.4. Autres informations sur la conformité

Aucune.

2. Tableau des éléments de conformité

Ex.	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-003-~~6~~7)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
E1	**Planification de l'exploitation**	**Moyen**	L'entité responsable a documenté et mis en œuvre une ou plusieurs politiques de cybersécurité pour ses *systèmes électroniques BES* à impact élevé et moyen, mais ~~il n'a pas traité de~~en omettant l'un des neuf thèmes indiqués à l'exigence E1. (E1.1) OU L'entité responsable a terminé le réexamen de sa ou ses politiques de cybersécurité documentées pour ses *systèmes électroniques BES* à impact élevé et moyen selon l'exigence E1, mais dans un délai de plus de 15 mois civils et d'au plus 16 mois civils suivant le réexamen précédent. (E1.1) OU L'entité responsable a fait approuver par le *cadre supérieur CIP* sa ou ses	L'entité responsable a documenté et mis en œuvre une ou plusieurs politiques de cybersécurité pour ses *systèmes électroniques BES* à impact élevé et moyen, mais en omettant deux des neuf thèmes indiqués à l'exigence E1. (E1.1) OU L'entité responsable a terminé le réexamen de sa ou ses politiques de cybersécurité documentées pour ses *systèmes électroniques BES* à impact élevé et moyen selon l'exigence E1, mais dans un délai de plus de 16 mois civils et d'au plus 17 mois civils suivant le réexamen précédent. (E1.1) OU L'entité responsable a fait approuver par le *cadre supérieur CIP* sa ou ses politiques de cybersécurité	L'entité responsable a documenté et mis en œuvre une ou plusieurs politiques de cybersécurité pour ses *systèmes électroniques BES* à impact élevé et moyen, mais en omettant trois des neuf thèmes indiqués à l'exigence E1. (E1.1) OU L'entité responsable a terminé le réexamen de sa ou ses politiques de cybersécurité documentées pour ses *systèmes électroniques BES* à impact élevé et moyen selon l'exigence E1, mais dans un délai de plus de 17 mois civils et d'au plus 18 mois civils suivant le réexamen précédent. (E1.1) OU L'entité responsable a fait approuver par le *cadre supérieur CIP* sa ou ses politiques de cybersécurité	L'entité responsable a documenté et mis en œuvre une ou plusieurs politiques de cybersécurité pour ses *systèmes électroniques BES* à impact élevé et moyen, mais en omettant au moins quatre des neuf thèmes indiqués à l'exigence E1. (E1.1) OU L'entité responsable n'avait aucune politique de cybersécurité documentée pour ses *systèmes électroniques BES* à impact élevé et moyen, comme le prescrit l'exigence E1. (E1.1) OU L'entité responsable n'a pas terminé le réexamen de sa ou ses politiques de cybersécurité selon l'exigence E1 dans un délai de 18 mois civils suivant le réexamen précédent. (E1) OU

Ex.	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-003-~~6~~7)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
			politiques de cybersécurité documentées pour ses *systèmes électroniques BES* à impact élevé et moyen selon l'exigence E1, mais dans un délai de plus de 15 mois civils et d'au plus 16 mois civils suivant l'approbation précédente. (E1.1) OU L'entité responsable a documenté une ou plusieurs politiques de cybersécurité pour ses actifs qui comportent des *systèmes électroniques BES* à impact faible selon les critères de la norme CIP-002, mais en omettant un des ~~quatre~~six thèmes indiqués à l'exigence E1. (E1.2) OU L'entité responsable a terminé le réexamen, selon l'exigence E1, de sa ou ses politiques de cybersécurité documentées pour ses actifs qui comportent des	documentées pour ses *systèmes électroniques BES* à impact élevé et moyen selon l'exigence E1, mais dans un délai de plus de 16 mois civils et d'au plus 17 mois civils suivant l'approbation précédente. (E1.1) OU L'entité responsable a documenté une ou plusieurs politiques de cybersécurité pour ses actifs qui comportent des *systèmes électroniques BES* à impact faible selon les critères de la norme CIP-002, mais en omettant deux des ~~quatre~~six thèmes indiqués à l'exigence E1. (E1.2) OU L'entité responsable a terminé le réexamen, selon l'exigence E1, de sa ou ses politiques de cybersécurité documentées pour ses actifs qui comportent des *systèmes électroniques*	documentées pour ses *systèmes électroniques BES* à impact élevé et moyen selon l'exigence E1, mais dans un délai de plus de 17 mois civils et d'au plus 18 mois civils suivant l'approbation précédente. (E1) OU L'entité responsable a documenté une ou plusieurs politiques de cybersécurité pour ses actifs qui comportent des *systèmes électroniques BES* à impact faible selon les critères de la norme CIP-002, mais en omettant trois des ~~quatre~~six thèmes indiqués à l'exigence E1. (E1.2) OU L'entité responsable a terminé le réexamen, selon l'exigence E1, de sa ou ses politiques de cybersécurité documentées pour ses actifs qui comportent des *systèmes électroniques*	L'entité responsable n'a pas fait approuver par le *cadre supérieur CIP* sa ou ses politiques de cybersécurité documentées pour ses *systèmes électroniques BES* à impact élevé et moyen selon l'exigence E1 dans un délai de 18 mois civils suivant l'approbation précédente. (E1.1) OU L'entité responsable a documenté une ou plusieurs politiques de cybersécurité pour ses actifs qui comportent des *systèmes électroniques BES* à impact faible selon les critères de la norme CIP-002, mais en omettant ~~les~~au moins quatre des six thèmes indiqués à l'exigence E1. (E1.2) OU L'entité responsable n'avait aucune politique de cybersécurité documentée, selon l'exigence E1, pour ses

Ex.	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-003-~~6~~7)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
			systèmes électroniques BES à impact faible selon les critères de la norme CIP-002, mais dans un délai de plus de 15 mois civils et d'au plus 16 mois civils suivant le réexamen précédent. (E1.2) OU L'entité responsable a fait approuver par le *cadre supérieur CIP*, selon l'exigence E1, sa ou ses politiques de cybersécurité documentées pour ses actifs qui comportent des *systèmes électroniques BES* à impact faible selon les critères de la norme CIP-002, mais dans un délai de plus de 15 mois civils et d'au plus 16 mois civils suivant l'approbation précédente. (E1.2)	*BES* à impact faible selon les critères de la norme CIP-002, mais dans un délai de plus de 16 mois civils et d'au plus 17 mois civils suivant le réexamen précédent. (E1.2) OU L'entité responsable a fait approuver par le *cadre supérieur CIP*, selon l'exigence E1, sa ou ses politiques de cybersécurité documentées pour ses actifs qui comportent des *systèmes électroniques BES* à impact faible selon les critères de la norme CIP-002, mais dans un délai de plus de 16 mois civils et d'au plus 17 mois civils suivant l'approbation précédente. (E1.2)	*BES* à impact faible selon les critères de la norme CIP-002, mais dans un délai de plus de 17 mois civils et d'au plus 18 mois civils suivant le réexamen précédent. (E1.2) OU L'entité responsable a fait approuver par le *cadre supérieur CIP*, selon l'exigence E1, sa ou ses politiques de cybersécurité documentées pour ses actifs qui comportent des *systèmes électroniques BES* à impact faible selon les critères de la norme CIP-002, mais dans un délai de plus de 17 mois civils et d'au plus 18 mois civils suivant l'approbation précédente. (E1.2)	actifs qui comportent des *systèmes électroniques BES* à impact faible selon les critères de la norme CIP-002. (E1.2) OU L'entité responsable n'a pas fait approuver par le *cadre supérieur CIP*, selon l'exigence E1, sa ou ses politiques de cybersécurité documentées pour ses actifs qui comportent des *systèmes électroniques BES* à impact faible selon les critères de la norme CIP-002~~,~~ dans un délai de 18 mois civils suivant l'approbation précédente. (E1.2)
E2	**Planification de l'exploitation**	**Faible**	L'entité responsable a documenté son ou ses plans de cybersécurité pour ses actifs comportant des *systèmes électroniques BES* à impact faible, mais n'a pas documenté son plan de sensibilisation à la	L'entité responsable a documenté son ou ses plans de cybersécurité pour ses actifs comportant des *systèmes électroniques BES* à impact faible, mais n'a pas fait de rappel des pratiques de cybersécurité au moins	L'entité responsable a documenté le contrôle des accès physiques pour ses actifs comportant des *systèmes électroniques BES* à impact faible, mais n'a pas mis en place les mesures de sécurité physique	L'entité responsable n'a pas documenté ~~ou~~et mis en œuvre un ou plusieurs plans de cybersécurité pour ses actifs comportant des *systèmes électroniques BES* à impact faible conformément à l'annexe 1

Ex.	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-003-~~6~~7)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
			cybersécurité conformément à la section 1 de l'annexe 1 portant sur l'exigence E2~~ de la norme CIP-003-6.~~ (E2) OU L'entité responsable a mis en place un contrôle des accès électroniques, mais n'a pas documenté son ou ses plans de cybersécurité concernant le contrôle des accès électroniques conformément à la section 3 de l'annexe 1 portant sur l'exigence E2. (E2) OU L'entité responsable a documenté son ou ses plans de cybersécurité pour ses actifs comportant des *systèmes électroniques BES* à impact faible, mais n'a pas documenté un ou plusieurs plans d'intervention en cas d'*incident de cybersécurité* conformément à la section 4 de l'annexe 1 portant sur l'exigence E2~~ de la norme CIP-003-6.~~ (E2)	une fois tous les 15 mois civils conformément à la section 1 de l'annexe 1 portant sur l'exigence E2~~ de la norme CIP-003-6.~~ (E2) OU L'entité responsable a documenté son ou ses plans de cybersécurité pour ses actifs comportant des *systèmes électroniques BES* à impact faible, mais n'a pas documenté de mesures de sécurité physique conformément à la section 2 de l'annexe 1 portant sur l'exigence E2. (E2) OU L'entité responsable a documenté son ou ses plans de cybersécurité pour ses actifs comportant des *systèmes électroniques BES* à impact faible, mais n'a pas documenté de mesures de contrôle des accès électroniques conformément à la section 3 de l'annexe 1 portant sur l'exigence E2.	conformément à la section 2 de l'annexe 1 portant sur l'exigence E2. (E2) OU L'entité responsable a documenté son ou ses plans de cybersécurité pour le contrôle des accès électroniques à ses actifs comportant des *systèmes électroniques BES* à impact faible, mais n'a pas limité les communications aux seuls accès entrants et sortants nécessaires conformément à la section 3.1 de l'annexe 1 portant sur l'exigence E2. (E2) OU L'entité responsable a documenté un ou plusieurs plans d'intervention en cas d'*incident de cybersécurité* dans le cadre de son ou ses plans de cybersécurité pour ses actifs comportant des *systèmes électroniques BES* à impact faible, mais n'a pas mis à l'essai chaque plan	portant sur l'exigence E2~~ de la norme CIP-003-6.~~ (E2)

Ex.	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-003-~~6~~7)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
			OU L'entité responsable a documenté un ou plusieurs plans d'intervention en cas d'*incident de cybersécurité* dans le cadre de son ou ses plans de cybersécurité pour ses actifs comportant des *systèmes électroniques BES* à impact faible, mais n'a pas mis à~~-~~ jour chaque plan d'intervention en cas d'*incident de cybersécurité* dans un délai de 180 jours conformément à la section 4 de l'annexe 1 portant sur l'exigence E2.~~.~~ (E2) OU ~~de la norme CIP-003-6. (E2)~~L'entité responsable a documenté son ou ses plans concernant les *actifs électroniques temporaires* et les *supports de stockage amovibles*, mais n'a pas géré ses *actifs électroniques temporaires* conformément à la section 5.1 de l'annexe 1 portant sur l'exigence E2. (E2)	(E2) OU L'entité responsable a documenté son ou ses plans de cybersécurité portant sur le contrôle des accès électroniques, mais n'a pas mis en place une authentification pour toute *connectivité par lien commuté* donnant accès à un ou des *systèmes électroniques BES* à impact faible, selon les capacités de l'*actif électronique*, conformément à la section 3.2 de l'annexe 1 portant sur l'exigence E2. (E2) OU L'entité responsable a documenté un ou plusieurs plans d'intervention en cas d'incident dans le cadre de son ou ses plans de cybersécurité pour ses actifs comportant des *systèmes électroniques BES* à impact faible, mais n'a pas inclus le processus de détection, de classement et	d'intervention en cas d'*incident de cybersécurité* au moins une fois tous les 36 mois civils conformément à la section 4 de l'annexe 1 portant sur l'exigence E2~~ de la norme CIP-003-6.~~. (E2) OU L'entité responsable a documenté le processus consistant à déterminer si un *incident de cybersécurité* constaté est un *incident de cybersécurité à déclarer*, mais n'a pas avisé l'Electricity ~~Sector~~ Information Sharing and Analysis Center (~~ES-~~E-ISAC) conformément à la section 4 de l'annexe 1 portant sur l'exigence E2~~ de la norme CIP-003-6~~. (E2) OU L'entité responsable a documenté ~~et mis en œuvre un contrôle des accès électroniques~~ son ou ses plans pour les ~~*LERC*~~*actifs électroniques temporaires* et les *supports*	

Mis en fo
Mis en fo
Mis en fo Automatiq
Mis en fo Automatiq
Mis en fo Automatiq
Mis en fo (Calibri)
Mis en fo (Calibri)
Mis en fo (Calibri)
Mis en fo (Calibri)
Mis en fo (Calibri)
Mis en fo : 0 pt, Apr
Mis en fo (Calibri)
Mis en fo (Calibri)

Ex.	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-003-~~6~~7)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
			OU L'entité responsable a documenté son ou ses plans concernant les *actifs électroniques temporaires*, mais n'a pas documenté les mesures applicables aux *supports de stockage amovibles* conformément à la section 5.3 de l'annexe 1 portant sur l'exigence E2. (E2)	d'intervention en cas d'*incident de cybersécurité* conformément à la section 4 de l'annexe 1 portant sur l'exigence E2 ~~de la norme CIP-003-6.~~. (E2) OU L'entité responsable a documenté son ou ses plans de cybersécurité pour ses actifs comportant des *systèmes électroniques BES* à impact faible, mais n'a pas documenté le processus consistant à déterminer si un *incident de cybersécurité* constaté est un *incident de cybersécurité à déclarer*, puis à en aviser l'Electricity ~~Sector~~ Information Sharing and Analysis Center (~~ES~~ E-ISAC) conformément à la section 4 de l'annexe 1 portant sur l'exigence E2 ~~de la norme CIP-003-6.~~ (E2) OU L'entité responsable a documenté son ou ses plans ~~de cybersécurité~~ pour ~~ses~~les *actifs* ~~comportant des systèmes~~ électroniques ~~*BES*~~	*de stockage amovibles*, mais n'a pas mis en place ~~un *LEAP* ou géré les accès entrants et sortants~~ de mesures pour atténuer le risque lié à l'introduction de programmes malveillants à partir d'*actifs électroniques temporaires* gérés par l'entité responsable conformément à la section ~~3 de l'annexe 1 portant sur l'exigence E2 de la norme CIP-003-6~~5.1 ~~(E2)~~ ~~OU~~ ~~L'entité responsable a documenté et mis en œuvre un contrôle des accès électroniques pour ses actifs comportant des *systèmes électroniques BES* à impact faible, mais n'a pas documenté et mis en place une authentification pour toutes les *connectivités par lien commuté* (s'il en existe) qui donnent accès à des *systèmes électroniques BES* à impact faible, conformément à la section 3~~ de l'annexe 1 portant sur l'exigence E2 ~~de~~	

Ex.	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-003-~~6~~7)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
				~~à impact faible~~*temporaires* et les *supports de stockage amovibles*, mais n'a pas documenté de mesures pour atténuer le risque lié à l'introduction de ~~sécurité physique~~ programmes malveillants à partir d'*actifs électroniques temporaires* gérés par l'entité responsable conformément ~~à la section 2~~aux sections 5.1 et 5.3 de l'annexe 1 portant sur l'exigence E2 ~~de la norme CIP-003-6~~. (E2) OU L'entité responsable a documenté son ou ses plans ~~de cybersécurité~~ pour ~~ses~~les *actifs* ~~comportant des systèmes~~ *électroniques* ~~*BES* à impact faible~~*temporaires* et les *supports de stockage amovibles*, mais n'a pas documenté de mesures pour atténuer le ~~contrôle des accès~~risque lié à l'introduction de programmes malveillants à partir d'*actifs électroniques temporaires* gérés par une	~~la norme CIP-003-6.~~ (E2) OU L'entité responsable a documenté ~~le contrôle des accès physiques pour~~ son ou ses plans pour les *actifs* ~~comportant des systèmes~~ *électroniques* ~~*BES* à impact faible, mais n'a pas mis en œuvre~~*temporaires* et les ~~mesures~~*supports de* ~~sécurité physique conformément à la section~~ *stockage amovibles*, mais n'a pas mis en place de mesures pour atténuer le risque lié à l'introduction de programmes malveillants à partir d'*actifs électroniques temporaires* gérés par une tierce partie autre que l'entité responsable conformément à la section 5.2 de l'annexe 1 portant sur l'exigence E2 ~~de la norme CIP-003-6.~~ (E2) OU L'entité responsable a documenté son ou ses plans pour les *actifs électroniques*	

Ex.	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-003-~~6~~7)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
				tierce partie autre que l'entité responsable conformément à la section 5.2 de l'annexe 1 portant sur l'exigence E2. (E2) OU L'entité responsable a documenté son ou ses plans concernant les *actifs électroniques temporaires* et les *supports de stockage amovibles*, mais n'a pas mis en place de mesures applicables aux *supports de stockage amovibles* conformément à la section 5.3 de l'annexe 1 portant sur l'exigence E2~~ de la norme CIP-003-6~~. (E2)	*temporaires* et les *supports de stockage amovibles*, mais n'a pas mis en place de mesures pour neutraliser la menace d'un programme malveillant détecté sur un *support de stockage amovible* avant de connecter celui-ci à un *système électronique BES* à impact faible conformément à la section 5.3 de l'annexe 1 portant sur l'exigence E2. (E2)	
E3	**Planification de l'exploitation**	**Moyen**	L'entité responsable a désigné nominativement un *cadre supérieur CIP*, mais a documenté un changement concernant celui-ci dans un délai de plus de 30 jours civils et de moins de 40 jours civils suivant ce changement. (E3)	L'entité responsable a désigné nominativement un *cadre supérieur CIP*, mais a documenté un changement concernant celui-ci dans un délai de plus de 40 jours civils et de moins de 50 jours civils suivant ce changement. (E3).	L'entité responsable a désigné nominativement un *cadre supérieur CIP*, mais a documenté un changement concernant celui-ci dans un délai de plus de 50 jours civils et de moins de 60 jours civils suivant ce changement. (E3).	L'entité responsable n'a pas désigné nominativement un *cadre supérieur CIP*. OU L'entité responsable a désigné nominativement un *cadre supérieur CIP*, mais n'a pas documenté un changement concernant celui-ci dans un délai de 60 jours civils suivant ce

Ex.	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-003-~~6~~7)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
						changement. (E3)
E4	**Planification de l'exploitation**	**Faible**	L'entité responsable a désigné un délégataire en indiquant son nom, son titre, la date de la délégation et les actes délégués, mais a documenté un changement à la délégation dans un délai de plus de 30 jours civils et de moins de 40 jours civils suivant ce changement. (E4)	L'entité responsable a désigné un délégataire en indiquant son nom, son titre, la date de la délégation et les actes délégués, mais a documenté un changement à la délégation dans un délai de plus de 40 jours civils et de moins de 50 jours civils suivant ce changement. (E4)	L'entité responsable a désigné un délégataire en indiquant son nom, son titre, la date de la délégation et les actes délégués, mais a documenté un changement à la délégation dans un délai de plus de 50 jours civils et de moins de 60 jours civils suivant ce changement. (E4)	L'entité responsable a délégué des pouvoirs relatifs à des actes autorisés par les normes CIP, mais n'a pas mis en œuvre de processus pour la délégation des actes du *cadre supérieur CIP*. (E4) OU L'entité responsable a désigné un délégataire en indiquant son nom, son titre, la date de la délégation et les actes délégués, mais n'a pas documenté un changement à la délégation dans un délai de 60 jours civils suivant le changement. (E4)

D. Différences régionales

Aucune.

E. Interprétations

Aucune.

F. Documents connexes

Aucun.

Historique des versions

Version	Date	Intervention	Suivi des modifications
1	16 janvier 2006	E3.2 — Remplacement de « Control Center » par « control center ».	24 mars 2006
2	30 septembre 2009	Modifications visant à clarifier les exigences et à mettre les éléments de conformité en concordance avec les plus récentes directives sur l'établissement des éléments de conformité des normes. Suppression de la mention sur la prise en compte des considérations d'affaires. Remplacement de l'organisation régionale de fiabilité par l'*entité régionale* comme entité responsable. Reformulation de la date d'entrée en vigueur. Remplacement de « *responsable de la surveillance de la conformité* » par « *responsable des mesures pour assurer la conformité* ».	
3	16 décembre 2009	Changement du numéro de version de -2 à -3. Dans l'exigence E1.6, suppression de la phrase concernant le retrait du service d'un composant ou d'un système aux fins d'essais, en réponse à l'ordonnance de la FERC du 30 septembre 2009.	
3	16 décembre 2009	Approbation par le Conseil d'administration de la NERC.	

3	31 mars 2010	Approbation par la FERC.	
4	24 janvier 2011	Approbation par le Conseil d'administration de la NERC.	
5	26 novembre 2012	Adoption par le Conseil d'administration de la NERC.	Modification en coordination avec les autres normes CIP et révision du format selon le modèle RBS.
5	22 novembre 2013	Ordonnance de la FERC approuvant la norme CIP-003-5.	
6	13 novembre 2014	Adoption par le Conseil d'administration de la NERC.	Mise en œuvre de deux prescriptions de l'ordonnance 791 de la FERC concernant l'obligation de « détecter, évaluer et corriger » ainsi que les réseaux de communication
6	12 février 2015	Adoption par le Conseil d'administration de la NERC.	~~Replace~~Remplacement de la version adoptée par le Conseil le 13 novembre 2014. La version à jour met en œuvre des prescriptions en instance de l'ordonnance 791 relativement aux actifs temporaires et aux *systèmes électroniques BES* à impact faible.
6	21 janvier 2016	Ordonnance de la FERC ~~émise~~ approuvant la norme CIP-003-6. ~~Dossier no.~~ (dossier RM15-14-000).	

7	9 février 2017	Adoption par le Conseil d'administration de la NERC.	Révision en réponse à des prescriptions de l'ordonnance 822 de la FERC concernant 1) la définition de *LERC* et 2) les actifs temporaires.
7	19 avril 2018	Ordonnance de la FERC approuvant la norme CIP-003-7 (dossier RM17-11-000).	

~~CIP-003-6 –~~ Annexe 1

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

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

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

Section 1. Sensibilisation à la cybersécurité : Chaque entité responsable doit rappeler, au moins une fois tous les 15 mois civils, les pratiques de cybersécurité (lesquelles peuvent comprendre des pratiques de sécurité physiques connexes).

Section 2. Mesures de sécurité physique : Chaque entité responsable doit contrôler l'accès physique, d'après les besoins qu'elle détermine elle-même, 1) à l'actif ou aux emplacements des *systèmes électroniques BES* à impact faible à l'intérieur de l'actif, et 2) ~~aux *points d'accès électronique de système électronique BES à impact faible (LEAP), s'il en existe*~~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 : ~~Chaque entité~~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~~:~~

~~pour toute *LERC,*~~ mettre en place un ~~*LEAP* afin de permettre~~contrôle des accès électroniques qui :

3.1 autorisent uniquement les accès entrants et sortants ~~bidirectionnels~~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 ;

~~**3.1**~~ assurée par un protocole routable ~~nécessaires ; et~~

ii. ~~mettre~~ en ~~place une authentification pour~~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* ~~qui donne~~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 ~~Sector~~ Information Sharing and Analysis Center (~~ES~~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.

Mis en fo
Mis en fo
Mis en fo (Calibri)
Mis en fo (Calibri)
Mis en fo Retrait : G Hiérarchisa Alignemen : 0,94" + tabulation
Mis en fo
Mis en fo
Mis en fo 0,88", Tac 1,04"

~~CIP-003-6 –~~ **Section 5.** Atténuation des risques liés à l'introduction de programmes malveillants à partir d'*actifs électroniques temporaires* ou de *supports de stockage amovibles* : Chaque entité responsable doit mettre en œuvre, sauf en cas de *circonstances CIP exceptionnelles*, un ou des plans visant à réaliser l'objectif d'atténuer le risque lié à l'introduction de programmes malveillants dans les *systèmes électroniques BES* à impact faible à partir d'*actifs électroniques temporaires* ou de *supports de stockage amovibles*. Ce ou ces plans doivent comprendre :

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

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

5.2 pour tout *actif électronique temporaire* géré par une tierce partie autre que l'entité responsable, l'application d'une ou de plusieurs des mesures suivantes avant de connecter l'*actif électronique temporaire* à un *système électronique BES* à impact faible (selon les capacités de l'*actif électronique temporaire*) :

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

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

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

Mis en fo

Mis en fo

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 l'*actif électronique*, le cas échéant, qui comporte un *LEAP*.~~

  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 que des connexions entrantes et sortantes de tout *LEAP* sont limitées à celles que l'entité responsable juge nécessaires (restriction des adresses IP, des ports ou des services, etc.) ; et~~ documentation 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 ~~Sector~~ Information Sharing and Analysis Center (~~ES~~E-ISAC) ;
2. établir et documenter les rôles et responsabilités des groupes ou des personnes chargés d'intervenir en cas d'*incident de cybersécurité* (déclenchement, documentation, surveillance, déclaration, etc.) ;
3. gérer les *incidents de cybersécurité* (confinement, élimination, reprise après incident ou résolution de l'incident, etc.) ;
4. mettre à l'essai le ou les plans, avec documents datés attestant qu'un essai a été fait au moins une fois tous les 36 mois civils ; et
5. mettre à jour au besoin les plans d'intervention en cas d'*incident de cybersécurité* dans les 180 jours civils suivant la mise à l'essai ou suivant un *incident de cybersécurité à déclarer* réel.

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

1. Exemples non limitatifs de pièces justificatives attestant la conformité à la section 5.1 : documentation des moyens utilisés pour atténuer le risque lié à l'introduction de programmes malveillants, comme des logiciels antivirus et des processus de gestion des mises à jour des signatures ou des séquences de code, des pratiques de liste blanche d'applications, des processus de restriction des communications ou d'autres moyens d'atténuation appropriés. Si un *actif électronique temporaire* n'a pas la capacité de mettre en place certains moyens d'atténuation du risque lié à l'introduction de programmes malveillants, les pièces justificatives peuvent comprendre une documentation du fournisseur ou de l'entité responsable indiquant que l'*actif électronique temporaire* n'a pas cette capacité.

2. Exemples non limitatifs de pièces justificatives attestant la conformité à la section 5.2 : documentation provenant de systèmes de gestion des changements, courriels ou procédures qui documentent un examen du degré de maintien à jour des antivirus installés ; notes de service, courriels, documentation de système, politiques ou contrats d'une tierce partie autre que l'entité responsable qui décrivent le processus de mise à jour des antivirus, l'utilisation d'une liste blanche d'applications, l'utilisation de systèmes d'exploitation sur support externe ou le renforcement du système d'exploitation par la tierce partie ; pièces justificatives provenant de systèmes de gestion des changements, courriels ou contrats indiquant que l'entité responsable juge acceptables les pratiques de la tierce partie ; ou documentation d'autres moyens d'atténuation du risque lié à l'introduction de programmes malveillants pour les *actifs électroniques temporaires* gérés par la tierce partie. Si un *actif électronique temporaire* n'a pas la capacité de mettre en place certains moyens d'atténuation du risque lié à l'introduction de programmes malveillants, les pièces justificatives peuvent comprendre une documentation de l'entité responsable ou de la tierce partie indiquant que l'*actif électronique temporaire* n'a pas cette capacité.

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

Mis en fo

Mis en fo

Principes directeurs et fondements techniques

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

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

La section 4.1~~ (~~. Entités fonctionnelles~~) présente la~~ estla liste des entités fonctionnelles de la NERC auxquelles s'applique la norme. Si l'entité est enregistrée au titre d'une ou de plusieurs des entités fonctionnelles énumérées à la section 4.1~~,~~., alors les normes CIP sur la cybersécurité de la NERC ~~s'y appliquent.~~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 ~~qui, selon~~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 ~~indique~~comprenne déjà ~~qu'il s'agit d'*éléments* du~~la caractéristique *BES*, l'utilisation additionnelle du terme « *BES* » vise ici à renforcer la portée d'applicabilité pour ces *installations*, en particulier dans cette section sur l'applicabilité. Cela ~~aide à clarifier~~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 ~~parapluie~~globale de haut niveau et confier les détails à des documents de niveau inférieur dans la hiérarchie documentaire. Dans le cas d'une politique ~~parapluie~~globale de haut niveau, l'entité responsable devrait fournir la politique ~~parapluie~~globale ainsi que les documents complémentaires afin de démontrer la conformité à l'exigence E1 de la norme~~ -~~ CIP-003-~~6~~7.

Si une entité responsable détient des *systèmes électroniques BES* à impact élevé ou moyen, la ou les politiques de cybersécurité doivent couvrir les neuf thèmes prescrits à ~~la partie~~l'alinéa 1.1 de l'exigence E1 de la norme CIP 003-~~6~~7. Si une entité responsable a ~~désigné~~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 ~~quatre~~six thèmes prescrits à ~~la partie~~ 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-~~6~~7, car on considère qu'elle se manifestera dans la bonne mise en œuvre des normes CIP-003 à CIP-011. Les entités responsables sont toutefois invitées à ne pas limiter la portée de leurs politiques de cybersécurité aux seules exigences des normes de fiabilité de la NERC sur la cybersécurité, mais plutôt à élaborer une politique de cybersécurité globale appropriée à leur organisation. Les éléments d'une politique qui s'étendent au-delà de la portée des normes de fiabilité de la NERC sur la cybersécurité ne seront pas considérés comme donnant lieu à des infractions potentielles ; ils aideront plutôt à témoigner de la culture de conformité au sein de de l'organisation et de sa posture de cybersécurité.

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

1.1.1 Personnel et formation (CIP-004)

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

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

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

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

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

- Méthodes acceptables de contrôle des accès physiques
- Surveillance et consignation des accès physiques

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

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

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

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

1.1.6 Plans de rétablissement des *systèmes électroniques BES* (CIP-009)

- Disponibilité des composants de rechange
- Disponibilité des sauvegardes système

1.1.7 Gestion des changements de configuration et analyses de vulnérabilité (CIP-010)

- Demandes de changement
- Approbation des changements
- Processus de réparation

1.1.8 Protection de l'information (CIP-011)

- Méthodes de contrôle d'accès à l'information
- Notification des divulgations non autorisées
- Accès à l'information selon le principe du besoin de savoir

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

- Processus de recours à des procédures spéciales en cas de *circonstance CIP exceptionnelle*
- Processus de tolérance des dérogations qui n'enfreignent pas les exigences CIP

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

1.2.1 Sensibilisation à la cybersécurité

- Mesures de sensibilisation à la sécurité

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

1.2.2 Mesures de sécurité physique

- Approches acceptables pour la sélection des mesures de sécurité physique

1.2.3 Contrôle des accès électroniques

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

1.2.4 Intervention en cas d'*incident de cybersécurité*

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

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

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

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

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

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

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

Exigence E2

~~À partir de la liste des actifs comportant des *systèmes électroniques BES* à impact faible établie selon la norme CIP-002,~~L'exigence E2 vise à obliger chaque entité responsable ~~doit~~à créer, à documenter et à mettre en œuvre un ou plusieurs plans de cybersécurité ~~fondés sur~~afin de

réaliser l'objectif de sécurité pour la protection des ~~critères objectifs et visant à protéger les~~ *systèmes électroniques BES* à impact faible. Les protections requises ~~par l'exigence E2~~ sont ~~liées au degré de risque pour~~ conçues dans le ~~*BES* en cas de mauvaise utilisation ou d'indisponibilité des *systèmes électroniques BES* à impact faible. Le but recherché est que les protections exigées fassent partie~~cadre d'un programme qui ~~vise les~~s'applique aux *systèmes électroniques BES* à impact faible de façon collective, au niveau des actifs (à partir de ~~l'actif ou du site (~~la liste des actifs comportant des *systèmes électroniques BES* à impact faible établie selon la norme CIP-002), et non au niveau ~~des appareils ou des systèmes individuels.~~de chaque dispositif ou système.

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

Exigence E2, annexe 1

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

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

Le programme de sensibilisation à la cybersécurité oblige les entités à rappeler les bonnes pratiques de cybersécurité à leur personnel au moins une fois tous les 15 mois civils. L'entité est libre de choisir les thèmes à couvrir et la manière de communiquer les rappels sur ces thèmes. Quant aux pièces justificatives ~~de~~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'entité responsable~~L'intention de l'équipe de rédaction n'est pas ~~obligée de~~ d'obliger les entités responsables à tenir des listes de destinataires ni ~~de~~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 ~~œuvre~~place des mesures de contrôle ~~de l'accès physique~~des accès physiques 1) ~~aux~~à l'actif ou aux emplacements des *systèmes électroniques BES* à impact faible à l'intérieur ~~d'actifs qui comportent de tels systèmes,~~ de l'actif et 2) ~~aux *LEAP*, s'il en existe.~~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 ~~le *LEAP* est situé~~des *actifs électroniques* affectés au contrôle des accès électroniques sont situés à l'intérieur ~~de l'actif~~ du même actif que le ou les *actifs électroniques BES* à impact faible et ~~qu'il hérite~~qu'ils héritent des mêmes mesures de contrôle ~~d'accès~~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 ~~afin d'éviter~~de manière à éviter une documentation redondante des mêmes mesures.

L'entité responsable est libre de choisir les méthodes ~~à utiliser~~utilisées pour ~~atteindre~~réaliser l'objectif de ~~contrôler l'accès physique~~ 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, ~~ou encore aux *LEAP*, s'il en existe~~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*. ~~Il n'est pas exigé d'avoir des programmes d'autorisation des utilisateurs et des listes d'utilisateurs autorisés à un accès physique, bien que ces mesures soient à envisager pour répondre à l'objectif de sécurité.~~

L'objectif ~~visé~~de sécurité est de contrôler l'accès physique d'après les besoins déterminés par l'entité responsable. ~~Les besoins peuvent~~Le besoin d'accès physique peut être ~~documentés~~documenté au niveau des politiques ~~d'accès au site ou aux systèmes, y compris les *LEAP*. L'exigence n'oblige pas~~ ; 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.). ~~Il~~L'intention de l'équipe de rédaction n'est pas de rendre nécessaire ~~d'avoir~~ une surveillance pour chaque *système électronique BES* à

impact faible, mais ~~la~~plutôt une surveillance ~~doit être~~ au niveau approprié pour ~~atteindre~~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 ~~exige~~demande la mise en place ~~de protections périmétriques~~ d'un contrôle des accès électroniques pour ~~les~~tout actif comportant un ou des *systèmes électroniques BES* à impact faible ~~lorsque ceux-ci ont~~s'il existe une communication ~~bidirectionnelle~~ par protocole routable ou une *connectivité par lien commuté* ~~avec~~entre un ou des ~~appareils~~ *actifs électroniques* situés à l'extérieur de ~~l'actif dans lequel se trouvent des *systèmes électroniques BES* à impact faible. Les protections périmétriques contrôlent les communications soit vers un~~ cet actif ~~comportant~~et un ou des *systèmes électroniques BES* à impact faible~~, soit vers les *systèmes*~~ situés à l'intérieur de cet actif. Ce contrôle des accès électroniques ~~*BES*~~vise à ~~impact faible eux-mêmes, afin de~~ réduire les risques associés à une communication non~~-~~ contrôlée ~~au moyen de~~ utilisant des protocoles routables ou ~~d'une~~une *connectivité par lien commuté*. ~~Le terme « contrôle des accès électroniques » est employé dans son sens général, soit celui de contrôle passif des accès, et non dans~~

Dans le ~~sens technique particulier qui évoque~~ contexte de la ~~mise en œuvre de mécanismes d'authentification, d'autorisation~~section 3.1 de l'annexe 1, il est à noter que l'obligation de restreindre les accès électroniques entrants et ~~d'audit.~~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 ~~n'est pas obligée d'établir une communication *LERC* ou un *LEAP* en l'absence de communication bidirectionnelle~~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 ~~ou de *connectivité par lien commuté* ; dans un tel cas, l'entité peut documenter l'absence d'une telle communication dans son ou ses plans de cybersécurité visant les actifs à impact faible~~.

~~Les termes définis *LERC* et *LEAP* sont utilisés pour éviter toute confusion avec des termes semblables associés aux *systèmes électroniques BES à* impact moyen ou élevé (par exemple « *connectivité externe routable* » ou « *point d'accès électronique* »). Afin de mettre les normes à l'abri des changements et des complications technologiques à l'avenir, la définition de *LERC* exclut nommément « les communications point à point~~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 ~~entre~~, 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 ~~actifs de poste de transport comportant des *systèmes*~~accès électroniques ~~*BES* à impact faible », comme la messagerie CEI 61850. Les~~. Cette exemption ne s'applique pas aux communications ~~ainsi exclues~~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 ~~celles des *centres*~~vraiment sensibles aux délais créés par les mesures de contrôle~~, mais plutôt celles entre les dispositifs~~ des accès électroniques ~~intelligents eux-mêmes.~~. 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 ~~un *LEAP*. Cette exception~~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 ~~empêcher~~entraver le recours futur à de telles fonctions afin d'améliorer la fiabilité au motif qu'elles utiliseraient un protocole routable.

~~Lorsqu'il s'agit de déterminer si un *système électronique BES* à impact faible comporte une *LERC*, il convient de se référer à la définition de ce terme : « accès interactif direct amorcé par l'utilisateur ou connexion directe entre appareils, vers un ou des *systèmes électroniques BES* à impact faible à partir d'un *actif électronique* situé à l'extérieur de l'actif qui comporte ce ou ces *systèmes électroniques BES* à impact faible, au moyen d'une liaison bidirectionnelle utilisant un protocole routable ». Dans cette définition, les mots « direct » et « directe » servent à indiquer~~

Mis en fo

Mis en fo

qu'il y a une *LERC* si une personne utilise un autre appareil situé à l'extérieur de l'actif qui comporte le *système électronique BES* à impact faible, et que cette personne peut se connecter (pour ouvrir une session, configurer, lire, interagir, etc.) avec le *système électronique BES* à impact faible au moyen d'une seule session bidirectionnelle avec protocole routable de bout en bout, même s'il y a conversion entre une liaison série et un protocole routable. Une *LERC* existe aussi dans le cas inverse où la personne utilise le *système électronique BES* à impact faible et se connecte à un appareil situé à l'extérieur de l'actif comportant des *systèmes électroniques BES* à impact faible, au moyen d'une seule session bidirectionnelle avec protocole routable de bout en bout. En outre, l'expression « liaison directe entre appareils » indique qu'il y a une *LERC* si l'entité responsable a des appareils qui sont situés à l'extérieur de l'actif comportant le *système électronique BES* à impact faible et qui établissent une communication bidirectionnelle avec protocole routable avec le *système électronique BES* à impact faible, en accès entrant ou sortant.

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

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

Mis en fo

Mis en fo

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

~~Exemples non limitatifs de contrôles d'accès adéquats :~~

- ~~Toute *LERC* de l'actif franchit un *LEAP* qui applique des autorisations d'accès entrant et sortant explicites, ou une méthode équivalente par laquelle les liaisons entrantes et sortantes sont limitées aux seuls éléments (adresses IP, ports, services, etc.) que l'entité responsable juge nécessaires.~~
- ~~Comme l'illustre le modèle de référence 1 ci-dessous, le *système électronique BES* à impact faible comporte un pare-feu hôte qui contrôle les accès entrants et sortants. Dans ce modèle, il est également possible que le pare-feu hôte soit situé dans un *actif électronique* hors *BES*. Le but recherché est que le pare-feu hôte contrôle les accès entrants et sortants entre le *système électronique BES* à impact faible et l'actif électronique situé dans le réseau d'entreprise.~~
- ~~Dans le modèle de référence 5 ci-dessous, un *actif électronique* hors *BES* est interposé entre le *système électronique BES* à impact faible situé dans le réseau du poste électrique et l'*actif électronique* situé dans le réseau d'entreprise. Le but recherché est que l'*actif électronique* hors *BES* assure une « coupure de protocole », de sorte que l'accès au *système électronique BES* à impact faible se fasse seulement à partir de l'*actif électronique* hors *BES* situé à l'intérieur de l'actif comportant le *système électronique BES* à impact faible.~~

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

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

Lorsqu'il s'agit de déterminer si un protocole routable est utilisé en entrée ou en sortie de l'actif comportant le ou les *systèmes électroniques BES* à impact faible, l'entité responsable dispose d'une certaine latitude. Une approche possible consiste pour l'entité responsable à définir une « frontière électronique » pour l'actif comportant un ou des *systèmes électroniques BES* à impact faible. Il ne s'agit pas ici d'un *périmètre de sécurité électronique*, mais d'une démarcation où l'on constate une communication par protocole routable, en entrée ou en sortie de l'actif en question, entre un *système électronique BES* à impact faible situé à l'intérieur de cet actif et un ou des *actifs électroniques* situés à l'extérieur de cet actif, et donc le besoin d'un contrôle des accès électroniques. Cette frontière électronique peut varier selon le type d'actif (*centre de contrôle*, poste électrique, ressource de production, etc.) et les particularités

de sa configuration. Si l'entité responsable adopte cette approche, elle doit définir la « frontière électronique » de façon que le ou les *systèmes électroniques BES* à impact faible présents dans l'actif soient situés à l'intérieur de cette frontière. Cet exercice vise strictement à établir quelles communications par protocole routable et quels réseaux sont internes ou locaux par rapport à l'actif et lesquels sont externes ou situés à l'extérieur de l'actif.

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

Détermination des contrôles des accès électroniques

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

Schémas conceptuels

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

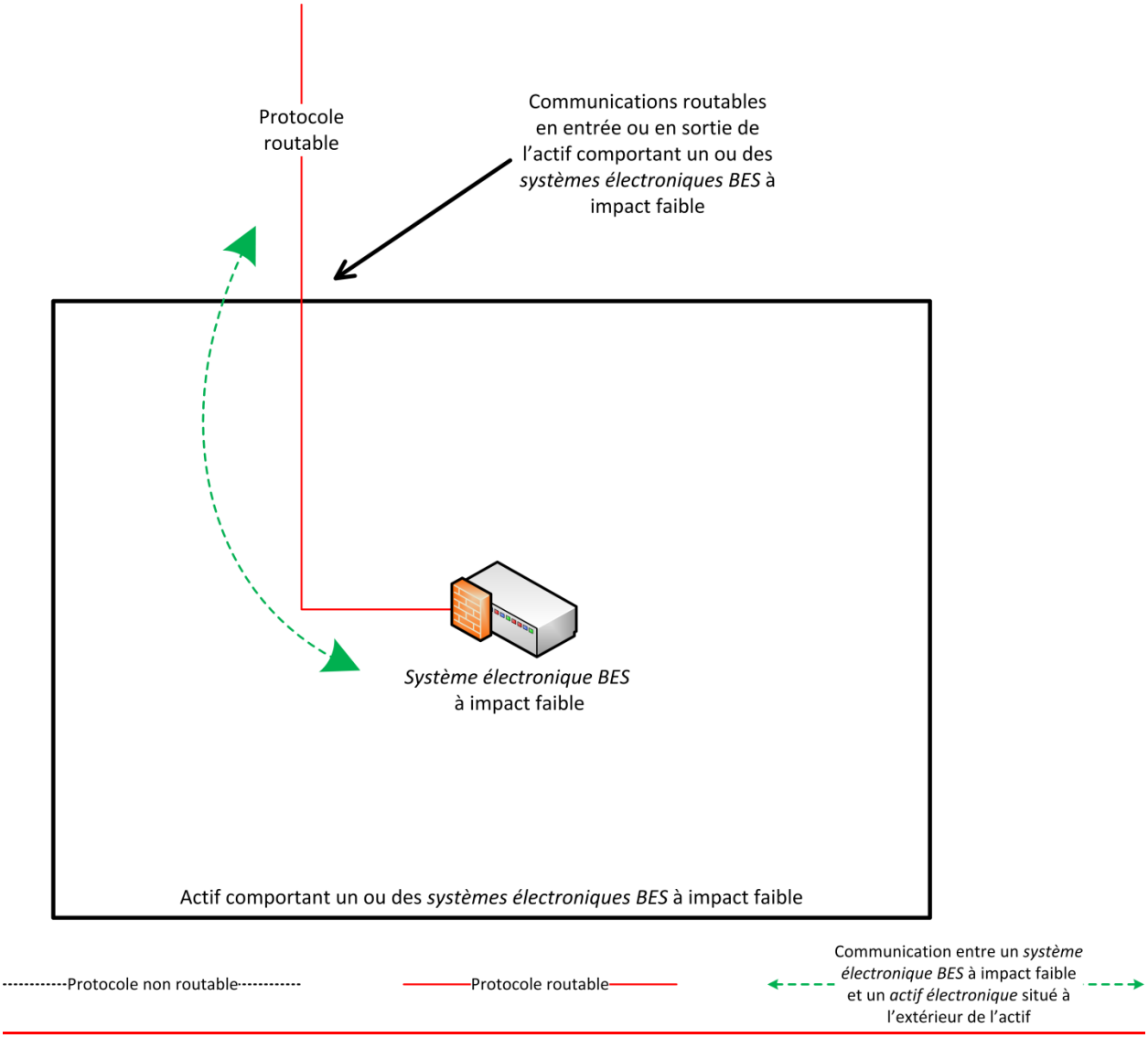
REMARQUES :

- Ces schémas ne représentent pas la totalité des concepts applicables.

- La même légende est utilisée pour tous les schémas ; cependant, chaque schéma ne comporte pas nécessairement tous les éléments de la légende.

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

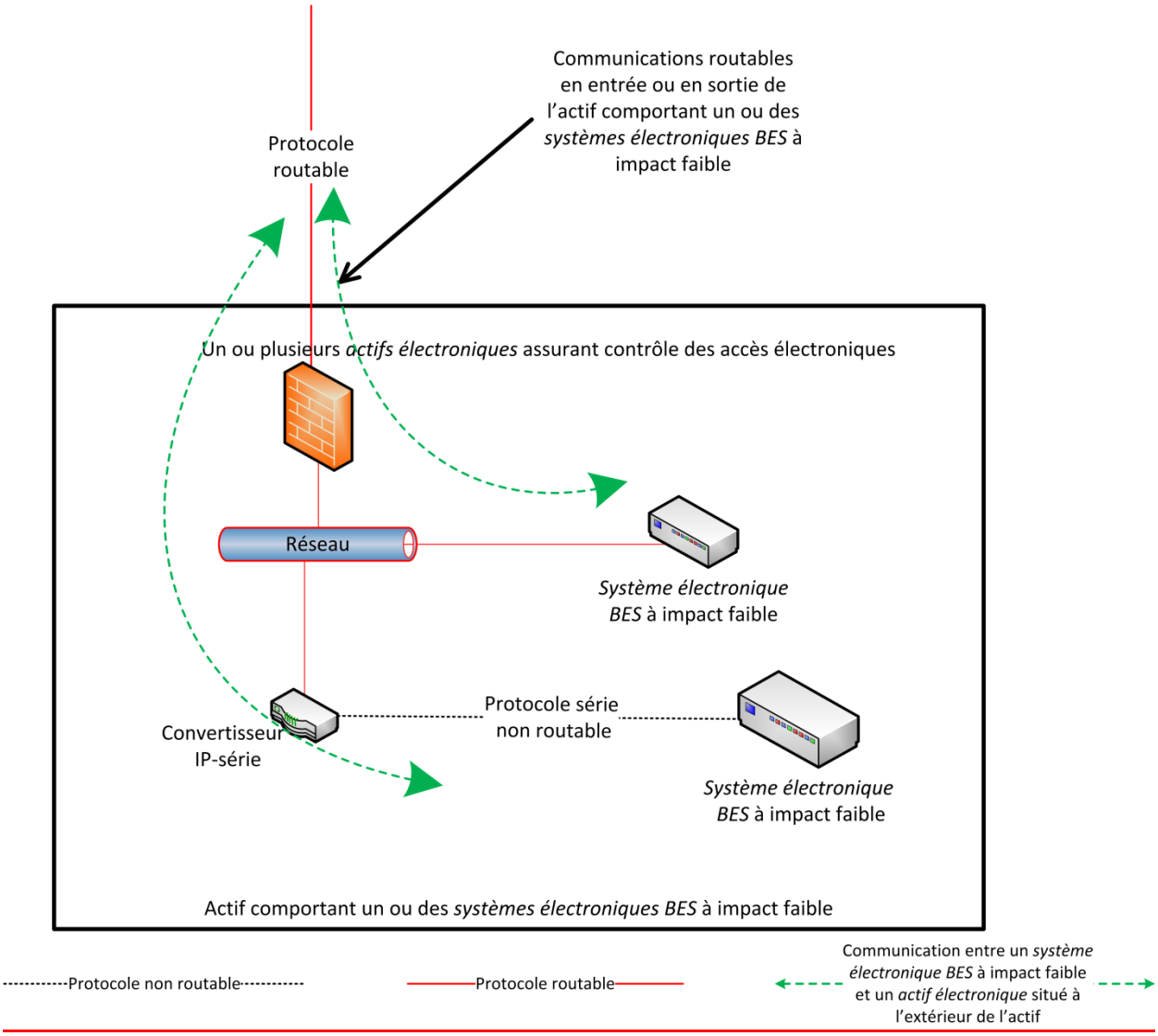
L'entité responsable peut opter pour une technologie de pare-feu hôte implantée dans le ou les *systèmes électroniques BES* à impact faible afin de gérer les autorisations d'accès électronique en les limitant aux accès entrants et sortants nécessaires entre le ou les *systèmes électroniques BES* à impact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



Modèle de référence 1

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

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

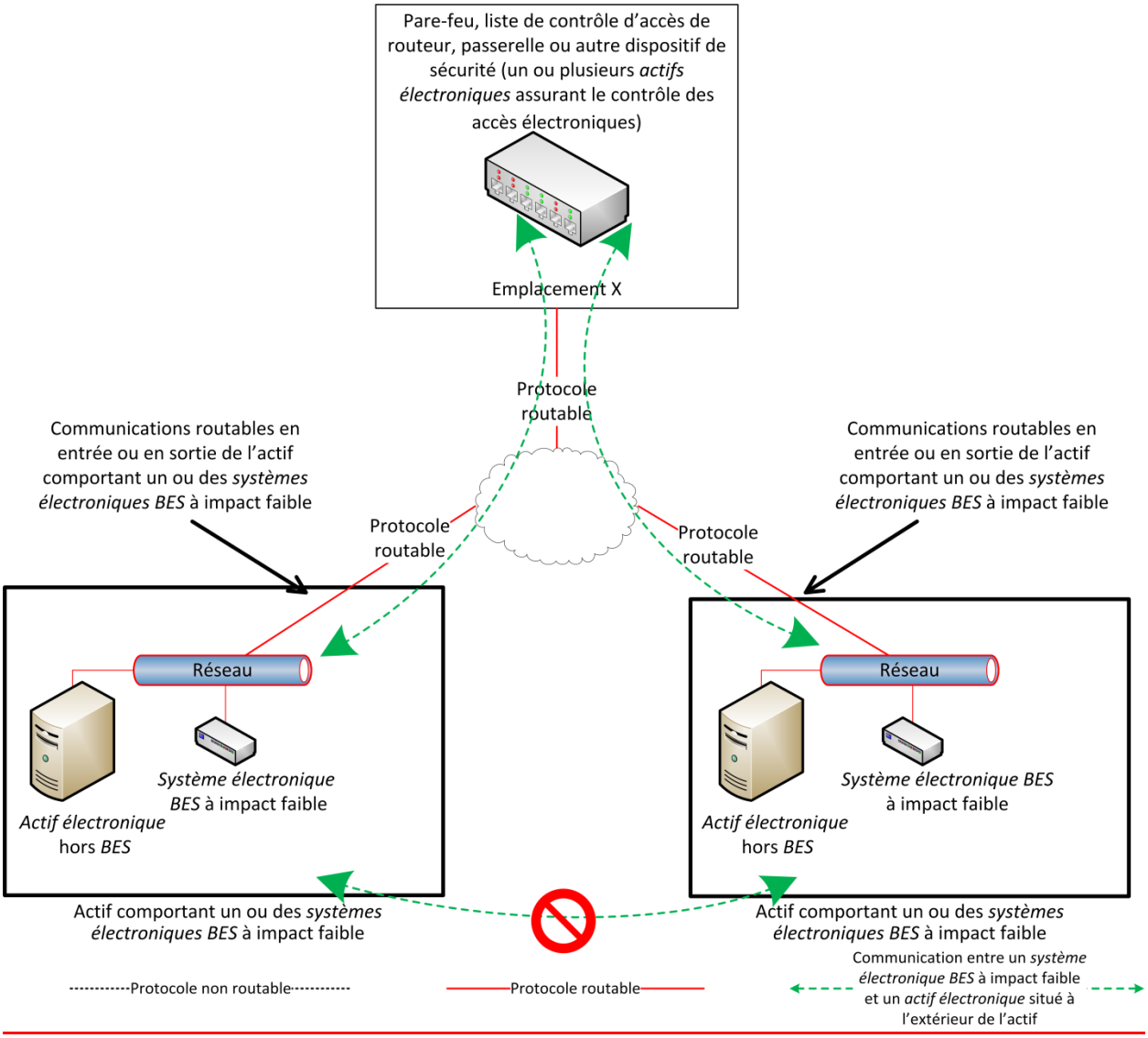


Modèle de référence 2

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

L'entité responsable peut opter pour un dispositif de sécurité situé à un emplacement centralisé, qui peut ou non être situé dans un autre actif comportant un ou des *systèmes électroniques BES* à impact faible. Le contrôle des accès électroniques ne réside pas nécessairement à l'intérieur de l'actif comportant le ou les *systèmes électroniques BES* à impact faible. Un dispositif de sécurité est en place à l'« emplacement X » pour assurer le contrôle des accès électroniques en autorisant uniquement les accès entrants et sortants par protocole routable nécessaires entre le ou les *systèmes électroniques BES* à impact faible et le ou les *actifs électroniques* situés à l'extérieur de chaque actif comportant un ou des *systèmes électroniques BES* à impact faible. Il faut prendre soin que chacun des accès électroniques entre les actifs transite bien par le ou les *actifs électroniques* désignés par l'entité responsable pour assurer le contrôle des accès électroniques à l'emplacement centralisé. Lorsque les autorisations sont

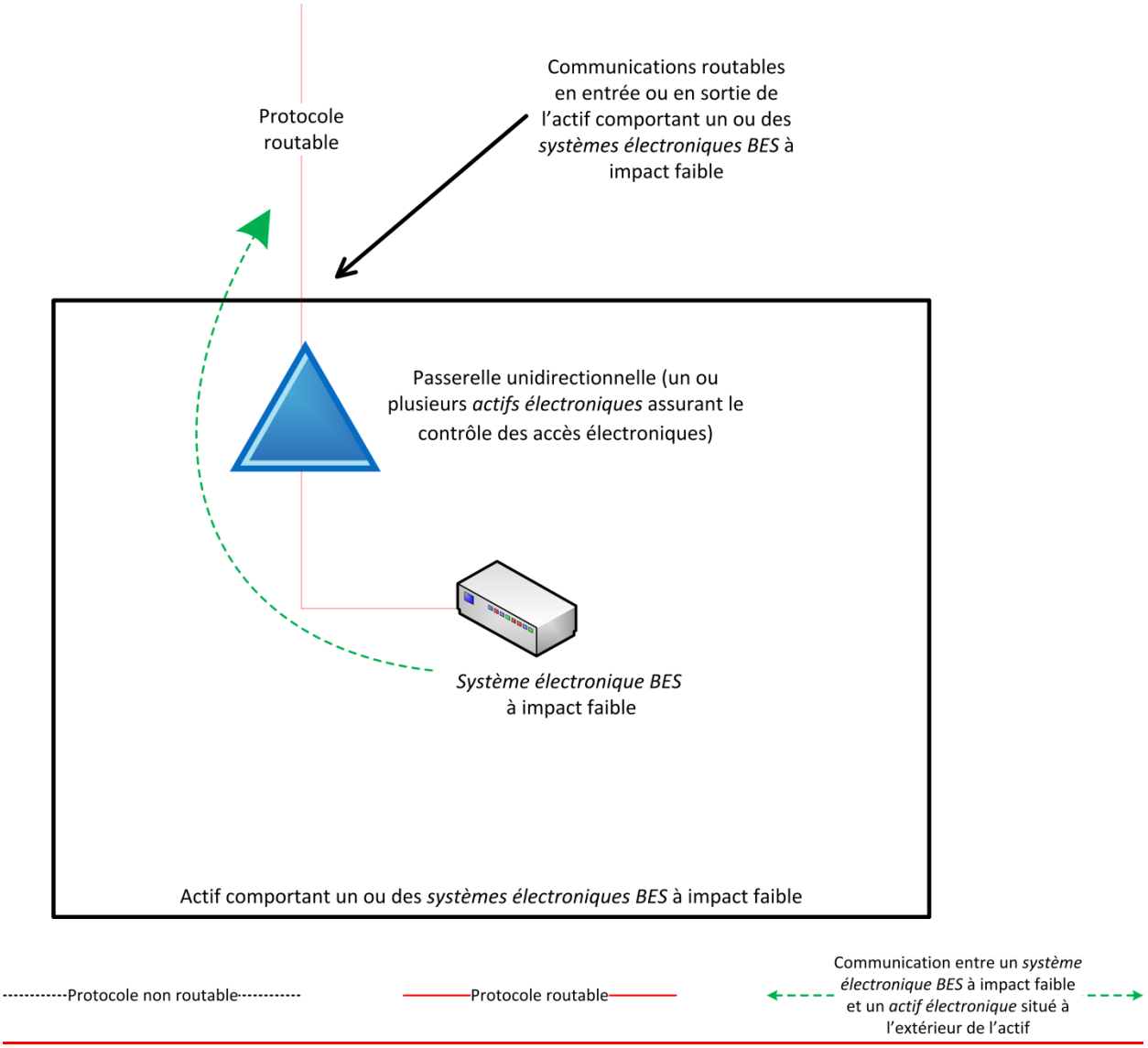
mises en œuvre au moyen de listes de contrôle d'accès, l'entité responsable peut restreindre les communications en spécifiant des adresses ou des plages d'adresses d'origine et de destination. L'entité responsable peut aussi restreindre les communications en spécifiant des ports ou des services, compte tenu de la capacité du dispositif de contrôle des accès électroniques, du ou des *systèmes électroniques BES* à impact faible ou des applications.



Modèle de référence 3

Modèle de référence 4 – Passerelle unidirectionnelle

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

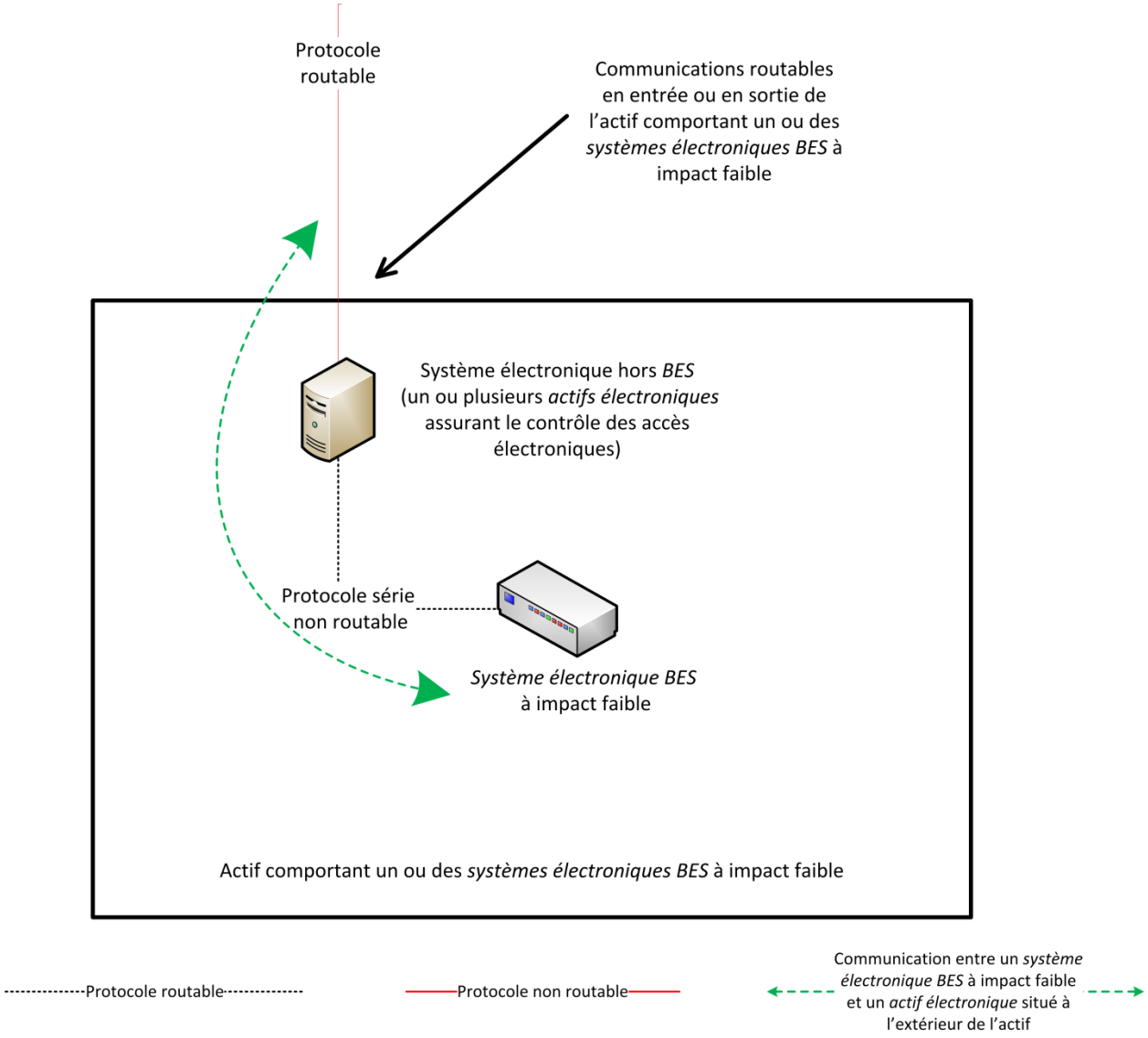


Modèle de référence 4

Modèle de référence 5 – Authentification de l'utilisateur

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

à partir du *système électronique BES* à impact faible. Cette configuration peut être avantageuse si les seules communications prévues se font par accès interactif commandé par l'utilisateur.

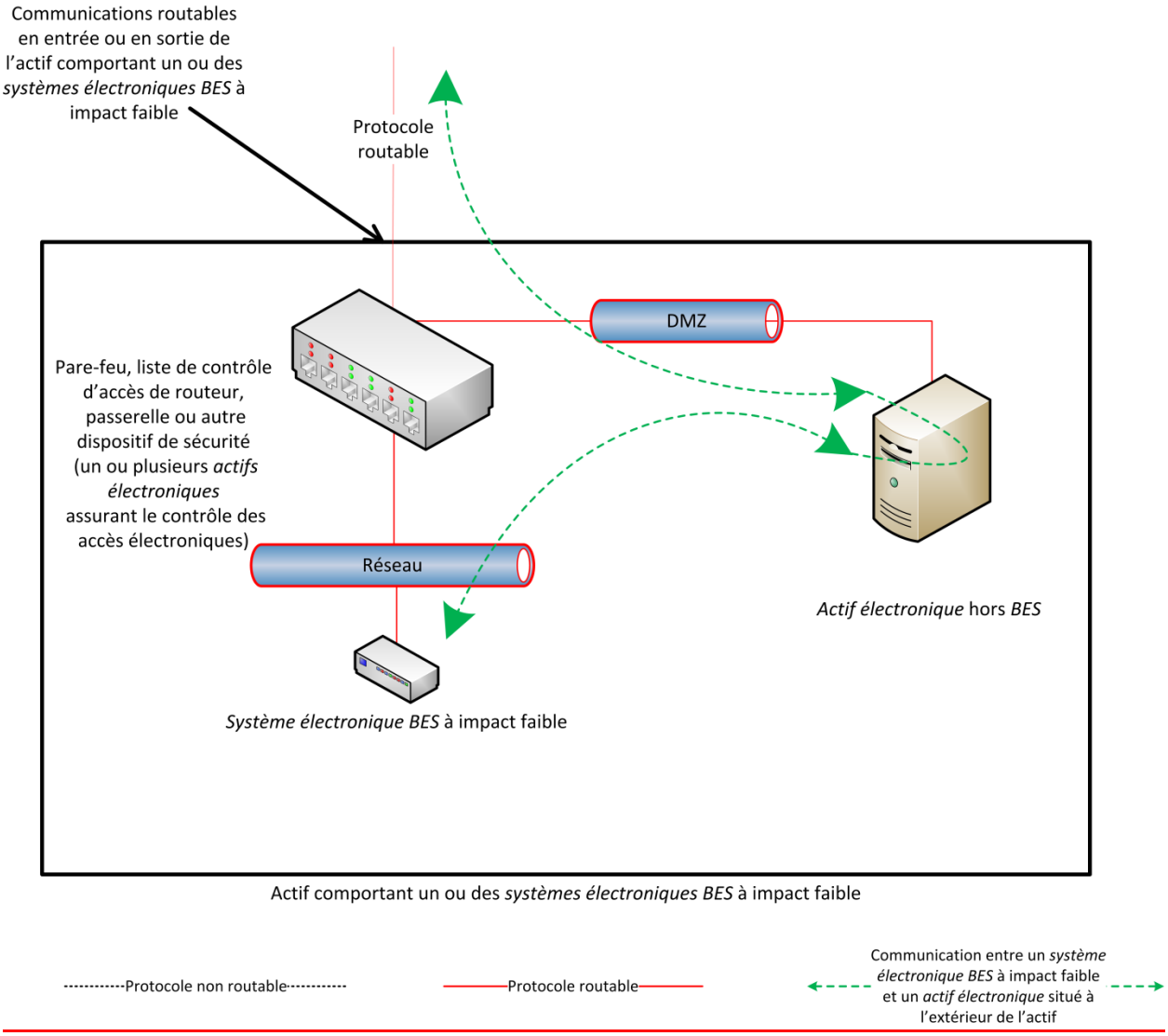


Modèle de référence 5

Modèle de référence 6 – Accès indirect

Dans la mise en place des mesures de contrôle des accès électroniques, l'entité responsable peut constater qu'il existe un accès indirect entre un *système électronique BES* à impact faible et un *actif électronique* situé à l'extérieur de l'actif comportant ce *système électronique BES* à impact faible, par l'intermédiaire d'un *actif électronique* hors *BES* situé à l'intérieur de l'actif en question. Cet accès indirect répond au critère d'une communication entre un *système électronique BES* à impact faible et un *actif électronique* situé à l'extérieur de l'actif comportant ce *système électronique BES* à impact faible. Dans ce modèle de référence, l'entité responsable devra mettre en place un contrôle des accès électroniques qui autorise uniquement les accès électroniques entrants et sortants nécessaires pour le *système électronique BES* à impact faible.

Comme pour les autres modèles de référence présentés, l'accès électronique dans ce modèle de référence est contrôlé au moyen du dispositif de sécurité qui restreint les communications entrantes ou sortantes de l'actif.

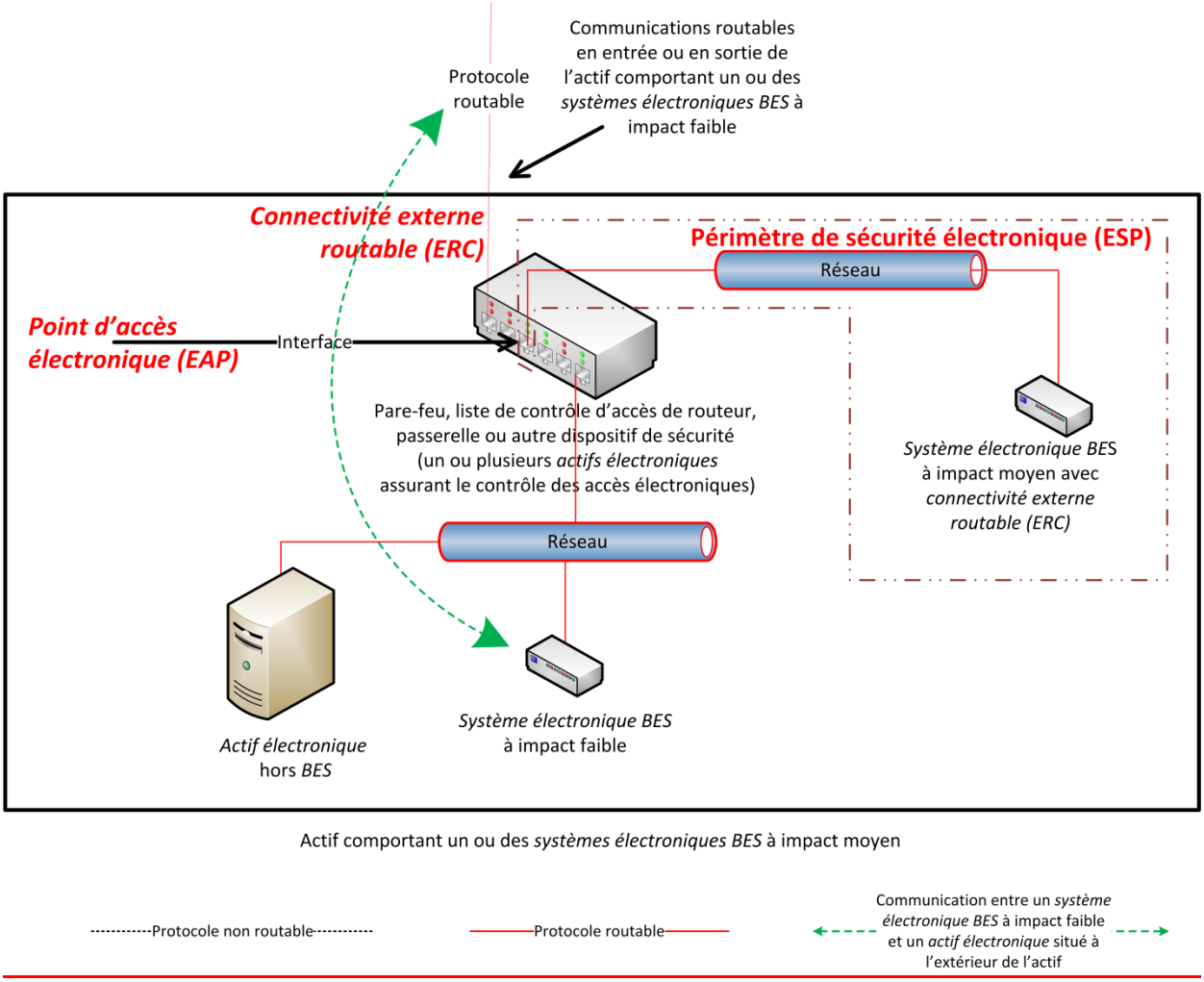


Modèle de référence 6

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

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

celle d'*EACMS* à impact moyen et celle de contrôle des accès électroniques pour un actif comportant des *systèmes électroniques BES* à impact faible.



Modèle de référence 7

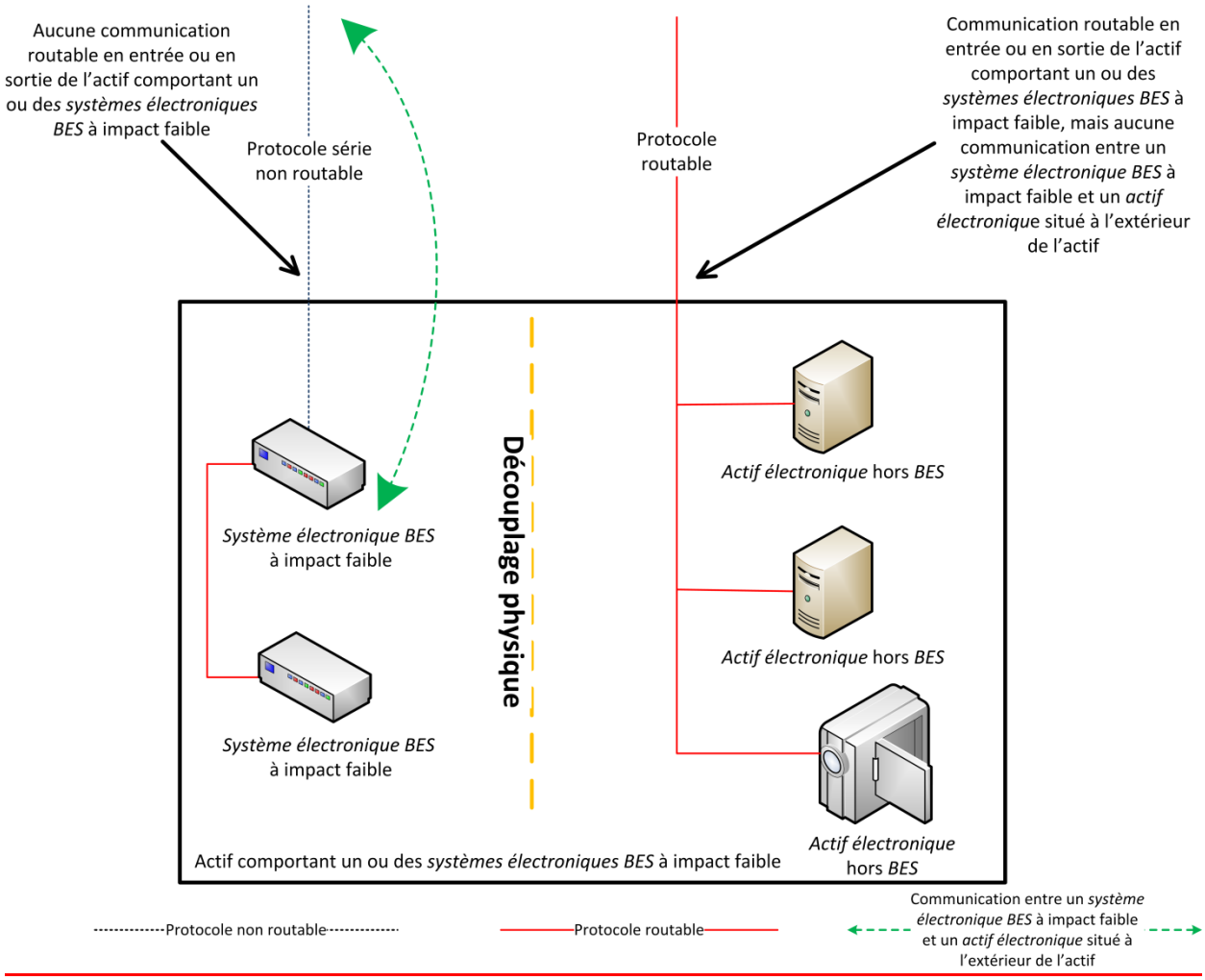
Modèle de référence 8 – Découplage physique et communication série non routable – Contrôle des accès électroniques non exigé

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

1) Étant donné le découplage physique (communément appelé « *air gap* » en anglais) du ou des *systèmes électroniques BES* à impact faible par rapport aux communications entrantes ou sortantes par protocole routable de l'actif comportant le ou les *systèmes électroniques BES* à impact faible, le contrôle des accès électroniques n'est pas exigé.
2) Étant donné que la communication avec les *systèmes électroniques BES* à impact faible à partir d'un *actif électronique* situé à l'extérieur de l'actif comportant ces *systèmes électroniques BES* à impact faible utilise uniquement un protocole série non routable au

point d'entrée ou de sortie de cette communication, le contrôle des accès électroniques n'est pas exigé.

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

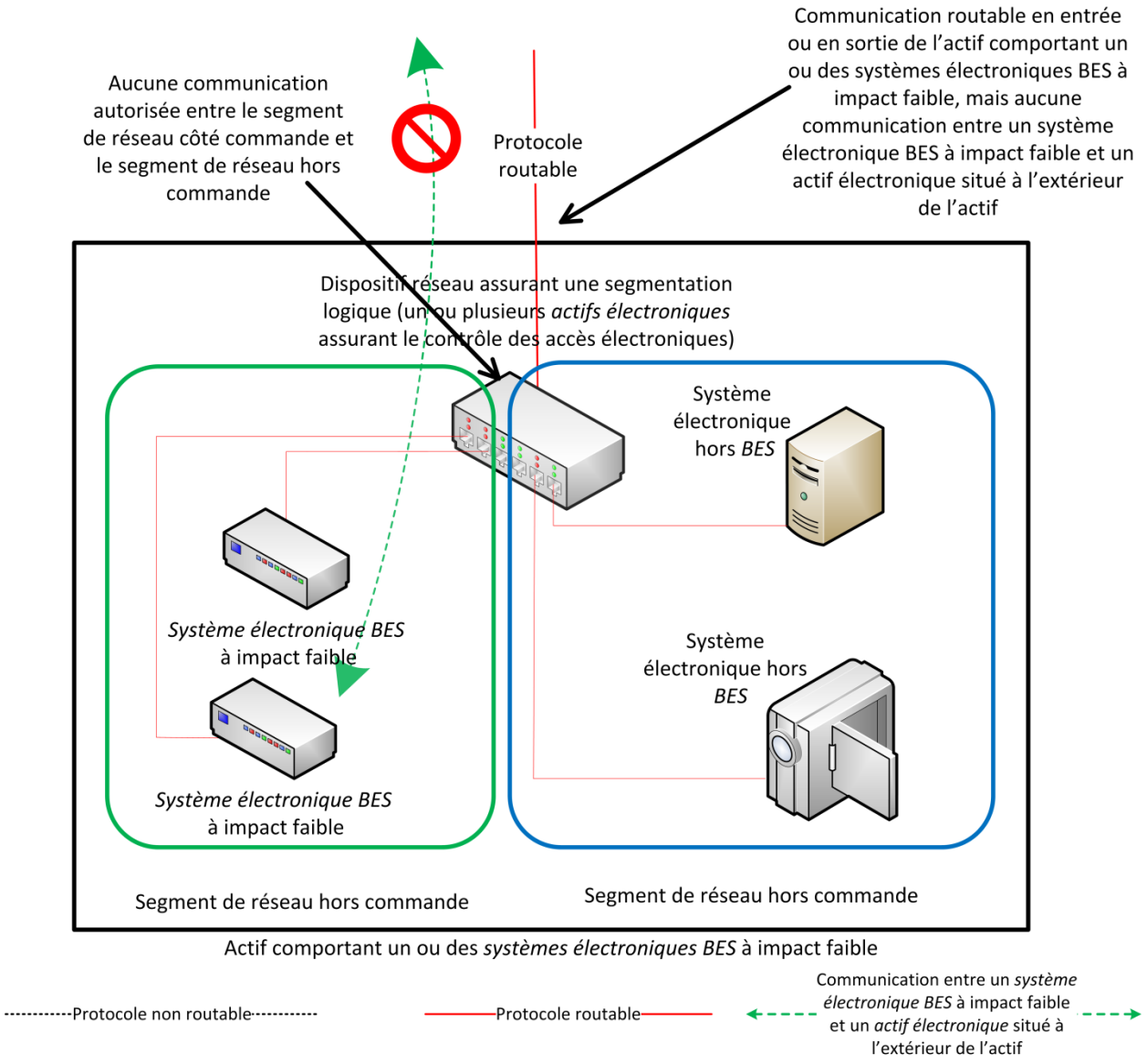


Modèle de référence 8

Modèle de référence 9 – Isolement logique – Contrôle des accès électroniques non exigé

Dans ce modèle de référence, les critères de la section 3.1 de l'annexe 1 concernant l'obligation de contrôler les accès électroniques ne sont pas remplis. L'entité responsable a isolé logiquement le ou les *systèmes électroniques BES* à impact faible par rapport aux communications entrantes ou sortantes par protocole routable de l'actif comportant le ou les *systèmes électroniques BES* à impact faible. La segmentation logique du réseau dans ce modèle de référence n'autorise aucune communication entre un *système électronique BES* à impact faible et un *actif électronique* situé à l'extérieur de l'actif. En outre, il n'existe aucun accès

indirect parce que les *actifs électroniques* hors *BES* capables de communiquer avec l'extérieur de l'actif sont strictement empêchés de communiquer vers le ou les *systèmes électroniques BES* à impact faible. Le ou les *systèmes électroniques BES* à impact faible sont confinés dans un segment de réseau isolé par des contrôles électroniques qui empêchent toute communication entrante ou sortante par protocole routable avec l'extérieur de ce segment de réseau ; ainsi, les communications des *systèmes électroniques BES* à impact faible ne sortent jamais de l'actif au moyen d'un protocole routable.



Modèle de référence 9

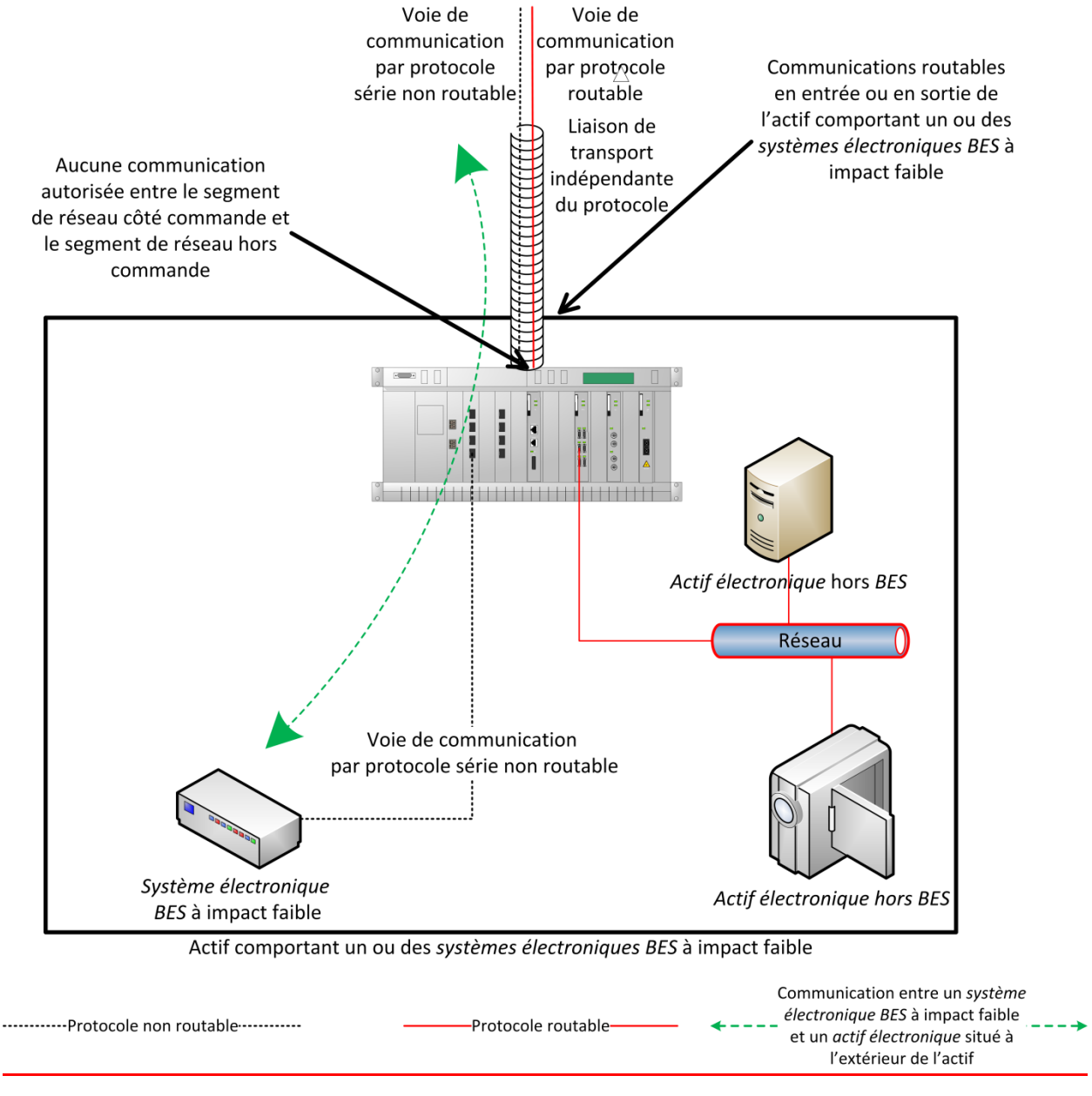
Modèle de référence 10 – Communication série non routable empruntant une voie isolée dans un réseau de transport non routable – Contrôle des accès électroniques non exigé

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

Mis en fo

Mis en fo

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

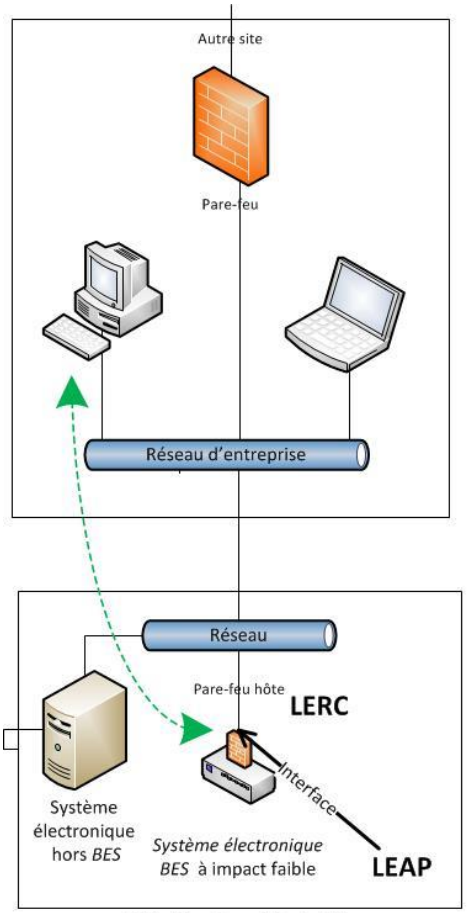
- La *connectivité par lien commuté* avec un *système électronique BES* à impact faible autorise seulement les appels sortants (pas de réponse automatique) vers un numéro préprogrammé pour l'envoi de données. S'il y a *connectivité par lien commuté* entrante, elle est réalisée par un modem à fonction 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 ~~actif comporte une *LERC*, car un~~ *système électronique BES* à ~~l'intérieur de cet actif~~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 ~~modèle de référence 5, si l'on utilise seulement des~~cas de cartes d'interface à double résidence ou multiréseaux sans ~~désactiver le~~désactivation du réacheminement IP dans l'*actif électronique* hors *BES* à l'intérieur de la zone DMZ afin d'assurer une coupure entre le ~~*système électronique*~~ou les *systèmes électroniques* *BES* à impact faible et le réseau ~~d'entreprise~~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'un autre appareil~~d'autres dispositifs de sécurité pour cet *actif électronique* hors *BES*.

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



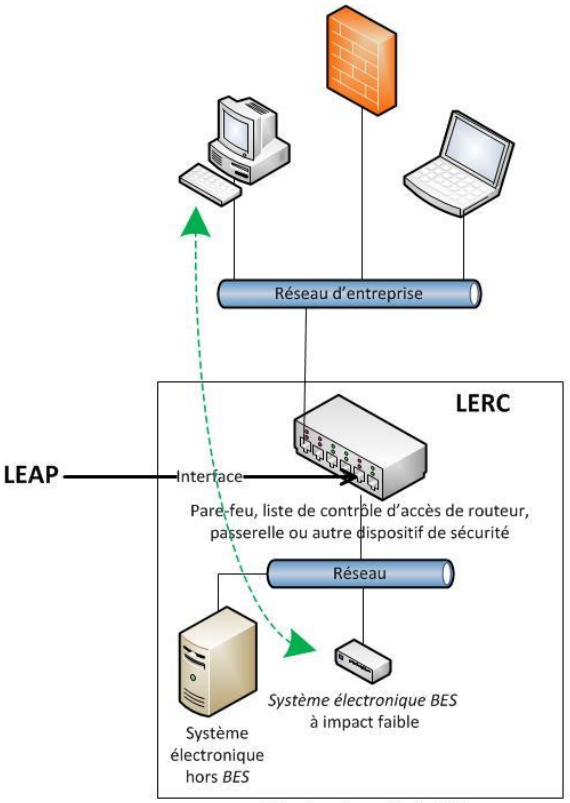
Périmètre des actifs du *BES*

MODÈLE DE RÉFÉRENCE - 1

Le *système électronique BES* à impact faible est accessible à partir d'un *actif électronique* situé à l'extérieur de l'actif dans lequel se trouve le *système électronique BES* à impact faible ; il y a donc une LERC. Un pare-feu hôte, configuré à même le *système électronique BES* à impact faible, sert de *LEAP* et autorise seulement les accès électroniques nécessaires au *système électronique BES* à impact faible.

Mis en fo

Mis en fo

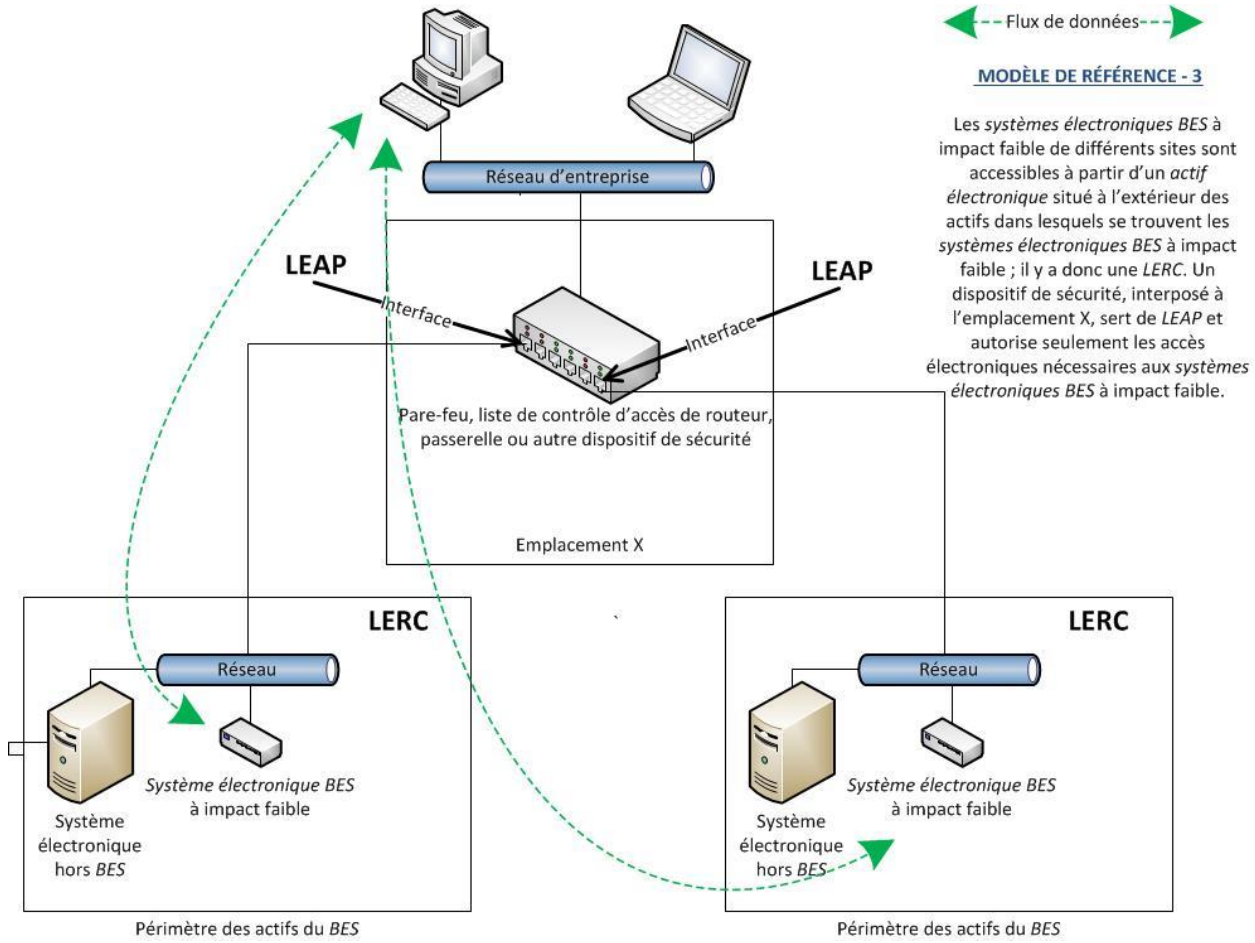


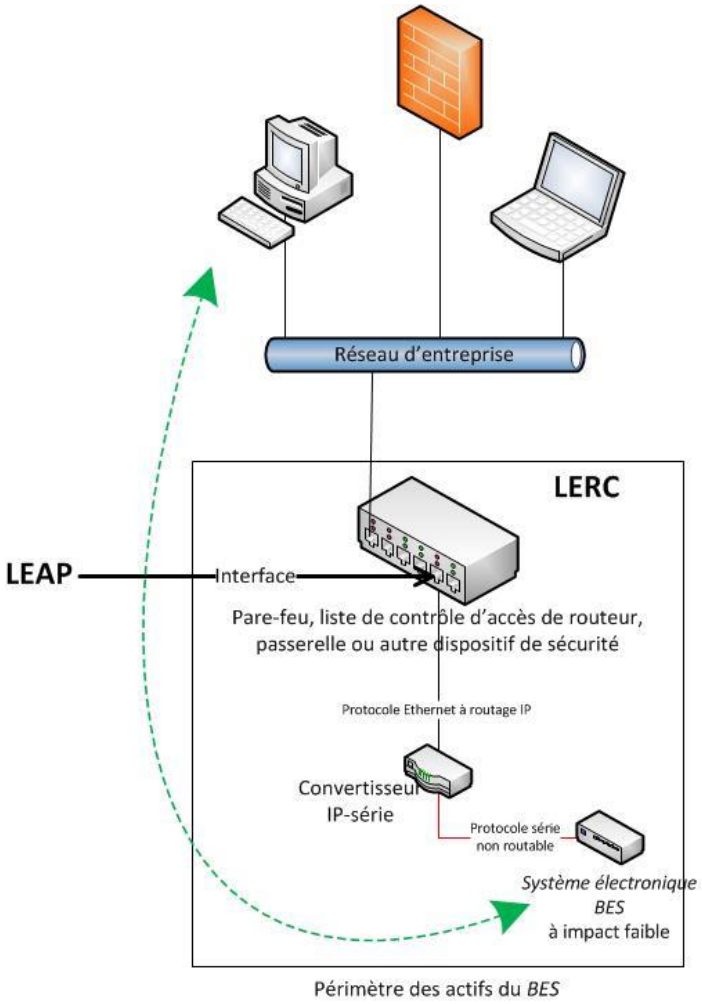
MODÈLE DE RÉFÉRENCE - 2

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

Mis en fo

Mis en fo





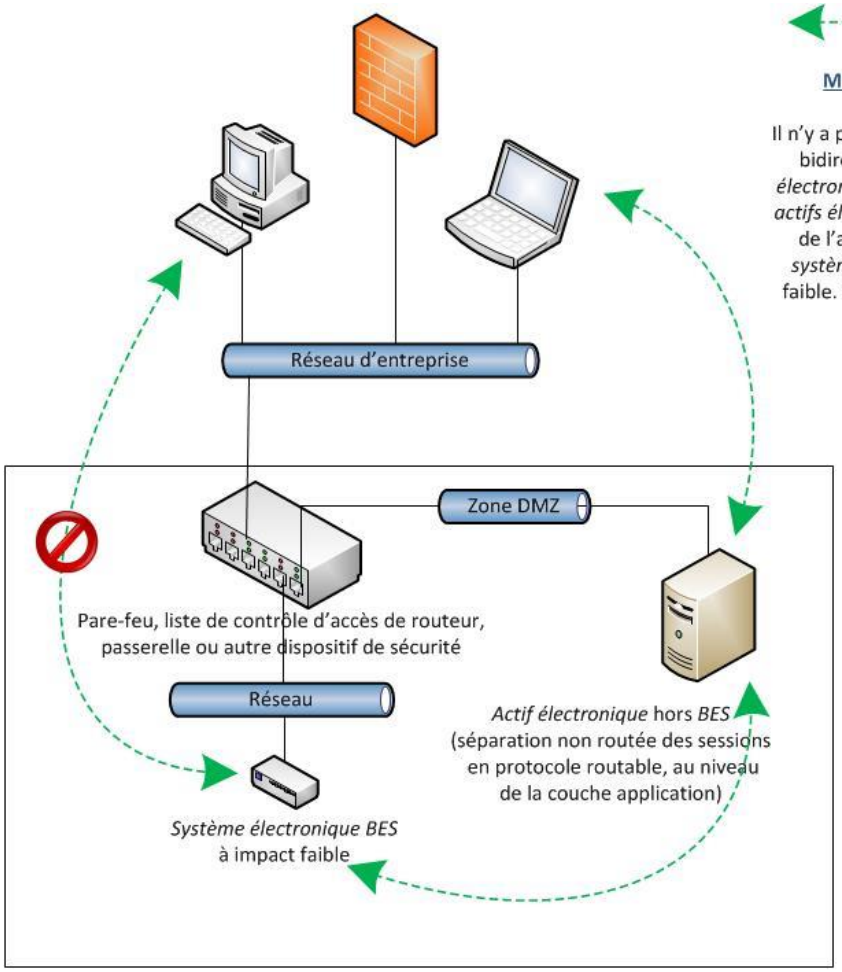
Flux de données

MODÈLE DE RÉFÉRENCE - 4

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

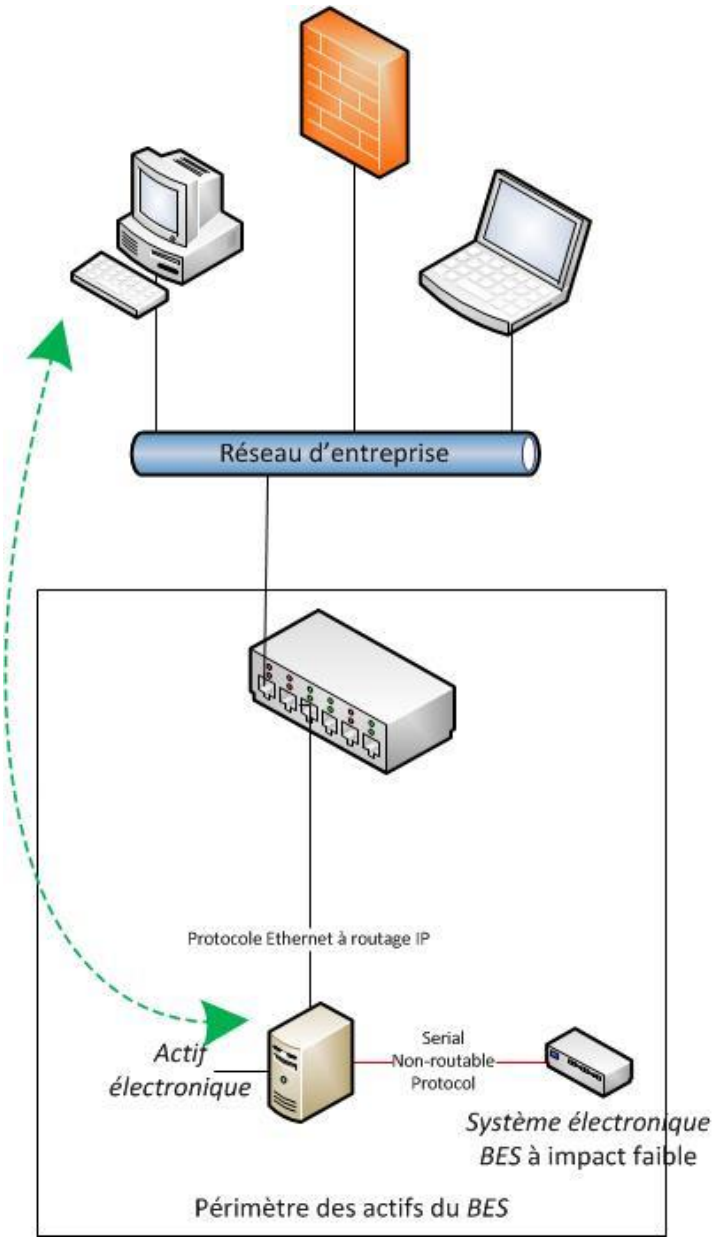
Mis en fo

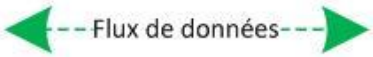
Mis en fo



Mis en fo

Mis en fo



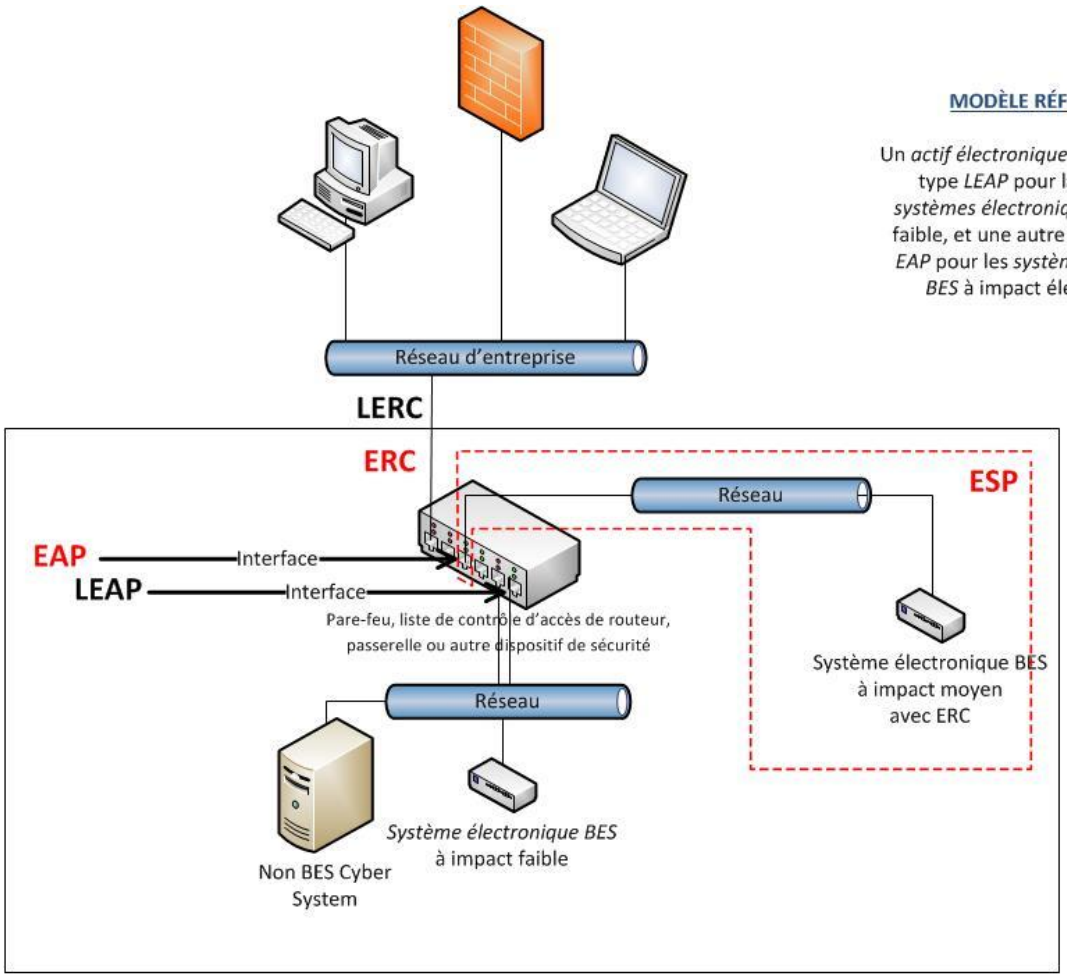


MODÈLE DE RÉFÉRENCE - 6

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

Mis en fo

Mis en fo



Périmètre des actifs du *BES*

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

Mis en fo

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.

~~Les~~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 ~~un~~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*.

Mis en fo

Mis en fo

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

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

Atténuation des risques liés à l'introduction de programmes malveillants

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

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

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

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

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

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

Quant à la méthode choisie pour atténuer le risque lié à l'introduction de programmes malveillants, l'entité est libre d'appliquer cette méthode soit en permanence, soit à la demande. Exemple d'application permanente : gérer la solution antivirus pour le dispositif dans

le cadre d'une solution de sécurité des points terminaux avec des mises à jour régulières des signatures ou des séquences de code, des balayages de système programmés, etc. Par contre, dans le cas de dispositifs utilisés assez rarement et dont les signatures ou les séquences de code ne sont pas tenues à jour, l'entité peut gérer ces dispositifs à la demande seulement, en demandant une mise à jour des signatures ou des séquences de code et un balayage du dispositif avant sa connexion afin de vérifier qu'il est exempt de programme malveillant.

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

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

- Les logiciels antivirus, avec mises à jour manuelles ou systématiques des signatures ou des séquences de code, offrent une certaine souplesse pour gérer les *actifs électroniques temporaires* en déployant des logiciels antivirus ou des outils de sécurité des points terminaux qui assurent une mise à jour programmée des signatures ou des séquences de code. Par ailleurs, pour les dispositifs dont la connexion non régulière ne leur permet pas de recevoir des mises à jour programmées, l'entité peut choisir de mettre à jour les signatures ou les séquences de code et de balayer l'*actif électronique temporaire* avant sa connexion afin de confirmer l'absence de programme malveillant.
- La liste blanche d'applications consiste à autoriser seulement les applications et les processus nécessaires pour l'*actif électronique temporaire*. Ce procédé réduit la possibilité que des programmes malveillants puissent s'exécuter sur l'*actif électronique temporaire* et attaquer l'*actif électronique BES* ou le *système électronique BES*.
- Si elles utilisent des méthodes autres que celles énumérées, les entités doivent documenter comment ces méthodes réalisent l'objectif d'atténuer le risque lié à l'introduction de programmes malveillants.

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

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

La section 5 reconnaît également que l'entité responsable n'a aucun contrôle direct sur les *actifs électroniques temporaires* qui sont gérés par une tierce partie. Cependant, même dans ce cas, l'entité responsable est tenue de s'assurer que des moyens ont été déployés pour atténuer

le risque lié à l'introduction de programmes malveillants dans des *systèmes électroniques BES* à impact faible à partir d'*actifs électroniques temporaires* qui ne relèvent pas de sa gestion. La section 5 demande aux entités d'examiner les pratiques de sécurité des tierces parties relativement aux *actifs électroniques temporaires* afin de réaliser l'objectif de l'exigence. La mention « avant de connecter l'*actif électronique temporaire* » vise à obliger l'entité responsable à effectuer l'examen avant la première connexion de l'*actif électronique temporaire* afin de réaliser l'objectif d'atténuer le risque lié à l'introduction de programmes malveillants. L'équipe de rédaction ne souhaite pas obliger l'entité responsable à effectuer un examen pour chaque connexion d'un *actif électronique temporaire* si l'entité responsable a déjà établi que cet *actif électronique temporaire* est conforme à l'objectif de sécurité. Il est exclu d'exiger une écriture de registre pour chaque connexion d'un *actif électronique temporaire* à un *actif électronique BES*.

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

Section 5.2 : Les entités doivent documenter et mettre en œuvre leurs processus d'atténuation du risque lié à l'introduction des programmes malveillants, comportant une ou plusieurs des mesures d'atténuation indiquées ci-après.

- Procéder à un examen des niveaux de tenue à jour des logiciels antivirus ainsi que des signatures ou des séquences de code afin de s'assurer que ces niveaux permettent à l'entité responsable d'atténuer adéquatement le risque lié à l'introduction de programmes malveillants dans un système visé.

- Procéder à un examen des processus antivirus ou de sécurisation des points terminaux de la tierce partie afin de s'assurer que ces processus permettent à l'entité responsable

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

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.

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*

Mis en fo

Mis en fo

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-~~6~~7 reste pratiquement inchangé par rapport aux versions antérieures de la norme. La description spécifique du *cadre supérieur CIP* est maintenant comprise dans les termes définis, ce qui évite de l'expliciter dans le texte de la norme de fiabilité et de devoir créer des renvois à la norme dans d'autres documents. Le *cadre supérieur CIP* est appelé à jouer un rôle clé pour assurer la planification stratégique appropriée, la sensibilisation des dirigeants et du conseil d'administration ~~et~~ainsi que la gouvernance générale du programme.

Exigence E4

Comme l'indique la justification de l'exigence E4 de la norme CIP-003-~~6~~7, cette exigence vise à démontrer une chaîne d'autorité et d'imputabilité claire en matière de sécurité. L'intention de l'équipe de rédaction (SDT) était de ne pas imposer une structure organisationnelle particulière ; elle laisse plutôt à l'entité responsable une ample marge de manœuvre pour adapter cette exigence à sa structure organisationnelle existante. Une entité responsable peut satisfaire à cette exigence au moyen d'un seul ou de plusieurs documents de délégation. L'entité responsable peut aussi déléguer les pouvoirs de délégation eux-mêmes pour augmenter la souplesse de mise en œuvre dans son organisation. Dans un tel cas, les délégations peuvent être dispersées dans de multiples documents, pourvu que l'ensemble de ces documents décrive une chaîne d'autorité claire qui remonte au *cadre supérieur CIP*. De plus, le *cadre supérieur CIP* pourrait aussi choisir de ne déléguer aucun pouvoir et de respecter cette exigence sans recourir à des documents de délégation.

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

Justification

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

Justification de l'exigence E1

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

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

Justification de l'exigence E2

En réponse à l'ordonnance 791 de la FERC, l'exigence E2 demande aux entités d'élaborer et de mettre en œuvre des plans de cybersécurité afin d'atteindre des objectifs précis en matière de mécanismes de sécurité pour leurs actifs comportant un ou des *systèmes électroniques BES* à impact faible. Les plans de cybersécurité couvrent ~~quatre~~cinq thèmes : 1) la sensibilisation à la cybersécurité ; 2) les mesures de sécurité physique ; 3) le contrôle des accès électroniques ; ~~et~~ 4) l'intervention en cas d'*incident de cybersécurité*~~.~~ ; 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 ~~la partie~~ 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 ~~la SDT~~l'équipe de rédaction à clarifier l'exigence en matière de délégation, de manière que la chaîne d'autorité en question soit claire et que les délégations de pouvoir soient dûment documentées.

A. Introduction

1. Title: Cyber Security — BES Cyber System Categorization

2. Number: CIP-002-5.1a

3. Purpose: To identify and categorize BES Cyber Systems and their associated BES Cyber Assets for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES. Identification and categorization of BES Cyber Systems support appropriate protection against compromises that could lead to misoperation or instability in the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1. Balancing Authority

4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1. Each underfrequency load shedding (UFLS) or undervoltage load shedding (UVLS) system that:

4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2. Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Interchange Coordinator or Interchange Authority

4.1.6. Reliability Coordinator

4.1.7. Transmission Operator

4.1.8. Transmission Owner

4.2. **Facilities:** For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-002-5.1a:

4.2.3.1. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

5. Effective Dates:

1. **24 Months Minimum** – CIP-002-5.1a shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval.
2. In those jurisdictions where no regulatory approval is required CIP-002-5.1a shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

6. Background:

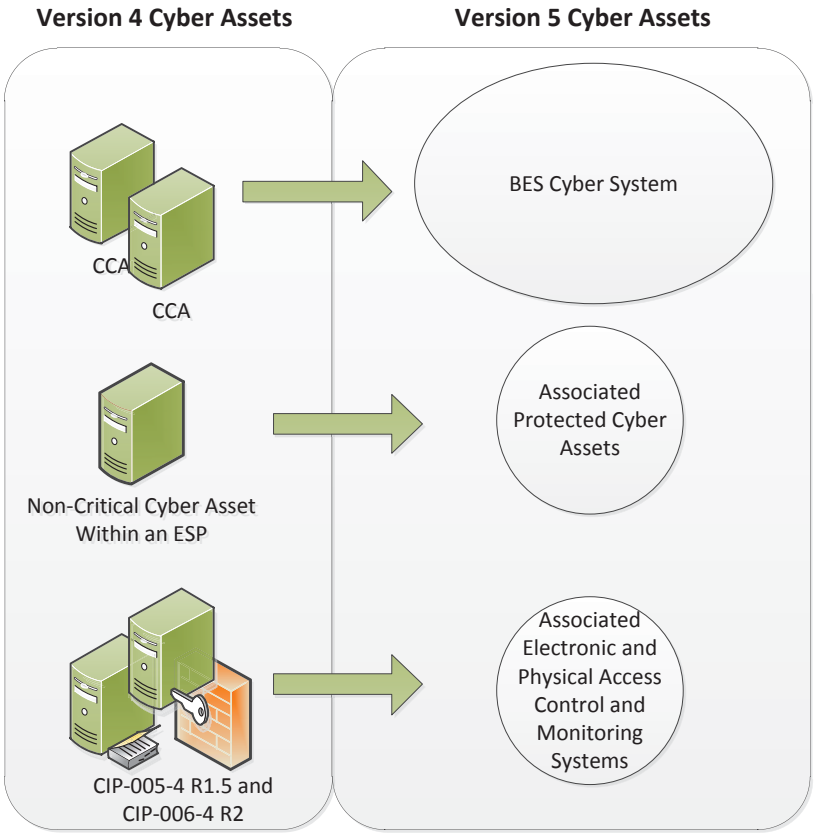
This standard provides "bright-line" criteria for applicable Responsible Entities to categorize their BES Cyber Systems based on the impact of their associated Facilities, systems, and equipment, which, if destroyed, degraded, misused, or otherwise rendered unavailable, would affect the reliable operation of the Bulk Electric System. Several concepts provide the basis for the approach to the standard.

Throughout the standards, unless otherwise stated, bulleted items in the requirements are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section and the criteria in Attachment 1 of CIP-002 use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

BES Cyber Systems

One of the fundamental differences between Versions 4 and 5 of the CIP Cyber Security Standards is the shift from identifying Critical Cyber Assets to identifying BES Cyber Systems. This change results from the drafting team's review of the NIST Risk Management Framework and the use of an analogous term "information system" as the target for categorizing and applying security controls.



In transitioning from Version 4 to Version 5, a BES Cyber System can be viewed simply as a grouping of Critical Cyber Assets (as that term is used in Version 4). The CIP Cyber Security Standards use the "BES Cyber System" term primarily to provide a higher level for referencing the object of a requirement. For example, it becomes possible to apply requirements dealing with recovery and malware protection to a grouping rather than individual Cyber Assets, and it becomes clearer in the requirement that malware protection applies to the system as a whole and may not be necessary for every individual device to comply.

Another reason for using the term "BES Cyber System" is to provide a convenient level at which a Responsible Entity can organize their documented implementation of the requirements and compliance evidence. Responsible Entities can use the well-developed concept of a *security plan* for each BES Cyber System to document the programs, processes, and plans in place to comply with security requirements.

It is left up to the Responsible Entity to determine the level of granularity at which to identify a BES Cyber System within the qualifications in the definition of BES Cyber System. For example, the Responsible Entity might choose to view an entire plant control system as a single BES Cyber System, or it might choose to view certain components of the plant control system as distinct BES Cyber Systems. The Responsible Entity should take into consideration the operational environment and

scope of management when defining the BES Cyber System boundary in order to maximize efficiency in secure operations. Defining the boundary too tightly may result in redundant paperwork and authorizations, while defining the boundary too broadly could make the secure operation of the BES Cyber System difficult to monitor and assess.

Reliable Operation of the BES

The scope of the CIP Cyber Security Standards is restricted to BES Cyber Systems that would impact the reliable operation of the BES. In order to identify BES Cyber Systems, Responsible Entities determine whether the BES Cyber Systems perform or support any BES reliability function according to those reliability tasks identified for their reliability function and the corresponding functional entity's responsibilities as defined in its relationships with other functional entities in the NERC Functional Model. This ensures that the *initial* scope for consideration includes only those BES Cyber Systems and their associated BES Cyber Assets that perform or support the reliable operation of the BES. The definition of BES Cyber Asset provides the basis for this scoping.

Real-time Operations

One characteristic of the BES Cyber Asset is a real-time scoping characteristic. The time horizon that is significant for BES Cyber Systems and BES Cyber Assets subject to the application of these Version 5 CIP Cyber Security Standards is defined as that which is material to real-time operations for the reliable operation of the BES. To provide a better defined time horizon than "Real-time," BES Cyber Assets are those Cyber Assets that, if rendered unavailable, degraded, or misused, would adversely impact the reliable operation of the BES within 15 minutes of the activation or exercise of the compromise. This time window must not include in its consideration the activation of redundant BES Cyber Assets or BES Cyber Systems: from the cyber security standpoint, redundancy does not mitigate cyber security vulnerabilities.

Categorization Criteria

The criteria defined in Attachment 1 are used to categorize BES Cyber Systems into impact categories. Requirement 1 only requires the discrete identification of BES Cyber Systems for those in the high impact and medium impact categories. All BES Cyber Systems for Facilities not included in Attachment 1 – Impact Rating Criteria, Criteria 1.1 to 1.4 and Criteria 2.1 to 2.11 default to be low impact.

This general process of categorization of BES Cyber Systems based on impact on the reliable operation of the BES is consistent with risk management approaches for the purpose of application of cyber security requirements in the remainder of the Version 5 CIP Cyber Security Standards.

Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets that are associated with BES Cyber Systems

BES Cyber Systems have associated Cyber Assets, which, if compromised, pose a threat to the BES Cyber System by virtue of: (a) their location within the Electronic Security Perimeter (Protected Cyber Assets), or (b) the security control function they perform (Electronic Access Control or Monitoring Systems and Physical Access Control Systems). These Cyber Assets include:

Electronic Access Control or Monitoring Systems ("EACMS") – Examples include: Electronic Access Points, Intermediate Systems, authentication servers (e.g., RADIUS servers, Active Directory servers, Certificate Authorities), security event monitoring systems, and intrusion detection systems.

Physical Access Control Systems ("PACS")– Examples include: authentication servers, card systems, and badge control systems.

Protected Cyber Assets ("PCA") – Examples may include, to the extent they are within the ESP: file servers, ftp servers, time servers, LAN switches, networked printers, digital fault recorders, and emission monitoring systems.

B. Requirements and Measures

R1. Each Responsible Entity shall implement a process that considers each of the following assets for purposes of parts 1.1 through 1.3: *[Violation Risk Factor: High][Time Horizon: Operations Planning]*

- **i.** Control Centers and backup Control Centers;
- **ii.** Transmission stations and substations;
- **iii.** Generation resources;
- **iv.** Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements;
- **v.** Special Protection Systems that support the reliable operation of the Bulk Electric System; and
- **vi.** For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above.

1.1. Identify each of the high impact BES Cyber Systems according to Attachment 1, Section 1, if any, at each asset;

1.2. Identify each of the medium impact BES Cyber Systems according to Attachment 1, Section 2, if any, at each asset; and

1.3. Identify each asset that contains a low impact BES Cyber System according to Attachment 1, Section 3, if any (a discrete list of low impact BES Cyber Systems is not required).

M1. Acceptable evidence includes, but is not limited to, dated electronic or physical lists required by Requirement R1, and Parts 1.1 and 1.2.

R2. The Responsible Entity shall: *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

2.1 Review the identifications in Requirement R1 and its parts (and update them if there are changes identified) at least once every 15 calendar months, even if it has no identified items in Requirement R1, and

2.2 Have its CIP Senior Manager or delegate approve the identifications required by Requirement R1 at least once every 15 calendar months, even if it has no identified items in Requirement R1.

M2. Acceptable evidence includes, but is not limited to, electronic or physical dated records to demonstrate that the Responsible Entity has reviewed and updated, where necessary, the identifications required in Requirement R1 and its parts, and has had its CIP Senior Manager or delegate approve the identifications required in Requirement R1 and its parts at least once every 15 calendar months, even if it has none identified in Requirement R1 and its parts, as required by Requirement R2.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.

- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information

- None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-002-5.1a)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	Operations Planning	High	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, five percent or fewer BES assets have not been considered according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, 2 or fewer BES assets in Requirement R1, have not been considered according to Requirement R1; OR For Responsible Entities with more than a total of 100 high and medium impact BES Cyber	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, more than five percent but less than or equal to 10 percent of BES assets have not been considered, according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, more than two, but fewer than or equal to four BES assets in Requirement R1, have not been considered according to Requirement R1; OR	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, more than 10 percent but less than or equal to 15 percent of BES assets have not been considered, according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, more than four, but fewer than or equal to six BES assets in Requirement R1, have not been considered according to Requirement R1; OR	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, more than 15 percent of BES assets have not been considered, according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, more than six BES assets in Requirement R1, have not been considered according to Requirement R1; OR For Responsible Entities with more than a total of 100 high and medium impact BES Cyber

R #	Time Horizon	VRF	Violation Severity Levels (CIP-002-5.1a)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Systems, five percent or fewer of identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, five or fewer identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact BES Cyber	For Responsible Entities with more than a total of 100 high and medium impact BES Cyber Systems, more than five percent but less than or equal to 10 percent of identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high and medium impact and BES Cyber Systems, more than five but less than or equal to 10 identified BES Cyber Systems have not been categorized or have been incorrectly	For Responsible Entities with more than a total of 100 high or medium impact BES Cyber Systems, more than 10 percent but less than or equal to 15 percent of identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high or medium impact and BES Cyber Assets, more than 10 but less than or equal to 15 identified BES Cyber Assets have not been categorized or have been incorrectly	Systems, more than 15 percent of identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, more than 15 identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact BES Cyber

R #	Time Horizon	VRF	Violation Severity Levels (CIP-002-5.1a)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Systems, five percent or fewer high or medium BES Cyber Systems have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, five or fewer high or medium BES Cyber Systems have not been identified.	categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact BES Cyber Systems, more than five percent but less than or equal to 10 percent high or medium BES Cyber Systems have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, more than five but less than or equal to 10 high or medium BES Cyber Systems have not been identified.	categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact BES Cyber Systems, more than 10 percent but less than or equal to 15 percent high or medium BES Cyber Systems have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, more than 10 but less than or equal to 15 high or medium BES Cyber Systems have not been identified.	Systems, more than 15 percent of high or medium impact BES Cyber Systems have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, more than 15 high or medium impact BES Cyber Systems have not been identified.

R #	Time Horizon	VRF	Violation Severity Levels (CIP-002-5.1a)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R2	Operations Planning	Lower	The Responsible Entity did not complete its review and update for the identification required for R1 within 15 calendar months but less than or equal to 16 calendar months of the previous review. (R2.1) OR The Responsible Entity did not complete its approval of the identifications required by R1 by the CIP Senior Manager or delegate according to Requirement R2 within 15 calendar months but less than or equal to 16 calendar months of the previous approval. (R2.2)	The Responsible Entity did not complete its review and update for the identification required for R1 within 16 calendar months but less than or equal to 17 calendar months of the previous review. (R2.1) OR The Responsible Entity failed to complete its approval of the identifications required by R1 by the CIP Senior Manager or delegate according to Requirement R2 within 16 calendar months but less than or equal to 17 calendar months of the previous approval. (R2.2)	The Responsible Entity did not complete its review and update for the identification required for R1 within 17 calendar months but less than or equal to 18 calendar months of the previous review. (R2.1) OR The Responsible Entity failed to complete its approval of the identifications required by R1 by the CIP Senior Manager or delegate according to Requirement R2 within 17 calendar months but less than or equal to 18 calendar months of the previous approval. (R2.2)	The Responsible Entity did not complete its review and update for the identification required for R1 within 18 calendar months of the previous review. (R2.1) OR The Responsible Entity failed to complete its approval of the identifications required by R1 by the CIP Senior Manager or delegate according to Requirement R2 within 18 calendar months of the previous approval. (R2.2)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

CIP-002-5.1a - Attachment 1

Impact Rating Criteria

The criteria defined in Attachment 1 do not constitute stand-alone compliance requirements, but are criteria characterizing the level of impact and are referenced by requirements.

1. High Impact Rating (H)

Each BES Cyber System used by and located at any of the following:

1.1. Each Control Center or backup Control Center used to perform the functional obligations of the Reliability Coordinator.

1.2. Each Control Center or backup Control Center used to perform the functional obligations of the Balancing Authority: 1) for generation equal to or greater than an aggregate of 3000 MW in a single Interconnection, or 2) for one or more of the assets that meet criterion 2.3, 2.6, or 2.9.

1.3. Each Control Center or backup Control Center used to perform the functional obligations of the Transmission Operator for one or more of the assets that meet criterion 2.2, 2.4, 2.5, 2.7, 2.8, 2.9, or 2.10.

1.4 Each Control Center or backup Control Center used to perform the functional obligations of the Generator Operator for one or more of the assets that meet criterion 2.1, 2.3, 2.6, or 2.9.

2. Medium Impact Rating (M)

Each BES Cyber System, not included in Section 1 above, associated with any of the following:

2.1. Commissioned generation, by each group of generating units at a single plant location, with an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection. For each group of generating units, the only BES Cyber Systems that meet this criterion are those shared BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection.

2.2. Each BES reactive resource or group of resources at a single location (excluding generation Facilities) with an aggregate maximum Reactive Power nameplate rating of 1000 MVAR or greater (excluding those at generation Facilities). The only BES Cyber Systems that meet this criterion are those shared BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of resources that in aggregate equal or exceed 1000 MVAR.

2.3. Each generation Facility that its Planning Coordinator or Transmission Planner designates, and informs the Generator Owner or Generator Operator, as necessary to avoid an Adverse Reliability Impact in the planning horizon of more than one year.

2.4. Transmission Facilities operated at 500 kV or higher. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.

2.5. Transmission Facilities that are operating between 200 kV and 499 kV at a single station or substation, where the station or substation is connected at 200 kV or higher voltages to three or more other Transmission stations or substations and has an "aggregate weighted value" exceeding 3000 according to the table below. The "aggregate weighted value" for a single station or substation is determined by summing the "weight value per line" shown in the table below for each incoming and each outgoing BES Transmission Line that is connected to another Transmission station or substation. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.

Voltage Value of a Line	Weight Value per Line
less than 200 kV (not applicable)	(not applicable)
200 kV to 299 kV	700
300 kV to 499 kV	1300
500 kV and above	0

2.6. Generation at a single plant location or Transmission Facilities at a single station or substation location that are identified by its Reliability Coordinator, Planning Coordinator, or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.

2.7. Transmission Facilities identified as essential to meeting Nuclear Plant Interface Requirements.

2.8. Transmission Facilities, including generation interconnection Facilities, providing the generation interconnection required to connect generator output to the Transmission Systems that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of the generation Facilities identified by any Generator Owner as a result of its application of Attachment 1, criterion 2.1 or 2.3.

2.9. Each Special Protection System (SPS), Remedial Action Scheme (RAS), or automated switching System that operates BES Elements, that, if destroyed, degraded, misused or otherwise rendered unavailable, would cause one or more Interconnection Reliability Operating Limits (IROLs) violations for failure to operate as designed or cause a reduction in one or more IROLs if destroyed, degraded, misused, or otherwise rendered unavailable.

2.10. Each system or group of Elements that performs automatic Load shedding under a common control system, without human operator initiation, of 300 MW or more implementing undervoltage load shedding (UVLS) or underfrequency load shedding (UFLS) under a load shedding program that is subject to one or more requirements in a NERC or regional reliability standard.

2.11. Each Control Center or backup Control Center, not already included in High Impact Rating (H) above, used to perform the functional obligations of the Generator Operator for an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection.

2.12. Each Control Center or backup Control Center used to perform the functional obligations of the Transmission Operator not included in High Impact Rating (H), above.

2.13. Each Control Center or backup Control Center, not already included in High Impact Rating (H) above, used to perform the functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MW in a single Interconnection.

3. Low Impact Rating (L)

BES Cyber Systems not included in Sections 1 or 2 above that are associated with any of the following assets and that meet the applicability qualifications in Section 4 - Applicability, part 4.2 – Facilities, of this standard:

3.1. Control Centers and backup Control Centers.

3.2. Transmission stations and substations.

3.3. Generation resources.

3.4. Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements.

3.5. Special Protection Systems that support the reliable operation of the Bulk Electric System.

3.6. For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in section 4.1, that is subject to the requirements of the standard. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the qualified set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards. This section is especially significant in CIP-002-5.1a and represents the total scope of Facilities, systems, and equipment to which the criteria in Attachment 1 apply. This is important because it determines the balance of these Facilities, systems, and equipment that are Low Impact once those that qualify under the High and Medium Impact categories are filtered out.

For the purpose of identifying groups of Facilities, systems, and equipment, whether by location or otherwise, the Responsible Entity identifies assets as described in Requirement R1 of CIP-002-5.1a. This is a process familiar to Responsible Entities that have to comply with versions 1, 2, 3, and 4 of the CIP standards for Critical Assets. As in versions 1, 2, 3, and 4, Responsible Entities may use substations, generation plants, and Control Centers at single site locations as identifiers of these groups of Facilities, systems, and equipment.

CIP-002-5.1a

CIP-002-5.1a requires that applicable Responsible Entities categorize their BES Cyber Systems and associated BES Cyber Assets according to the criteria in Attachment 1. A BES Cyber Asset includes in its definition, "…that if rendered unavailable, degraded, or misused would, within 15 minutes adversely impact the reliable operation of the BES."

The following provides guidance that a Responsible Entity may use to identify the BES Cyber Systems that would be in scope. The concept of BES reliability operating service is useful in providing Responsible Entities with the option of a defined process for scoping those BES Cyber

Systems that would be subject to CIP-002-5.1a. The concept includes a number of named BES reliability operating services. These named services include:

Dynamic Response to BES conditions
Balancing Load and Generation
Controlling Frequency (Real Power)
Controlling Voltage (Reactive Power)
Managing Constraints
Monitoring & Control
Restoration of BES
Situational Awareness
Inter-Entity Real-Time Coordination and Communication

Responsibility for the reliable operation of the BES is spread across all Entity Registrations. Each entity registration has its own special contribution to reliable operations and the following discussion helps identify which entity registration, in the context of those functional entities to which these CIP standards apply, performs which reliability operating service, as a process to identify BES Cyber Systems that would be in scope. The following provides guidance for Responsible Entities to determine applicable reliability operations services according to their Function Registration type.

Entity Registration	RC	BA	TOP	TO	DP	GOP	GO
Dynamic Response		X	X	X	X	X	X
Balancing Load & Generation	X	X	X	X	X	X	X
Controlling Frequency		X				X	X
Controlling Voltage			X	X	X		X
Managing Constraints	X		X			X	
Monitoring and Control			X			X	
Restoration			X			X	
Situation Awareness	X	X	X			X	
Inter-Entity coordination	X	X	X	X		X	X

Dynamic Response

The Dynamic Response Operating Service includes those actions performed by BES Elements or subsystems which are automatically triggered to initiate a response to a BES condition. These actions are triggered by a single element or control device or a combination of these elements or devices in concert to perform an action or cause a condition in reaction to the triggering action or condition. The types of dynamic responses that may be considered as potentially having an impact on the BES are:

- Spinning reserves (contingency reserves)
  - Providing actual reserve generation when called upon (GO,GOP)
  - Monitoring that reserves are sufficient (BA)
- Governor Response
  - Control system used to actuate governor response (GO)
- Protection Systems (transmission & generation)
  - Lines, buses, transformers, generators (DP, TO, TOP, GO, GOP)
  - Zone protection for breaker failure (DP, TO, TOP)
  - Breaker protection (DP, TO, TOP)
  - Current, frequency, speed, phase (TO,TOP, GO,GOP)
- Special Protection Systems or Remedial Action Schemes
  - Sensors, relays, and breakers, possibly software (DP, TO, TOP)
- Under and Over Frequency relay protection (includes automatic load shedding)
  - Sensors, relays & breakers (DP)
- Under and Over Voltage relay protection (includes automatic load shedding)
  - Sensors, relays & breakers (DP)
- Power System Stabilizers (GO)

Balancing Load and Generation

The Balancing Load and Generation Operations Service includes activities, actions and conditions necessary for monitoring and controlling generation and load in the operations planning horizon and in real-time. Aspects of the Balancing Load and Generation function include, but are not limited to:

- Calculation of Area Control Error (ACE)
  - Field data sources (real time tie flows, frequency sources, time error, etc) (TO, TOP)
  - Software used to perform calculation (BA)
- Demand Response
  - Ability to identify load change need (BA)
  - Ability to implement load changes (TOP,DP)
- Manually Initiated Load shedding
  - Ability to identify load change need (BA)
  - Ability to implement load changes (TOP, DP)

- Non-spinning reserve (contingency reserve)
  - Know generation status, capability, ramp rate, start time (GO, BA)
  - Start units and provide energy (GOP)

Controlling Frequency (Real Power)

The Controlling Frequency Operations Service includes activities, actions and conditions which ensure, in real time, that frequency remains within bounds acceptable for the reliability or operability of the BES. Aspects of the Controlling Frequency function include, but are limited to:

- Generation Control (such as AGC)
  - ACE, current generator output, ramp rate, unit characteristics (BA, GOP, GO)
  - Software to calculate unit adjustments (BA)
  - Transmit adjustments to individual units (GOP)
  - Unit controls implementing adjustments (GOP)
- Regulation (regulating reserves)
  - Frequency source, schedule (BA)
  - Governor control system (GO)

Controlling Voltage (Reactive Power)

The Controlling Voltage Operations Service includes activities, actions and conditions which ensure, in real time, that voltage remains within bounds acceptable for the reliability or operability of the BES. Aspects of the Controlling Voltage function include, but are not limited to:

- Automatic Voltage Regulation (AVR)
  - Sensors, stator control system, feedback (GO)
- Capacitive resources
  - Status, control (manual or auto), feedback (TOP, TO,DP)
- Inductive resources (transformer tap changer, or inductors)
  - Status, control (manual or auto), feedback (TOP,TO,DP)
- Static VAR Compensators (SVC)
  - Status, computations, control (manual or auto), feedback (TOP, TO,DP)

Managing Constraints

Managing Constraints includes activities, actions and conditions that are necessary to ensure that elements of the BES operate within design limits and constraints established for the reliability and operability of the BES. Aspects of the Managing Constraints include, but are not limited to:

- Available Transfer Capability (ATC) (TOP)
- Interchange schedules (TOP, RC)
- Generation re-dispatch and unit commit (GOP)
- Identify and monitor SOL's & IROL's (TOP, RC)
- Identify and monitor Flow gates (TOP, RC)

Monitoring and Control

Monitoring and Control includes those activities, actions and conditions that provide monitoring and control of BES Elements. An example aspect of the Control and Operation function is:

- All methods of operating breakers and switches
  - SCADA (TOP, GOP)
  - Substation automation (TOP)

Restoration of BES

The Restoration of BES Operations Service includes activities, actions and conditions necessary to go from a shutdown condition to an operating condition delivering electric power without external assistance. Aspects of the Restoration of BES function include, but are not limited to:

- Restoration including planned cranking path
  - Through black start units (TOP, GOP)
  - Through tie lines (TOP, GOP)
- Off-site power for nuclear facilities. (TOP, TO, BA, RC, DP, GO, GOP)
- Coordination (TOP, TO, BA, RC, DP, GO, GOP)

Situational Awareness

The Situational Awareness function includes activities, actions and conditions established by policy, directive or standard operating procedure necessary to assess the current condition of the BES and anticipate effects of planned and unplanned changes to conditions. Aspects of the Situation Awareness function include:

- Monitoring and alerting (such as EMS alarms) (TOP, GOP, RC,BA)
- Change management (TOP,GOP,RC,BA)
- Current Day and Next Day planning (TOP)
- Contingency Analysis (RC)
- Frequency monitoring (BA, RC)

Inter-Entity Coordination

The Inter-Entity coordination and communication function includes activities, actions, and conditions established by policy, directive, or standard operating procedure necessary for the coordination and communication between Responsible Entities to ensure the reliability and operability of the BES. Aspects of the Inter-Entity Coordination and Communication function include:

- Scheduled interchange (BA,TOP,GOP,RC)
- Facility operational data and status (TO, TOP, GO, GOP, RC, BA)
- Operational directives (TOP, RC, BA)

Applicability to Distribution Providers

It is expected that only Distribution Providers that own or operate facilities that qualify in the Applicability section will be subject to these Version 5 Cyber Security Standards. Distribution Providers that do not own or operate any facility that qualifies are not subject to these standards. The qualifications are based on the requirements for registration as a Distribution Provider and on the requirements applicable to Distribution Providers in NERC Standard EOP-005.

Requirement R1:

Requirement R1 implements the methodology for the categorization of BES Cyber Systems according to their impact on the BES. Using the traditional risk assessment equation, it reduces the measure of the risk to an impact (consequence) assessment, assuming the vulnerability index of 1 (the Systems are assumed to be vulnerable) and a probability of threat of 1 (100 percent). The criteria in Attachment 1 provide a measure of the impact of the BES assets supported by these BES Cyber Systems.

Responsible Entities are required to identify and categorize those BES Cyber Systems that have high and medium impact. BES Cyber Systems for BES assets not specified in Attachment 1, Criteria 1.1 – 1.4 and Criteria 2.1 – 2.11 default to low impact.

Attachment 1

Overall Application

In the application of the criteria in Attachment 1, Responsible Entities should note that the approach used is based on the impact of the BES Cyber System as measured by the bright-line criteria defined in Attachment 1.

- When the drafting team uses the term "Facilities", there is some latitude to Responsible Entities to determine included Facilities. The term Facility is defined in the NERC Glossary of Terms as "A set of electrical equipment that operates as a single Bulk Electric System Element (e.g., a line, a generator, a shunt compensator, transformer, etc.)." In most cases, the criteria refer to a group of Facilities in a given location that supports the reliable operation of the BES. For example, for Transmission assets, the substation may be designated as the group of Facilities. However, in a substation that includes equipment that supports BES operations along with equipment that only supports Distribution operations, the Responsible Entity may be better served to consider only the group of Facilities that supports BES operation. In that case, the Responsible Entity may designate the group of Facilities by location, with qualifications on the group of Facilities that supports reliable operation of the BES, as the Facilities that are subject to the criteria for categorization of BES Cyber Systems. Generation Facilities are separately discussed in the Generation section below. In CIP-002-5.1a, these groups of Facilities, systems, and equipment are sometimes designated as BES assets. For example, an identified BES asset may be a named substation, generating plant, or Control Center. Responsible Entities have flexibility in how they group Facilities, systems, and equipment at a location.
- In certain cases, a BES Cyber System may be categorized by meeting multiple criteria. In such cases, the Responsible Entity may choose to document all criteria that result in the categorization. This will avoid inadvertent miscategorization when it no longer meets one of the criteria, but still meets another.
- It is recommended that each BES Cyber System should be listed by only one Responsible Entity. Where there is joint ownership, it is advisable that the owning Responsible Entities should formally agree on the designated Responsible Entity responsible for compliance with the standards.

High Impact Rating (H)

This category includes those BES Cyber Systems, used by and at Control Centers (and the associated data centers included in the definition of Control Centers), that perform the functional obligations of the Reliability Coordinator (RC), Balancing Authority (BA), Transmission Operator (TOP), or Generator Operator (GOP), as defined under the Tasks heading of the applicable Function and the Relationship with Other Entities heading of the functional entity in the NERC Functional Model, and as scoped by the qualification in Attachment 1, Criteria 1.1, 1.2, 1.3 and 1.4. While those entities that have been registered as the above-named functional entities are specifically referenced, it must be noted that there may be agreements where some

of the functional obligations of a Transmission Operator may be delegated to a Transmission Owner (TO). In these cases, BES Cyber Systems at these TO Control Centers that perform these functional obligations would be subject to categorization as high impact. The criteria notably specifically emphasize functional obligations, not necessarily the RC, BA, TOP, or GOP facilities. One must note that the definition of Control Center specifically refers to reliability tasks for RCs, Bas, TOPs, and GOPs. A TO BES Cyber System in a TO facility that does not perform or does not have an agreement with a TOP to perform any of these functional tasks does not meet the definition of a Control Center. However, if that BES Cyber System operates any of the facilities that meet criteria in the Medium Impact category, that BES Cyber System would be categorized as a Medium Impact BES Cyber System.

The 3000 MW threshold defined in criterion 1.2 for BA Control Centers provides a sufficient differentiation of the threshold defined for Medium Impact BA Control Centers. An analysis of BA footprints shows that the majority of Bas with significant impact are covered under this criterion.

Additional thresholds as specified in the criteria apply for this category.

Medium Impact Rating (M)

Generation

The criteria in Attachment 1's medium impact category that generally apply to Generation Owner and Operator (GO/GOP) Registered Entities are criteria 2.1, 2.3, 2.6, 2.9, and 2.11. Criterion 2.13 for BA Control Centers is also included here.

- Criterion 2.1 designates as medium impact those BES Cyber Systems that impact generation with a net Real Power capability exceeding 1500 MW. The 1500 MW criterion is sourced partly from the Contingency Reserve requirements in NERC standard BAL-002, whose purpose is "to ensure the Balancing Authority is able to utilize its Contingency Reserve to balance resources and demand and return Interconnection frequency within defined limits following a Reportable Disturbance." In particular, it requires that "as a minimum, the Balancing Authority or Reserve Sharing Group shall carry at least enough Contingency Reserve to cover the most severe single contingency." The drafting team used 1500 MW as a number derived from the most significant Contingency Reserves operated in various Bas in all regions.

  In the use of net Real Power capability, the drafting team sought to use a value that could be verified through existing requirements as proposed by NERC standard MOD-024 and current development efforts in that area.

  By using 1500 MW as a bright-line, the intent of the drafting team was to ensure that BES Cyber Systems with common mode vulnerabilities that could result in the loss of 1500 MW or more of generation at a single plant for a unit or group of units are adequately protected.

The drafting team also used additional time and value parameters to ensure the bright-lines and the values used to measure against them were relatively stable over the review period. Hence, where multiple values of net Real Power capability could be used for the Facilities' qualification against these bright-lines, the highest value was used.

- In Criterion 2.3, the drafting team sought to ensure that BES Cyber Systems for those generation Facilities that have been designated by the Planning Coordinator or Transmission Planner as necessary to avoid BES Adverse Reliability Impacts in the planning horizon of one year or more are categorized as medium impact. In specifying a planning horizon of one year or more, the intent is to ensure that those are units that are identified as a result of a "long term" reliability planning, i.e that the plans are spanning an operating period of at least 12 months: it does not mean that the operating day for the unit is necessarily beyond one year, but that the period that is being planned for is more than 1 year: it is specifically intended to avoid designating generation that is required to be run to remediate short term emergency reliability issues. These Facilities may be designated as "Reliability Must Run," and this designation is distinct from those generation Facilities designated as "must run" for market stabilization purposes. Because the use of the term "must run" creates some confusion in many areas, the drafting team chose to avoid using this term and instead drafted the requirement in more generic reliability language. In particular, the focus on preventing an Adverse Reliability Impact dictates that these units are designated as must run for reliability purposes beyond the local area. Those units designated as must run for voltage support in the local area would not generally be given this designation. In cases where there is no designated Planning Coordinator, the Transmission Planner is included as the Registered Entity that performs this designation.

  If it is determined through System studies that a unit must run in order to preserve the reliability of the BES, such as due to a Category C3 contingency as defined in TPL-003, then BES Cyber Systems for that unit are categorized as medium impact.

  The TPL standards require that, where the studies and plans indicate additional actions, that these studies and plans be communicated by the Planning Coordinator or Transmission Planner in writing to the Regional Entity/RRO. Actions necessary for the implementation of these plans by affected parties (generation owners/operators and Reliability Coordinators or other necessary party) are usually formalized in the form of an agreement and/or contract.

- Criterion 2.6 includes BES Cyber Systems for those Generation Facilities that have been identified as critical to the derivation of IROLs and their associated contingencies, as specified by FAC-014-2, **Establish and Communicate System Operating Limits**, R5.1.1 and R5.1.3.

  IROLs may be based on dynamic System phenomena such as instability or voltage collapse. Derivation of these IROLs and their associated contingencies often considers the effect of generation inertia and AVR response.

- Criterion 2.9 categorizes BES Cyber Systems for Special Protection Systems and Remedial Action Schemes as medium impact. Special Protection Systems and Remedial Action Schemes may be implemented to prevent disturbances that would result in exceeding IROLs if they do not provide the function required at the time it is required or if it operates outside of the parameters it was designed for. Generation Owners and Generator Operators which own BES Cyber Systems for such Systems and schemes designate them as medium impact.

- Criterion 2.11 categorizes as medium impact BES Cyber Systems used by and at Control Centers that perform the functional obligations of the Generator Operator for an aggregate generation of 1500 MW or higher in a single interconnection, and that have not already been included in Part 1.

- Criterion 2.13 categorizes as medium impact those BA Control Centers that "control" 1500 MW of generation or more in a single interconnection and that have not already been included in Part 1. The 1500 MW threshold is consistent with the impact level and rationale specified for Criterion 2.1.

Transmission

The SDT uses the phrases "Transmission Facilities at a single station or substation" and "Transmission stations or substations" to recognize the existence of both stations and substations. Many entities in industry consider a substation to be a location with physical borders (i.e. fence, wall, etc.) that contains at least an autotransformer. Locations also exist that do not contain autotransformers, and many entities in industry refer to those locations as stations (or switchyards). Therefore, the SDT chose to use both "station" and "substation" to refer to the locations where groups of Transmission Facilities exist.

- Criteria 2.2, 2.4 through 2.10, and 2.12 in Attachment 1 are the criteria that are applicable to Transmission Owners and Operators. In many of the criteria, the impact threshold is defined as the capability of the failure or compromise of a System to result in exceeding one or more Interconnection Reliability Operating Limits (IROLs). Criterion 2.2 includes BES Cyber Systems for those Facilities in Transmission Systems that provide reactive resources to enhance and preserve the reliability of the BES. The nameplate value is used here because there is no NERC requirement to verify actual capability of these Facilities. The value of 1000 MVARs used in this criterion is a value deemed reasonable for the purpose of determining criticality.

- Criterion 2.4 includes BES Cyber Systems for any Transmission Facility at a substation operated at 500 kV or higher. While the drafting team felt that Facilities operated at 500 kV or higher did not require any further qualification for their role as components of the backbone on the Interconnected BES, Facilities in the lower EHV range should have additional qualifying criteria for inclusion in the medium impact category.

It must be noted that if the collector bus for a generation plant (i.e. the plant is smaller in aggregate than the threshold set for generation in Criterion 2.1) is operated at 500kV, the collector bus should be considered a Generation Interconnection Facility, and not a Transmission Facility, according to the "Final Report from the Ad Hoc Group for Generation Requirements at the Transmission Interface." This collector bus would not be a facility for a medium impact BES Cyber System because it does not significantly affect the 500kV Transmission grid; it only affects a plant which is below the generation threshold.

- Criterion 2.5 includes BES Cyber Systems for facilities at the lower end of BES Transmission with qualifications for inclusion if they are deemed highly likely to have significant impact on the BES. While the criterion has been specified as part of the rationale for requiring protection for significant impact on the BES, the drafting team included, in this criterion, additional qualifications that would ensure the required level of impact to the BES. The drafting team:

    - Excluded radial facilities that would only provide support for single generation facilities.

    - Specified interconnection to at least three transmission stations or substations to ensure that the level of impact would be appropriate.

  The total aggregated weighted value of 3,000 was derived from weighted values related to three connected 345 kV lines and five connected 230 kV lines at a transmission station or substation. The total aggregated weighted value is used to account for the true impact to the BES, irrespective of line kV rating and mix of multiple kV rated lines.

  Additionally, in NERC's document "Integrated Risk Assessment Approach – Refinement to Severity Risk Index", Attachment 1, the report used an average MVA line loading based on kV rating:

    - 230 kV –> 700 MVA

    - 345 kV –> 1,300 MVA

    - 500 kV –> 2,000 MVA

    - 765 kV –> 3,000 MVA

  In the terms of applicable lines and connecting "other Transmission stations or substations" determinations, the following should be considered:

    - For autotransformers in a station, Responsible Entities have flexibility in determining whether the groups of Facilities are considered a single substation or station location or multiple substations or stations. In most cases, Responsible Entities would probably consider them as Facilities at a single substation or station unless geographically dispersed. In these cases of these transformers being within the "fence" of the substation or station, autotransformers may not count as separate

connections to other stations. The use of common BES Cyber Systems may negate any rationale for any consideration otherwise. In the case of autotransformers that are geographically dispersed from a station location, the calculation would take into account the connections in and out of each station or substation location.

- Multiple-point (or multiple-tap) lines are considered to contribute a single weight value per line and affect the number of connections to other stations. Therefore, a single 230 kV multiple-point line between three Transmission stations or substations would contribute an aggregated weighted value of 700 and connect Transmission Facilities at a single station or substation to two other Transmission stations or substations.

- Multiple lines between two Transmission stations or substations are considered to contribute multiple weight values per line, but these multiple lines between the two stations only connect one station to one other station. Therefore, two 345 kV lines between two Transmission stations or substations would contribute an aggregated weighted value of 2600 and connect Transmission Facilities at a single station or substation to one other Transmission station or substation.

Criterion 2.5's qualification for Transmission Facilities at a Transmission station or substation is based on 2 distinct conditions.

1. The first condition is that Transmission Facilities at a single station or substation where that station or substation connect, at voltage levels of 200 kV or higher to three (3) other stations or substations, to three other stations or substations. This qualification is meant to ensure that connections that operate at voltages of 500 kV or higher are included in the count of connections to other stations or substations as well.
2. The second qualification is that the aggregate value of all lines entering or leaving the station or substation must exceed 3000. This qualification does not include the consideration of lines operating at lower than 200 kV, or 500 kV or higher, the latter already qualifying as medium impact under criterion 2.4. : there is no value to be assigned to lines at voltages of less than 200 kV or 500 kV or higher in the table of values for the contribution to the aggregate value of 3000.

The Transmission Facilities at the station or substation must meet both qualifications to be considered as qualified under criterion 2.5.

- Criterion 2.6 include BES Cyber Systems for those Transmission Facilities that have been identified as critical to the derivation of IROLs and their associated contingencies, as specified by FAC-014-2, **Establish and Communicate System Operating Limits**, R5.1.1 and R5.1.3.

- Criterion 2.7 is sourced from the NUC-001 NERC standard, Requirement R9.2.2, for the support of Nuclear Facilities. NUC-001 ensures that reliability of NPIR's are ensured through adequate coordination between the Nuclear Generator Owner/Operator and its Transmission provider "for the purpose of ensuring nuclear plant safe operation and shutdown." In particular, there are specific requirements to coordinate physical and cyber security protection of these interfaces.

- Criterion 2.8 designates as medium impact those BES Cyber Systems that impact Transmission Facilities necessary to directly support generation that meet the criteria in Criteria 2.1 (generation Facilities with output greater than 1500 MW) and 2.3 (generation Facilities generally designated as "must run" for wide area reliability in the planning horizon). The Responsible Entity can request a formal statement from the Generation owner as to the qualification of generation Facilities connected to their Transmission systems.

- Criterion 2.9 designates as medium impact those BES Cyber Systems for those Special Protection Systems (SPS), Remedial Action Schemes (RAS), or automated switching Systems installed to ensure BES operation within IROLs. The degradation, compromise or unavailability of these BES Cyber Systems would result in exceeding IROLs if they fail to operate as designed. By the definition of IROL, the loss or compromise of any of these have Wide Area impacts.

- Criterion 2.10 designates as medium impact those BES Cyber Systems for Systems or Elements that perform automatic Load shedding, without human operator initiation, of 300 MW or more. The SDT spent considerable time discussing the wording of Criterion 2.10, and chose the term "Each" to represent that the criterion applied to a discrete System or Facility. In the drafting of this criterion, the drafting team sought to include only those Systems that did not require human operator initiation, and targeted in particular those underfrequency load shedding (UFLS) Facilities and systems and undervoltage load shedding (UVLS) systems and Elements that would be subject to a regional Load shedding requirement to prevent Adverse Reliability Impact. These include automated UFLS systems or UVLS systems that are capable of Load shedding 300 MW or more. It should be noted that those qualifying systems which require a human operator to arm the system, but once armed, trigger automatically, are still to be considered as not requiring human operator initiation and should be designated as medium impact. The 300 MW threshold has been defined as the aggregate of the highest MW Load value, as defined by the applicable regional Load Shedding standards, for the preceding 12 months to account for seasonal fluctuations.

  This particular threshold (300 MW) was provided in CIP, Version 1. The SDT believes that the threshold should be lower than the 1500MW generation requirement since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System and hence requires a lower threshold. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

In ERCOT, the Load acting as a Resource ("LaaR") Demand Response Program is not part of the regional load shedding program, but an ancillary services market. In general, similar demand response programs that are not part of the NERC or regional reliability Load shedding programs, but are offered as components of an ancillary services market do not qualify under this criterion.

The language used in section 4 for UVLS and UFLS and in criterion 2.10 of Attachment 1 is designed to be consistent with requirements set in the PRC standards for UFLS and UVLS.

- Criterion 2.12 categorizes as medium impact those BES Cyber Systems used by and at Control Centers and associated data centers performing the functional obligations of a Transmission Operator and that have not already been categorized as high impact.

- Criterion 2.13 categorizes as Medium Impact those BA Control Centers that "control" 1500 MW of generation or more in a single Interconnection. The 1500 MW threshold is consistent with the impact level and rationale specified for Criterion 2.1.

Low Impact Rating (L)

BES Cyber Systems not categorized in high impact or medium impact default to low impact. Note that low impact BES Cyber Systems do not require discrete identification.

Restoration Facilities

- Several discussions on the CIP Version 5 standards suggest entities owning Blackstart Resources and Cranking Paths might elect to remove those services to avoid higher compliance costs. For example, one Reliability Coordinator reported a 25% reduction of Blackstart Resources as a result of the Version 1 language, and there could be more entities that make this choice under Version 5.

  In response, the CIP Version 5 drafting team sought informal input from NERC's Operating and Planning Committees. The committees indicate there has already been a reduction in Blackstart Resources because of increased CIP compliance costs, environmental rules, and other risks; continued inclusion within Version 5 at a category that would very significantly increase compliance costs can result in further reduction of a vulnerable pool.

  The drafting team moved from the categorization of restoration assets such as Blackstart Resources and Cranking Paths as medium impact (as was the case in earlier drafts) to categorization of these assets as low impact as a result of these considerations. This will not relieve asset owners of all responsibilities, as would have been the case in CIP-002, Versions 1-4 (since only Cyber Assets with routable connectivity which are essential to restoration assets are included in those versions). Under the low impact categorization, those assets will be protected in the areas of cyber security awareness, physical access control, and electronic access control, and they will have obligations regarding incident response. This represents a net gain to bulk power system reliability, however, since many of those assets do not meet criteria for inclusion under Versions 1-4.

Weighing the risks to overall BES reliability, the drafting team determined that this re-categorization represents the option that would be the least detrimental to restoration function and, thus, overall BES reliability. Removing Blackstart Resources and Cranking Paths from medium impact promotes overall reliability, as the likely alternative is fewer Blackstart Resources supporting timely restoration when needed.

BES Cyber Systems for generation resources that have been designated as Blackstart Resources in the Transmission Operator's restoration plan default to low impact. NERC Standard EOP-005-2 requires the Transmission Operator to have a Restoration Plan and to list its Blackstart Resources in its plan, as well as requirements to test these Resources. This criterion designates only those generation Blackstart Resources that have been designated as such in the Transmission Operator's restoration plan. The glossary term Blackstart Capability Plan has been retired.

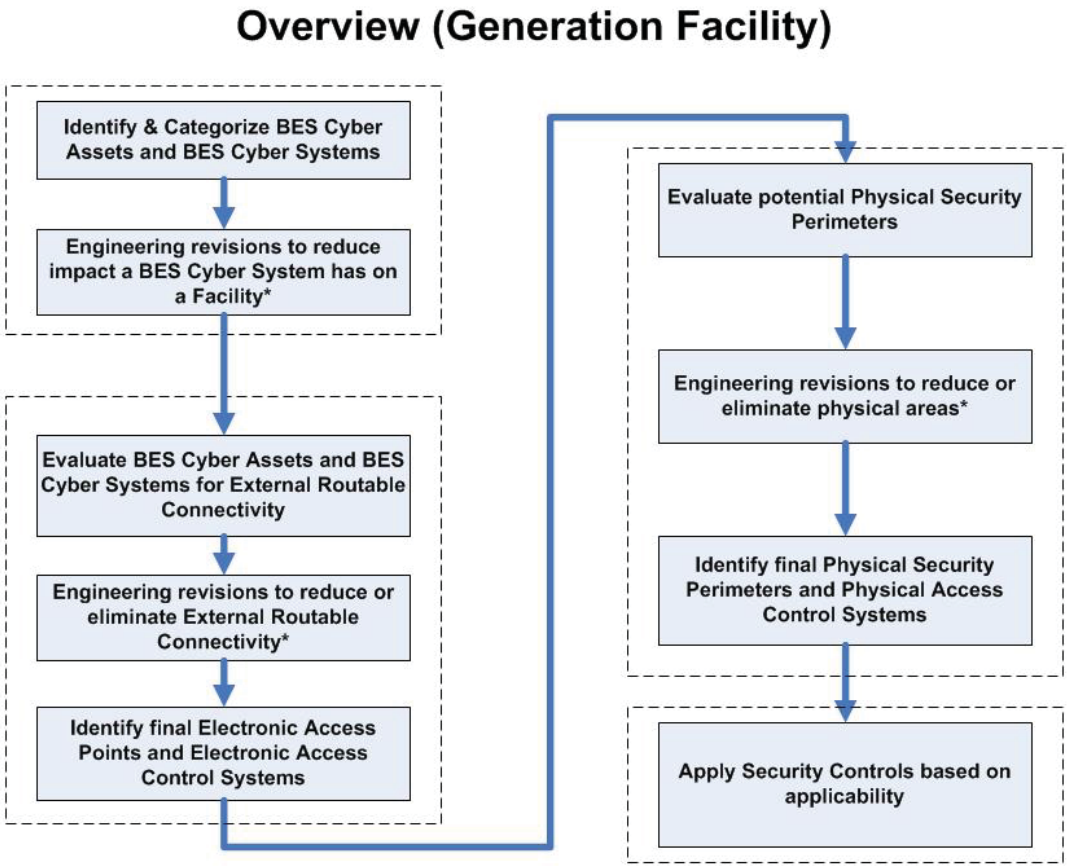
Regarding concerns of communication to BES Asset Owners and Operators of their role in the Restoration Plan, Transmission Operators are required in NERC Standard EOP-005-2 to "provide the entities identified in its approved restoration plan with a description of any changes to their roles and specific tasks prior to the implementation date of the plan."

- BES Cyber Systems for Facilities and Elements comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource to the first Interconnection point of the generation unit(s) to be started, as identified in the Transmission Operator's restoration plan, default to the category of low impact: however, these systems are explicitly called out to ensure consideration for inclusion in the scope of the version 5 CIP standards. This requirement for inclusion in the scope is sourced from requirements in NERC standard EOP-005-2, which requires the Transmission Operator to include in its Restoration Plan the Cranking Paths and initial switching requirements from the Blackstart Resource and the unit(s) to be started.

  Distribution Providers may note that they may have BES Cyber Systems that must be scoped in if they have Elements listed in the Transmission Operator's Restoration Plan that are components of the Cranking Path.

Use Case: CIP Process Flow

The following CIP use case process flow for a generator Operator/Owner was provided by a participant in the development of the Version 5 standards and is provided here as an example of a process used to identify and categorize BES Cyber Systems and BES Cyber Assets; review, develop, and implement strategies to mitigate overall risks; and apply applicable security controls.



* - Engineering revisions will need to be reviewed for cost justification, operational\safety requirements, support requirements, and technical limitations.

Rationale:

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for R1:

BES Cyber Systems at each site location have varying impact on the reliable operation of the Bulk Electric System. Attachment 1 provides a set of "bright-line" criteria that the Responsible Entity must use to identify these BES Cyber Systems in accordance with the impact on the BES. BES Cyber Systems must be identified and categorized according to their impact so that the appropriate measures can be applied, commensurate with their impact. These impact categories will be the basis for the application of appropriate requirements in CIP-003-CIP-011.

Rationale for R2:

The lists required by Requirement R1 are reviewed on a periodic basis to ensure that all BES Cyber Systems required to be categorized have been properly identified and categorized. The miscategorization or non-categorization of a BES Cyber System can lead to the application of inadequate or non-existent cyber security controls that can lead to compromise or misuse that can affect the real-time operation of the BES. The CIP Senior Manager's approval ensures proper oversight of the process by the appropriate Responsible Entity personnel.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a Responsible Entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3.	Update

		Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5.1	9/30/13	Replaced “Devices” with “Systems” in a definition in background section.	Errata
5.1	11/22/13	FERC Order issued approving CIP-002-5.1.	
5.1a	11/02/16	Adopted by the NERC Board of Trustees.	

Appendix 1

Requirement Number and Text of Requirement
CIP-002-5.1, Requirement R1 R1. Each Responsible Entity shall implement a process that considers each of the following assets for purposes of parts 1.1 through 1.3: i. Control Centers and backup Control Centers; ii. Transmission stations and substations; iii. Generation resources; iv. Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements; v. Special Protection Systems that support the reliable operation of the Bulk Electric System; and vi. For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above. 1.1. Identify each of the high impact BES Cyber Systems according to Attachment 1, Section 1, if any, at each asset; 1.2. Identify each of the medium impact BES Cyber Systems according to Attachment 1, Section 2, if any, at each asset; and 1.3. Identify each asset that contains a low impact BES Cyber System according to Attachment 1, Section 3, if any (a discrete list of low impact BES Cyber Systems is not required). Attachment 1, Criterion 2.1 2. Medium Impact Rating (M) Each BES Cyber System, not included in Section 1 above, associated with any of the following: 2.1. Commissioned generation, by each group of generating units at a single plant location, with an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection. For each group of generating units, the only BES Cyber Systems that meet this criterion are those shared BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection.

Questions

Energy Sector Security Consortium, Inc. (EnergySec) submitted a Request for Interpretation (RFI) seeking clarification of Criterion 2.1 of Attachment 1 in Reliability Standard CIP-002-5.1 regarding the use of the phrase "shared BES Cyber Systems."

The Interpretation Drafting Team identified the following questions in the RFI:

1. Whether the phrase "shared BES Cyber Systems" means that the evaluation for Criterion 2.1 shall be performed individually for each discrete BES Cyber System at a single plant location, or collectively for groups of BES Cyber Systems?
2. Whether the phrase "shared BES Cyber Systems" refers to discrete BES Cyber Systems that are shared by multiple units, or groups of BES Cyber Systems that could collectively impact multiple units?
3. If the phrase applies collectively to groups of BES Cyber Systems, what criteria should be used to determine which BES Cyber Systems should be grouped for collective evaluation?

Responses

Question 1: Whether the phrase "shared BES Cyber Systems," means that the evaluation for Criterion 2.1 shall be performed individually for each discrete BES Cyber System at a single plant location, or collectively for groups of BES Cyber Systems?

The evaluation as to whether a BES Cyber System is shared should be performed individually for each discrete BES Cyber System. In the standard language of CIP-002-5.1, there is no reference to or obligation to group BES Cyber Systems. Requirement R1, part 1.2 states "Identify *each* of the medium impact BES Cyber Systems according to Attachment 1, Section 2…" Further, the preamble of Section 2 of CIP-002-5.1 Attachment 1 states "*Each BES Cyber System*…associated with any of the following [criteria]." (emphasis added)

Additionally, the Background section of CIP-002-5.1 states that "[i]t is left up to the Responsible Entity to determine the level of granularity at which to identify a BES Cyber System within the qualifications in the definition of BES Cyber System." The Background section also provides:

> The Responsible Entity should take into consideration the operational environment and scope of management when defining the BES Cyber System boundary in order to maximize efficiency in secure operations. Defining the boundary too tightly may result in redundant paperwork and authorizations, while defining the boundary too broadly could make the secure operation of the BES Cyber System difficult to monitor and assess.

Question 2: Whether the phrase "shared BES Cyber Systems" refers to discrete BES Cyber Systems that are shared by multiple units, or groups of BES Cyber Systems that could collectively impact multiple units?

The phrase "shared BES Cyber Systems" refers to discrete BES Cyber Systems that are shared by multiple generation units.

The use of the term "shared" is also clarified in the NERC Frequently Asked Questions (FAQ) document issued by NERC Compliance to support implementation of the CIP Reliability Standards. FAQ #49 provides:

> Shared BES Cyber Systems are those that are associated with any combination of units in a single Interconnection, as referenced in CIP-002-5.1, Attachment 1, impact rating criteria 2.1 and 2.2. For criterion 2.1 "BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection." For criterion 2.2: "BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of resources that in aggregate equal or exceed 1000 MVAR. Also refer to the Lesson Learned for CIP-002-5.1 Requirement R1: **Impact Rating of Generation Resource Shared BES Cyber Systems** for further information and examples.

Question 3: If the phrase applies collectively to groups of BES Cyber Systems, what criteria should be used to determine which BES Cyber Systems should be grouped for collective evaluation?

The phrase applies to each discrete BES Cyber System.

A. Introduction

1. **Title:** Cyber Security — Security Management Controls

2. **Number:** CIP-003-~~6~~7

3. **Purpose:** To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1. Balancing Authority

   4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2. Each Special Protection System (SPS) or Remedial Action Scheme (RAS) where the SPS or RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

   4.1.3. Generator Operator

   4.1.4. Generator Owner

   4.1.5. Interchange Coordinator or Interchange Authority

   4.1.6. Reliability Coordinator

4.1.7. Transmission Operator

4.1.8. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in Section 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each SPS or RAS where the SPS or RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-003-~~6:~~ 7:

4.2.3.1. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESPs).

4.2.3.3. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

5. Effective Dates:

See Implementation Plan for CIP-003-~~6~~7.

6. ~~6.~~ Background:

Standard CIP-003 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.

The term policy refers to one or a collection of written documents that are used to communicate the Responsible Entities' management goals, objectives and expectations for how the Responsible Entity will protect its BES Cyber Systems. The use of policies also establishes an overall governance foundation for creating a culture of security and compliance with laws, regulations, and standards.

The term documented processes refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements.

The terms program and plan are sometimes used in place of documented processes where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as plans (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term program may refer to the organization's overall implementation of its policies, plans, and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Reliability Standards could also be referred to as a program. However, the terms program and plan do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high, medium, and low impact BES Cyber Systems. For example, a single cyber security awareness program could meet the requirements across multiple BES Cyber Systems.

Measures provide examples of evidence to show documentation and implementation of the requirement. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the BES. A review of UFLS tolerances defined within Regional Reliability Standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

B. Requirements and Measures

R1. Each Responsible Entity shall review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies that collectively address the following topics: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1. For its high impact and medium impact BES Cyber Systems, if any:

1.1.1. Personnel and training (CIP-004);

1.1.2. Electronic Security Perimeters (CIP-005) including Interactive Remote Access;

1.1.3. Physical security of BES Cyber Systems (CIP-006);

1.1.4. System security management (CIP-007);

1.1.5. Incident reporting and response planning (CIP-008);

1.1.6. Recovery plans for BES Cyber Systems (CIP-009);

1.1.7. Configuration change management and vulnerability assessments (CIP-010);

1.1.8. Information protection (CIP-011); and

1.1.9. Declaring and responding to CIP Exceptional Circumstances.

1.2. For its assets identified in CIP-002 containing low impact BES Cyber Systems, if any:

1.2.1. Cyber security awareness;

1.2.2. Physical security controls;

1.2.3. Electronic access controls ~~for Low Impact External Routable Connectivity (LERC) and Dial-up Connectivity; and~~;

1.2.4. Cyber Security Incident response;

1.2.5. Transient Cyber Assets and Removable Media malicious code risk mitigation; and

1.2.6. Declaring and responding to CIP Exceptional Circumstances.

M1. Examples of evidence may include, but are not limited to, policy documents; revision history, records of review, or workflow evidence from a document management system that indicate review of each cyber security policy at least once every 15 calendar months; and documented approval by the CIP Senior Manager for each cyber security policy.

R2. Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall implement one or more documented cyber security plan(s) for its low impact BES Cyber Systems that include the sections in Attachment 1. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

Note: An inventory, list, or discrete identification of low impact BES Cyber Systems or their BES Cyber Assets is not required. Lists of authorized users are not required.

M2. Evidence shall include each of the documented cyber security plan(s) that collectively include each of the sections in Attachment 1 and additional evidence to demonstrate implementation of the cyber security plan(s). Additional examples of evidence per section are located in Attachment 2.

R3. Each Responsible Entity shall identify a CIP Senior Manager by name and document any change within 30 calendar days of the change. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. An example of evidence may include, but is not limited to, a dated and approved document from a high level official designating the name of the individual identified as the CIP Senior Manager.

R4. The Responsible Entity shall implement a documented process to delegate authority, unless no delegations are used. Where allowed by the CIP Standards, the CIP Senior Manager may delegate authority for specific actions to a delegate or delegates. These delegations shall be documented, including the name or title of the delegate, the specific actions delegated, and the date of the delegation; approved by the CIP Senior Manager; and updated within 30 days of any change to the delegation. Delegation changes do not need to be reinstated with a change to the delegator. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M4. An example of evidence may include, but is not limited to, a dated document, approved by the CIP Senior Manager, listing individuals (by name or title) who are delegated the authority to approve or authorize specifically identified items.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority:

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audits
- Self-Certifications
- Spot Checking
- Compliance Investigations
- Self-Reporting
- Complaints

1.4. Additional Compliance Information:

None.

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	Operations Planning	Medium	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address one of the nine topics required by R1. (R1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 15 calendar months but did	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address two of the nine topics required by R1. (R1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 16 calendar months but did	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address three of the nine topics required by R1. (R1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 17 calendar months but did complete this review in less than or equal to 18	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address four or more of the nine topics required by R1. (R1.1) OR The Responsible Entity did not have any documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1. (R1.1) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			complete this review in less than or equal to 16 calendar months of the previous review. (R1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of	complete this review in less than or equal to 17 calendar months of the previous review. (R1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of	calendar months of the previous review. (R1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (R1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact	The Responsible Entity did not complete its review of the one or more documented cyber security policies as required by R1 within 18 calendar months of the previous review. (R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 18 calendar months of

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address one of the ~~four~~six topics required by R1. (R1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as	the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address two of the ~~four~~six topics required by R1. (R1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as	BES Cyber Systems, but did not address three of the ~~four~~six topics required by R1. (R1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its	the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address ~~any~~four or more of the ~~four~~six topics required by R1. (R1.2) OR The Responsible Entity did not have any documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			required by Requirement R1 within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the previous review. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 15 calendar months but did complete this	required by Requirement R1 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 16 calendar months but	assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (R1.2)	Systems as required by R1. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (R1.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-67)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			approval in less than or equal to 16 calendar months of the previous approval. (R1.2)	did complete this approval in less than or equal to 17 calendar months of the previous approval. (R1.2)		
R2	**Operations Planning**	**Lower**	The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document cyber security awareness according to CIP-003-6, Requirement R2, Attachment 1, Section 1. (R2) OR The Responsible Entity implemented electronic access controls but failed to document its cyber security plan(s) for	The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to reinforce cyber security practices at least once every 15 calendar months according to CIP-003-6, Requirement R2, Attachment 1, Section 1. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets	The Responsible Entity documented the physical access controls for its assets containing low impact BES Cyber Systems, but failed to implement the physical security controls according to Requirement R2, Attachment 1, Section 2. (R2) OR The Responsible Entity documented its cyber security plan(s) for electronic access controls for its assets containing low impact BES Cyber Systems, but	The Responsible Entity failed to document or and implement one or more cyber security plan(s) for its assets containing low impact BES Cyber Systems according to CIP-003-6, Requirement R2, Attachment 1. (R2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			electronic access controls according to Requirement R2, Attachment 1, Section 3. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document one or more Cyber Security Incident response ~~plans~~plan(s) according to ~~CIP-003-6,~~ Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented one or more Cyber Security Incident	containing low impact BES Cyber Systems, but failed to document physical security controls according to Requirement R2, Attachment 1, Section 2. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document electronic access controls according to Requirement R2, Attachment 1, Section 3. (R2) OR The Responsible Entity documented	failed to permit only necessary inbound and outbound electronic access controls according to Requirement R2, Attachment 1, Section 3.1. (R2) OR The Responsible Entity documented one or more Cyber Security Incident response ~~plans~~plan(s) within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to test each Cyber Security Incident response plan(s) at least once every 36 calendar months according to ~~CIP-003-6,~~ Requirement R2, Attachment 1, Section 4. (R2)	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-67)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			response plansplan(s) within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to update each Cyber Security Incident response plan(s) within 180 days according to CIP-003-6, Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to manage its Transient Cyber Asset(s) according to Requirement R2,	its cyber security plan(s) for electronic access controls but failed to implement authentication for all Dial-up Connectivity that provides access to low impact BES Cyber System(s), per Cyber Asset capability according to Requirement R2, Attachment 1, Section 3.2 (R2) OR The Responsible Entity documented one or more incident response plansplan(s) within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to include the process for	OR The Responsible Entity documented the determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident, but failed to notify the Electricity Sector Information Sharing and Analysis Center (ESE-ISAC) according to CIP-003-6, Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented and implemented electronic access controlsits plan(s) for LERCTransient Cyber Assets and Removable Media, but failed to implement a LEAP or permit inbound and	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Attachment 1, Section 5.1. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets, but failed to document the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (R2)	identification, classification, and response to Cyber Security Incidents according to ~~CIP-003-6,~~ Requirement R2, Attachment 1, Section 4. (R2) OR ~~(R2)~~ ~~OR~~ The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document the determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent	~~outbound access~~ mitigation for the introduction of malicious code for Transient Cyber Assets managed by the Responsible Entity according to ~~CIP-003-6,~~ Requirement R2, Attachment 1, Section ~~3~~5.1. (R2) OR The Responsible Entity documented ~~and implemented electronic access controls~~its plan(s) for ~~its assets containing low impact BES~~Transient Cyber ~~Systems~~Assets and Removable Media, but failed to ~~document and~~ implement ~~authentication of all Dial-up Connectivity, if any, that provides access to low impact BES Cyber Systems~~mitigation for the introduction of	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-67)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				notification to the Electricity Sector Information Sharing and Analysis Center (ESE-ISAC) according to CIP-003-6, Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BESTransient Cyber SystemsAssets and Removable Media, but failed to document physical security controls mitigation for the introduction of malicious code for Transient Cyber Assets managed by the Responsible	malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to CIP-003-6, Requirement R2, Attachment 1, Section 35.2. (R2) OR The Responsible Entity documented the physical access controlsits plan(s) for its assets containing low impact BESTransient Cyber SystemsAssets and Removable Media, but failed to implement the physical security controlsmitigation for the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact BES Cyber System according to CIP-	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-67)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				Entity according to CIP-003-6, Requirement R2, Attachment 1, Section 2. Sections 5.1 and 5.3. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BESTransient Cyber SystemsAssets and Removable Media, but failed to document electronic access controlsmitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to CIP-003-6,Requirement	003-6, Requirement R2, Attachment 1, Section 25.3. (R2)	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				R2, Attachment 1, Section 5.2. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (R2)		
R3	**Operations Planning**	**Medium**	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 30 calendar days but did document this change in less than	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 40 calendar days but did document this	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 50 calendar days but did document this change in less than 60 calendar days of the change. (R3)	The Responsible Entity has not identified, by name, a CIP Senior Manager. OR The Responsible Entity has identified by name a CIP Senior

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			40 calendar days of the change. (R3)	change in less than 50 calendar days of the change. (R3)		Manager, but did not document changes to the CIP Senior Manager within 60 calendar days of the change. (R3)
R4	**Operations Planning**	**Lower**	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 30 calendar days but did document this change in less than 40 calendar days of the change. (R4)	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 40 calendar days but did document this change in less than 50 calendar days of the change. (R4)	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 50 calendar days but did document this change in less than 60 calendar days of the change. (R4)	The Responsible Entity has used delegated authority for actions where allowed by the CIP Standards, but does not have a process to delegate actions from the CIP Senior Manager. (R4) OR The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						changes to the delegate within 60 calendar days of the change. (R4)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-003-5.	

Version	Date	Action	Change Tracking
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
6	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
6	1/21/16	FERC Order issued approving CIP-003-6. Docket No. RM15-14-000	
7	2/9/17	Adopted by the NERC Board of Trustees.	Revised to address FERC Order No. 822 directives regarding (1) the definition of LERC and (2) transient devices.

Attachment 1

Required Sections for Cyber Security Plan(s) for Assets Containing Low Impact BES Cyber Systems

Responsible Entities shall include each of the sections provided below in the cyber security plan(s) required under Requirement R2.

Responsible Entities with multiple-impact BES Cyber Systems ratings can utilize policies, procedures, and processes for their high or medium impact BES Cyber Systems to fulfill the sections for the development of low impact cyber security plan(s). Each Responsible Entity can develop a cyber security plan(s) either by individual asset or groups of assets.

Section 1. Cyber Security Awareness: Each Responsible Entity shall reinforce, at least once every 15 calendar months, cyber security practices (which may include associated physical security practices).

Section 2. Physical Security Controls: Each Responsible Entity shall control physical access, based on need as determined by the Responsible Entity, to (1) the asset or the locations of the low impact BES Cyber Systems within the asset ~~and (2) the Low Impact BES Cyber System Electronic Access Points (LEAPs),~~, and (2) the Cyber Asset(s), as specified by the Responsible Entity, that provide electronic access control(s) implemented for Section 3.1, if any.

~~**Section 3.**~~ Electronic Access Controls: ~~Each~~For each asset containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall~~:~~

Section 3. ~~For LERC, if any,~~ implement ~~a LEAP to permit~~electronic access controls to:

3.1 Permit only necessary inbound and outbound ~~bi-directional~~electronic access as determined by the Responsible Entity for any communications that are:

i. between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s);

~~i.~~ii. using a routable protocol ~~access;~~when entering or leaving the asset containing the low impact BES Cyber System(s); and

iii. ~~Implement authentication for~~not used for time-sensitive protection or control functions between intelligent electronic devices (e.g., communications using protocol IEC TR-61850-90-5 R-GOOSE).

3.2 Authenticate all Dial-up Connectivity, if any, that provides access to low impact BES Cyber ~~Systems,~~System(s), per Cyber Asset capability.

Section 4. Cyber Security Incident Response: Each Responsible Entity shall have one or more Cyber Security Incident response plan(s), either by asset or group of assets, which shall include:

4.1 Identification, classification, and response to Cyber Security Incidents;

4.2 Determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity ~~Sector~~ Information Sharing and Analysis Center (~~ES~~E-ISAC), unless prohibited by law;

4.3 Identification of the roles and responsibilities for Cyber Security Incident response by groups or individuals;

4.4 Incident handling for Cyber Security Incidents;

4.5 Testing the Cyber Security Incident response plan(s) at least once every 36 calendar months by: (1) responding to an actual Reportable Cyber Security Incident; (2) using a drill or tabletop exercise of a Reportable Cyber Security Incident; or (3) using an operational exercise of a Reportable Cyber Security Incident; and

4.6 Updating the Cyber Security Incident response plan(s), if needed, within 180 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident.

~~CIP-003-6 - Attachment 2~~

Section 5. Transient Cyber Asset and Removable Media Malicious Code Risk Mitigation: Each Responsible Entity shall implement, except under CIP Exceptional Circumstances, one or more plan(s) to achieve the objective of mitigating the risk of the introduction of malicious code to low impact BES Cyber Systems through the use of Transient Cyber Assets or Removable Media. The plan(s) shall include:

5.1 For Transient Cyber Asset(s) managed by the Responsible Entity, if any, the use of one or a combination of the following in an ongoing or on-demand manner (per Transient Cyber Asset capability):

- Antivirus software, including manual or managed updates of signatures or patterns;
- Application whitelisting; or
- Other method(s) to mitigate the introduction of malicious code.

5.2 For Transient Cyber Asset(s) managed by a party other than the Responsible Entity, if any, the use of one or a combination of the following prior to connecting the Transient Cyber Asset to a low impact BES Cyber System (per Transient Cyber Asset capability):

- Review of antivirus update level;
- Review of antivirus update process used by the party;
- Review of application whitelisting used by the party;
- Review use of live operating system and software executable only from read-only media;
- Review of system hardening used by the party; or
- Other method(s) to mitigate the introduction of malicious code.

5.3 For Removable Media, the use of each of the following:

5.3.1 Method(s) to detect malicious code on Removable Media using a Cyber Asset other than a BES Cyber System; and

5.3.2 Mitigation of the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact BES Cyber System.

Attachment 2

Examples of Evidence for Cyber Security Plan(s) for Assets Containing Low Impact BES Cyber Systems

Section 1. ~~Section 1 -~~ Cyber Security Awareness: An example of evidence for Section 1 may include, but is not limited to, documentation that the reinforcement of cyber security practices occurred at least once every 15 calendar months. The evidence could be documentation through one or more of the following methods:

- Direct communications (for example, e-mails, memos, or computer-based training);
- Indirect communications (for example, posters, intranet, or brochures); or
- Management support and reinforcement (for example, presentations or meetings).

Section 2. ~~Section 2 -~~ Physical Security Controls: Examples of evidence for Section 2 may include, but are not limited to:

- Documentation of the selected access control(s) (e.g., card key, locks, perimeter controls), monitoring controls (e.g., alarm systems, human observation), or other operational, procedural, or technical physical security controls that control physical access to both:
  a. The asset, if any, or the locations of the low impact BES Cyber Systems within the asset; and

~~b.~~ The Cyber Asset~~, if any, containing a LEAP.~~

b. (s) specified by the Responsible Entity that provide(s) electronic access controls implemented for Attachment 1, Section 3~~.~~.1, if any.

Section 3. Electronic Access Controls: Examples of evidence for Section 3 may include, but are not limited to:

1. ~~Documentation showing that inbound and outbound connections for any LEAP(s) are confined to only those the Responsible Entity deems necessary (e.g., by restricting IP addresses, ports, or services); and documentation~~Documentation showing that at each asset or group of assets containing low impact BES Cyber Systems, routable communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset is restricted by electronic access controls to permit only inbound and outbound electronic access that the Responsible Entity deems necessary, except where an entity provides rationale that communication is used for time-sensitive protection or control functions between intelligent electronic devices. Examples of such documentation may include, but are not limited to representative diagrams that illustrate control of

inbound and outbound communication(s) between the low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s) or lists of implemented electronic access controls (e.g., access control lists restricting IP addresses, ports, or services; implementing unidirectional gateways).

1.2. Documentation of authentication for Dial-up Connectivity (e.g., dial out only to a preprogrammed number to deliver data, dial-back modems, modems that must be remotely controlled by the control center or control room, or access control on the BES Cyber System).

Section 4. Section 4 - Cyber Security Incident Response: An example of evidence for Section 4 may include, but is not limited to, dated documentation, such as policies, procedures, or process documents of one or more Cyber Security Incident response plan(s) developed either by asset or group of assets that include the following processes:

1. to identify, classify, and respond to Cyber Security Incidents; to determine whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and for notifying the Electricity Sector Information Sharing and Analysis Center (ESE-ISAC);
2. to identify and document the roles and responsibilities for Cyber Security Incident response by groups or individuals (e.g., initiating, documenting, monitoring, reporting, etc.);
3. for incident handling of a Cyber Security Incident (e.g., containment, eradication, or recovery/incident resolution);
4. for testing the plan(s) along with the dated documentation that a test has been completed at least once every 36 calendar months; and
5. to update, as needed, Cyber Security Incident response plan(s) within 180 calendar days after completion of a test or actual Reportable Cyber Security Incident.

Section 5. Transient Cyber Asset and Removable Media Malicious Code Risk Mitigation:

1. Examples of evidence for Section 5.1 may include, but are not limited to, documentation of the method(s) used to mitigate the introduction of malicious code such as antivirus software and processes for managing signature or pattern updates, application whitelisting practices, processes to restrict communication, or other method(s) to mitigate the introduction of malicious code. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the vendor or Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.
2. Examples of evidence for Section 5.2 may include, but are not limited to, documentation from change management systems, electronic mail or

procedures that document a review of the installed antivirus update level; memoranda, electronic mail, system documentation, policies or contracts from the party other than the Responsible Entity that identify the antivirus update process, the use of application whitelisting, use of live operating systems or system hardening performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail or contracts that identifies the Responsible Entity's acceptance that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate malicious code for Transient Cyber Asset(s) managed by a party other than the Responsible Entity. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the Transient Cyber Asset does not have the capability

3. Examples of evidence for Section 5.3.1 may include, but are not limited to, documented process(es) of the method(s) used to detect malicious code such as results of scan settings for Removable Media, or implementation of on-demand scanning. Examples of evidence for Section 5.3.2 may include, but are not limited to, documented process(es) for the method(s) used for mitigating the threat of detected malicious code on Removable Media, such as logs from the method(s) used to detect malicious code that show the results of scanning and the mitigation of detected malicious code on Removable Media or documented confirmation by the entity that the Removable Media was deemed to be free of malicious code.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

In developing policies in compliance with Requirement R1, the number of policies and their content should be guided by a Responsible Entity's management structure and operating conditions. Policies might be included as part of a general information security program for the entire organization, or as components of specific programs. The Responsible Entity has the flexibility to develop a single comprehensive cyber security policy covering the required topics, or it may choose to develop a single high-level umbrella policy and provide additional policy detail in lower level documents in its documentation hierarchy. In the case of a high-level umbrella policy, the Responsible Entity would be expected to provide the high-level policy as well as the additional documentation in order to demonstrate compliance with CIP-003-~~6~~7, Requirement R1.

If a Responsible Entity has any high or medium impact BES Cyber Systems, the one or more cyber security policies must cover the nine subject matter areas required by CIP-003-~~6~~7, Requirement R1, Part 1.1. If a Responsible Entity has identified from CIP-002 any assets containing low impact BES Cyber Systems, the one or more cyber security policies must cover the ~~four~~six subject matter areas required by Requirement R1, Part 1.2.

Responsible Entities that have multiple-impact rated BES Cyber Systems are not required to create separate cyber security policies for high, medium, or low impact BES Cyber Systems. The Responsible Entities have the flexibility to develop policies that cover all three impact ratings.

Implementation of the cyber security policy is not specifically included in CIP-003-~~6~~7, Requirement R1 as it is envisioned that the implementation of this policy is evidenced through successful implementation of CIP-003 through CIP-011. However, Responsible Entities are encouraged not to limit the scope of their cyber security policies to only those requirements in NERC cyber security Reliability Standards, but to develop a holistic cyber security policy

appropriate for its organization. Elements of a policy that extend beyond the scope of NERC's cyber security Reliability Standards will not be considered candidates for potential violations although they will help demonstrate the organization's internal culture of compliance and posture towards cyber security.

For Part 1.1, the Responsible Entity ~~should~~may consider the following for each of the required topics in its one or more cyber security policies for medium and high impact BES Cyber Systems, if any:

1.1.1 Personnel and training (CIP-004)

- Organization position on acceptable background investigations
- Identification of possible disciplinary action for violating this policy
- Account management

1.1.2 Electronic Security Perimeters (CIP-005) including Interactive Remote Access

- Organization stance on use of wireless networks
- Identification of acceptable authentication methods
- Identification of trusted and untrusted resources
- Monitoring and logging of ingress and egress at Electronic Access Points
- Maintaining up-to-date anti-malware software before initiating Interactive Remote Access
- Maintaining up-to-date patch levels for operating systems and applications used to initiate Interactive Remote Access
- Disabling VPN "split-tunneling" or "dual-homed" workstations before initiating Interactive Remote Access
- For vendors, contractors, or consultants: include language in contracts that requires adherence to the Responsible Entity's Interactive Remote Access controls

1.1.3 Physical security of BES Cyber Systems (CIP-006)

- Strategy for protecting Cyber Assets from unauthorized physical access
- Acceptable physical access control methods
- Monitoring and logging of physical ingress

1.1.4 System security management (CIP-007)

- Strategies for system hardening
- Acceptable methods of authentication and access control
- Password policies including length, complexity, enforcement, prevention of brute force attempts
- Monitoring and logging of BES Cyber Systems

1.1.5 Incident reporting and response planning (CIP-008)

- Recognition of Cyber Security Incidents
- Appropriate notifications upon discovery of an incident
- Obligations to report Cyber Security Incidents

1.1.6 Recovery plans for BES Cyber Systems (CIP-009)

- Availability of spare components
- Availability of system backups

1.1.7 Configuration change management and vulnerability assessments (CIP-010)

- Initiation of change requests
- Approval of changes
- Break-fix processes

1.1.8 Information protection (CIP-011)

- Information access control methods
- Notification of unauthorized information disclosure
- Information access on a need-to-know basis

1.1.9 Declaring and responding to CIP Exceptional Circumstances

- Processes to invoke special procedures in the event of a CIP Exceptional Circumstance
- Processes to allow for exceptions to policy that do not violate CIP requirements

For Part 1.2, the Responsible Entity may consider the following for each of the required topics in its one or more cyber security policies for assets containing low impact BES Cyber Systems, if any:

1.2.1 Cyber security awareness

- Method(s) for delivery of security awareness
- Identification of groups to receive cyber security awareness

1.2.2 Physical security controls

- Acceptable approach(es) for selection of physical security control(s)

1.2.3 Electronic access controls

- Acceptable approach(es) for selection of electronic access control(s)

1.2.4 Cyber Security Incident response

- Recognition of Cyber Security Incidents

- Appropriate notifications upon discovery of an incident
- Obligations to report Cyber Security Incidents

1.2.5 Transient Cyber Assets and Removable Media Malicious Code Risk Mitigation

- Acceptable use of Transient Cyber Asset(s) and Removable Media
- Method(s) to mitigate the risk of the introduction of malicious code to low impact BES Cyber Systems from Transient Cyber Assets and Removable Media
- Method(s) to request Transient Cyber Asset and Removable Media

1.2.6 Declaring and responding to CIP Exceptional Circumstances

- Process(es) to declare a CIP Exceptional Circumstance
- Process(es) to respond to a declared CIP Exceptional Circumstance

Requirements relating to exceptions to a Responsible Entity's security policies were removed because it is a general management issue that is not within the scope of a reliability requirement. It is an internal policy requirement and not a reliability requirement. However, Responsible Entities are encouraged to continue this practice as a component of their cyber security policies.

In this and all subsequent required approvals in the NERC CIP Reliability Standards, the Responsible Entity may elect to use hardcopy or electronic approvals to the extent that there is sufficient evidence to ensure the authenticity of the approving party.

Requirement R2:

~~Using the list of assets containing low impact BES Cyber Systems from CIP-002, the intent of the requirement~~The intent of Requirement R2 is for each Responsible Entity to create, document, and implement one or more cyber security plan(s) that ~~addresses~~address the security objective ~~criteria~~ for the protection of low impact BES Cyber Systems. ~~The protections required by Requirement R2 reflect the level of risk that misuse or the unavailability of low impact BES Cyber Systems poses to the BES. The intent is that the~~The required protections are designed to be part of a program that covers the low impact BES Cyber Systems collectively ~~either~~ at an asset ~~or site~~ level (based on the list of assets containing low impact BES Cyber Systems identified in CIP-002), but not at an individual device or system level.

~~There are four subject matter areas, as identified in Attachment 1, that must be covered by the cyber security plan: (1) cyber security awareness, (2) physical security controls, (3) electronic access controls for LERC and **Dial-up Connectivity**, and (4) Cyber Security Incident response.~~

Requirement R2, Attachment 1

As noted, Attachment 1 contains the sections that must be included in the cyber security plan(s). The intent is to allow entities that have a combination of high, medium, and low impact BES Cyber Systems the flexibility to choose, if desired, to cover their low impact BES Cyber Systems (or any subset) under their programs used for the high or medium impact BES Cyber Systems rather than maintain two separate programs. The purpose of the cyber security plan(s) in Requirement R2 is for Responsible Entities to use the cyber security plan(s) as a means of documenting their approaches to meeting the subject matter areas. The cyber security plan(s) can be used to reference other policies and procedures that demonstrate "how" the Responsible Entity is meeting each of the subject matter areas, or Responsible Entities can develop comprehensive cyber security plan(s) that contain all of the detailed implementation content solely within the cyber security plan itself. To meet the obligation for the cyber security plan, the expectation is that the cyber security plan contains or references sufficient details to address the implementation of each of the required subject matters areas.

Guidance for each of the ~~four~~ subject matter areas of Attachment 1 is provided below.

Requirement R2, Attachment 1, Section 1 – Cyber Security Awareness

The intent of the cyber security awareness program is for entities to reinforce good cyber security practices with their personnel at least once every 15 calendar months. The entity has the discretion to determine the topics to be addressed and the manner in which it will communicate these topics. As evidence of compliance, the Responsible Entity should be able to produce the awareness material that was delivered according to the delivery method(s) (e.g., posters, emails, or topics at staff meetings, etc.). The standard drafting team does not intend for Responsible ~~Entity is not~~Entities to be required to maintain lists of recipients and track the reception of the awareness material by personnel.

Although the focus of the awareness is cyber security, it does not mean that only technology-related topics can be included in the program. Appropriate physical security topics (e.g., tailgating awareness and protection of badges for physical security, or "If you see something, say something" campaigns, etc.) are valid for cyber security awareness. The intent is to cover topics concerning any aspect of the protection of BES Cyber Systems.

Requirement R2, Attachment 1, Section 2 – Physical Security Controls

The Responsible Entity must document and implement methods to control physical access to (1) the asset or the locations of low impact BES Cyber Systems ~~at assets containing low impact BES Cyber System(s)~~ within the asset, and (2) ~~LEAPs~~Cyber Assets that implement the electronic access control(s) specified by the Responsible Entity in Attachment 1, Section 3.1, if any. If ~~the LEAP is~~these Cyber Assets implementing the electronic access controls are located within the ~~BES asset and inherits the~~ same ~~controls~~ asset as the low impact BES Cyber Asset(s) and inherit the same physical access controls and the same need as outlined in Section 2, this ~~can~~may be noted by the Responsible Entity in either its policies or cyber security plan(s) to avoid duplicate documentation of the same controls.

The Responsible Entity has the flexibility ~~in the selection of~~to select the methods used to meet the objective ~~to control~~ of controlling physical access to (1) the asset(s) containing low impact BES Cyber ~~Systems,~~System(s) or the low impact BES Cyber Systems themselves~~, or LEAPs~~ and (2) the electronic access control Cyber Assets specified by the Responsible Entity, if any. The Responsible Entity may use one or a combination of physical access controls, monitoring controls, or other operational, procedural, or technical physical security controls. Entities may use perimeter controls (e.g., fences with locked gates, guards, or site access policies, etc.) or more granular areas of physical access control in areas where low impact BES Cyber Systems are located, such as control rooms or control houses. ~~User authorization programs and lists of authorized users for physical access are not required although they are an option to meet the security objective.~~

The security objective is to control the physical access based on need as determined by the Responsible Entity. The need for physical access can be documented at the policy level ~~for access to the site or systems, including LEAPs.~~. The ~~requirement does~~standard drafting team did not intend to obligate an entity to specify a need for each physical access or authorization of ~~a user~~an individual for physical access.

Monitoring as a physical security control can be used as a complement or an alternative to physical access control. Examples of monitoring controls include, but are not limited to: (1) alarm systems to detect motion or entry into a controlled area, or (2) human observation of a controlled area. Monitoring does not necessarily require logging and maintaining logs but could include monitoring that physical access has occurred or been attempted (e.g., door alarm, or human observation, etc.). ~~The~~The standard drafting team's intent is that the monitoring does not need to be per low impact BES Cyber System but should be at the appropriate level to meet the security objective of controlling physical access.

User authorization programs and lists of authorized users for physical access are not required although they are an option to meet the security objective.

Requirement R2, Attachment 1, Section 3 – Electronic Access Controls

Section 3 requires the establishment of ~~boundary protections~~electronic access controls for assets containing low impact BES Cyber Systems when ~~the low impact BES Cyber Systems have bi-directional~~there is routable protocol communication or Dial-up Connectivity ~~to devices external to~~ between Cyber Asset(s) outside of the asset containing the low impact BES Cyber ~~Systems. The establishment of boundary protections is intended to control communication either into the asset containing low impact BES Cyber~~ System(s) ~~or to~~and the low impact BES Cyber System ~~itself to~~ (s) within such asset. The establishment of electronic access controls is intended to reduce the risks associated with uncontrolled communication using routable protocols or Dial-up Connectivity. ~~The term "electronic access control" is used in the general sense, i.e., to control access, and not in the specific technical sense requiring authentication, authorization, and auditing. The Responsible Entity is not required to establish LERC communication or a LEAP if there is no bi-directional routable protocol communication or Dial-up Connectivity present. In the case where there is no external bi-directional routable protocol communication or Dial-up Connectivity, the Responsible Entity can document the absence of such communication in its low impact cyber security plan(s).~~

~~The defined terms LERC~~When implementing Attachment 1, Section 3.1, Responsible Entities should note that electronic access controls to permit only necessary inbound and ~~LEAP~~outbound electronic access are ~~used to avoid confusion with the similar terms used~~required for ~~high~~communications when those communications meet all three of the criteria identified in Attachment 1, Section 3.1. The Responsible Entity should evaluate the communications and ~~medium~~when all three criteria are met, the Responsible Entity must document and implement electronic access control(s).

When identifying electronic access controls, Responsible Entities are provided flexibility in the selection of the electronic access controls that meet their operational needs while meeting the security objective of allowing only necessary inbound and outbound electronic access to low impact BES Cyber Systems ~~(e.g., External Routable~~that use routable protocols between a low impact BES Cyber System(s) and Cyber Asset(s) outside the asset.

In essence, the intent is for Responsible Entities to determine whether there is communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s) that uses a routable protocol when entering or leaving the asset or Dial-up Connectivity ~~(ERC) or~~ to the low impact BES Cyber System(s). Where such communication is present, Responsible Entities should document and implement electronic access control(s). Where routable protocol communication for time-sensitive protection or control functions between intelligent electronic devices that meets the exclusion language is present, Responsible Entities should document that communication, but are not required to establish any specific electronic access controls.

The inputs to this requirement are the assets identified in CIP-002 as containing low impact BES Cyber System(s); therefore, the determination of routable protocol communications or Dial-up Connectivity is an attribute of the asset. However, it is not intended for communication that provides no access to or from the low impact BES Cyber System(s), but happens to be located at the asset with the low impact BES Cyber System(s), to be evaluated for electronic access controls.

Electronic Access ~~Point (EAP)). To future-proof the standards, and in~~Control Exclusion

In order to avoid future technology issues, the ~~definitions specifically~~obligations for electronic access controls exclude ~~"point-to-point~~ communications between intelligent electronic devices that use routable communication protocols for time-sensitive protection or control functions ~~between Transmission station or substation assets containing low impact BES Cyber Systems,",~~ such as IEC TR-61850-90-5 R-GOOSE messaging. ~~This does not exclude Control Center communication but rather excludes the communication between the intelligent electronic devices themselves.~~Time-sensitive in this context generally means functions that would be negatively impacted by the latency introduced in the communications by the required electronic access controls. This time-sensitivity exclusion does not apply to SCADA communications which typically operate on scan rates of 2 seconds or greater. While technically time-sensitive, SCADA communications over routable protocols can withstand the delay introduced by electronic access controls. Examples of excluded time-sensitive communications are those communications which may necessitate the tripping of a breaker within a few cycles. A Responsible Entity using this technology is not expected to implement ~~a~~

~~LEAP.~~the electronic access controls noted herein. This exception was included so as not to inhibit the functionality of the time-sensitive ~~requirements~~characteristics related to this technology ~~nor~~and not to preclude the use of such time-sensitive reliability enhancing functions if they use a routable protocol in the future.

~~When determining whether~~ **Considerations for Determining Routable Protocol Communications**

To determine whether electronic access controls need to be implemented, the Responsible Entity has to determine whether there is ~~LERC to the low impact BES Cyber System, the definition uses the phrases "direct user-initiated interactive access or a direct device-to-device connection to~~ communication between a low impact BES Cyber System(s) ~~from~~and a Cyber Asset(s) outside the asset containing ~~those~~the low impact BES Cyber System(s) ~~via~~that uses a routable protocol when entering or leaving the asset.

When determining whether a ~~bi-directional~~ routable protocol ~~connection." The intent of "direct" in the definition~~ is ~~to indicate LERC exists if a person is sitting at another device outside of~~entering or leaving the asset containing the low impact BES Cyber System~~, and~~ (s), Responsible Entities have flexibility in identifying an approach. One approach is for Responsible Entities to identify an "electronic boundary" associated with the asset containing low impact BES Cyber System(s). This is not an Electronic Security Perimeter *per se*, but a demarcation that demonstrates the ~~person can connect to logon, configure, read, or interact, etc. with the low impact BES Cyber System using a bi-directional routable protocol within a single end-to-end protocol session even if there is a serial-to-~~routable protocol ~~conversion. The reverse case would also be LERC, in which the individual sits at the~~communication entering or leaving the asset between a low impact BES Cyber System and ~~connects~~ Cyber Asset(s) outside the asset to then have electronic access controls implemented. This electronic boundary may vary by asset type (Control Center, substation, generation resource) and the specific configuration of the asset. If this approach is used, the intent is for the Responsible Entity to define the electronic boundary such that the low impact BES Cyber System(s) located at the asset are contained within the "electronic boundary." This is strictly for determining which routable protocol communications and networks are internal or inside or local to the asset and which are external to or outside the asset.

Alternatively, the Responsible Entity may find the concepts of what is inside and outside to ~~a device~~ be intuitively obvious for a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s) communicating to a low impact BES Cyber System(s) inside the asset. This may be the case when a low impact BES Cyber System(s) is communicating with a Cyber Asset many miles away and a clear and unambiguous demarcation exists. In this case, a Responsible Entity may decide not to identify an "electronic boundary," but rather to simply leverage the unambiguous asset demarcation to ensure that the electronic access controls are placed between the low impact BES Cyber System(s) and the Cyber Asset(s) outside the asset.

Determining Electronic Access Controls

Once a Responsible Entity has determined that there is routable communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s) that uses a routable protocol when entering or leaving the asset containing

the low impact BES Cyber System(s), the intent is for the Responsible Entity to document and implement its chosen electronic access control(s). The control(s) are intended to allow only "necessary" inbound and outbound electronic access as determined by the Responsible Entity. However the Responsible Entity chooses to document the inbound and outbound access permissions and the need, the intent is that the Responsible Entity is able to explain the reasons for the electronic access permitted. The reasoning for "necessary" inbound and outbound electronic access controls may be documented within the Responsible Entity's cyber security plan(s), within a comment on an access control list, a database, spreadsheet or other policies or procedures associated with the electronic access controls.

Concept Diagrams

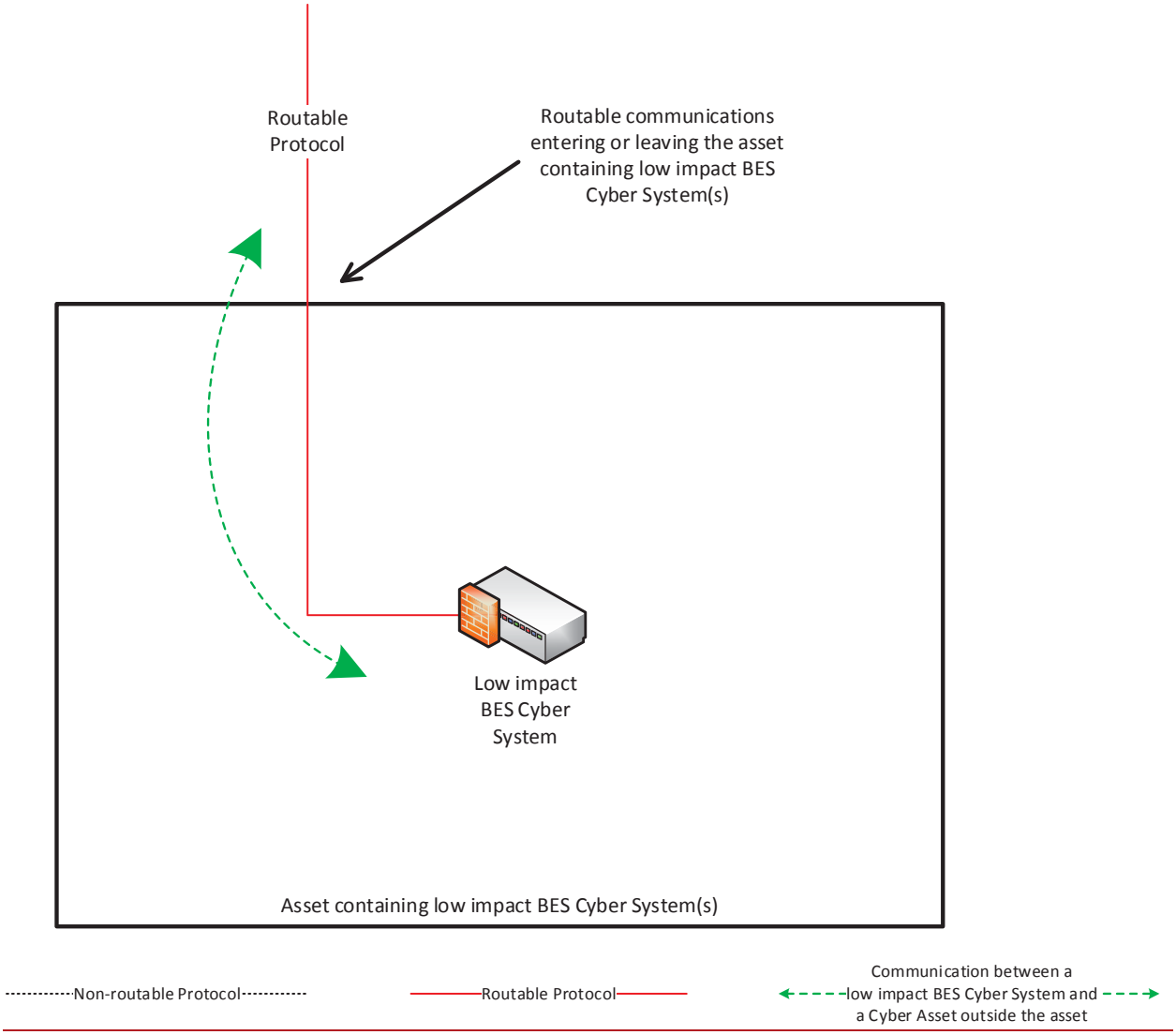
The diagrams on the following pages are provided as examples to illustrate various electronic access controls at a conceptual level. Regardless of the concepts or configurations chosen by the Responsible Entity, the intent is to achieve the security objective of permitting only necessary inbound and outbound electronic access for communication between low impact BES Cyber Systems and Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s) using a routable protocol when entering or leaving the asset.

NOTE:

- This is not an exhaustive list of applicable concepts.
- The same legend is used in each diagram; however, the diagram may not contain all of the articles represented in the legend.

Reference Model 1 – Host-based Inbound & Outbound Access Permissions

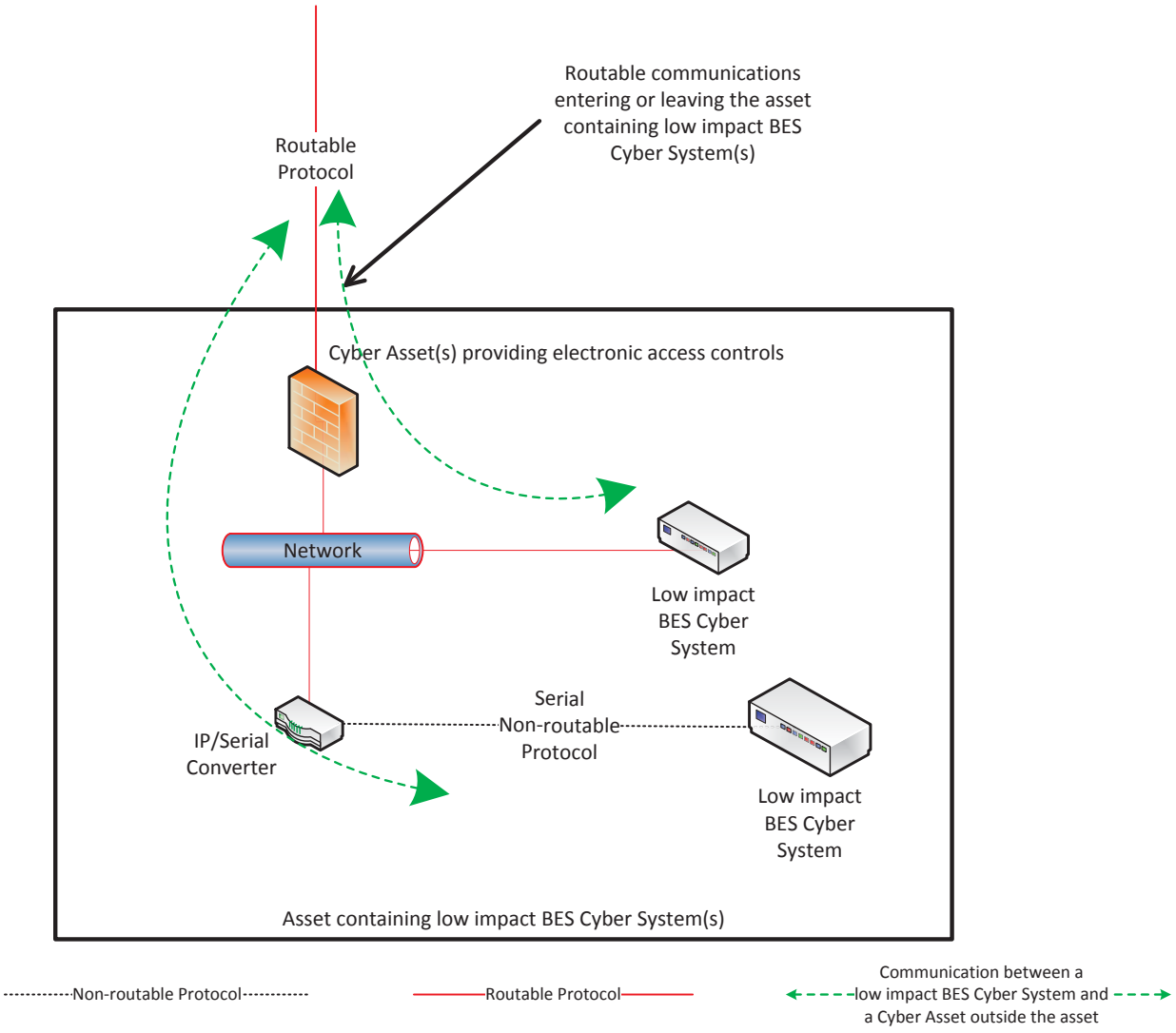
The Responsible Entity may choose to utilize a host-based firewall technology on the low impact BES Cyber System(s) itself that manages the inbound and outbound electronic access permissions so that only necessary inbound and outbound electronic access is allowed between the low impact BES Cyber System(s) and the Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s). When permitting the inbound and outbound electronic access permissions using access control lists, the Responsible Entity could restrict communication(s) using source and destination addresses or ranges of addresses. Responsible Entities could also restrict communication(s) using ports or services based on the capability of the electronic access control, the low impact BES Cyber System(s), or the application(s).



Reference Model 1

Reference Model 2 – Network-based Inbound & Outbound Access Permissions

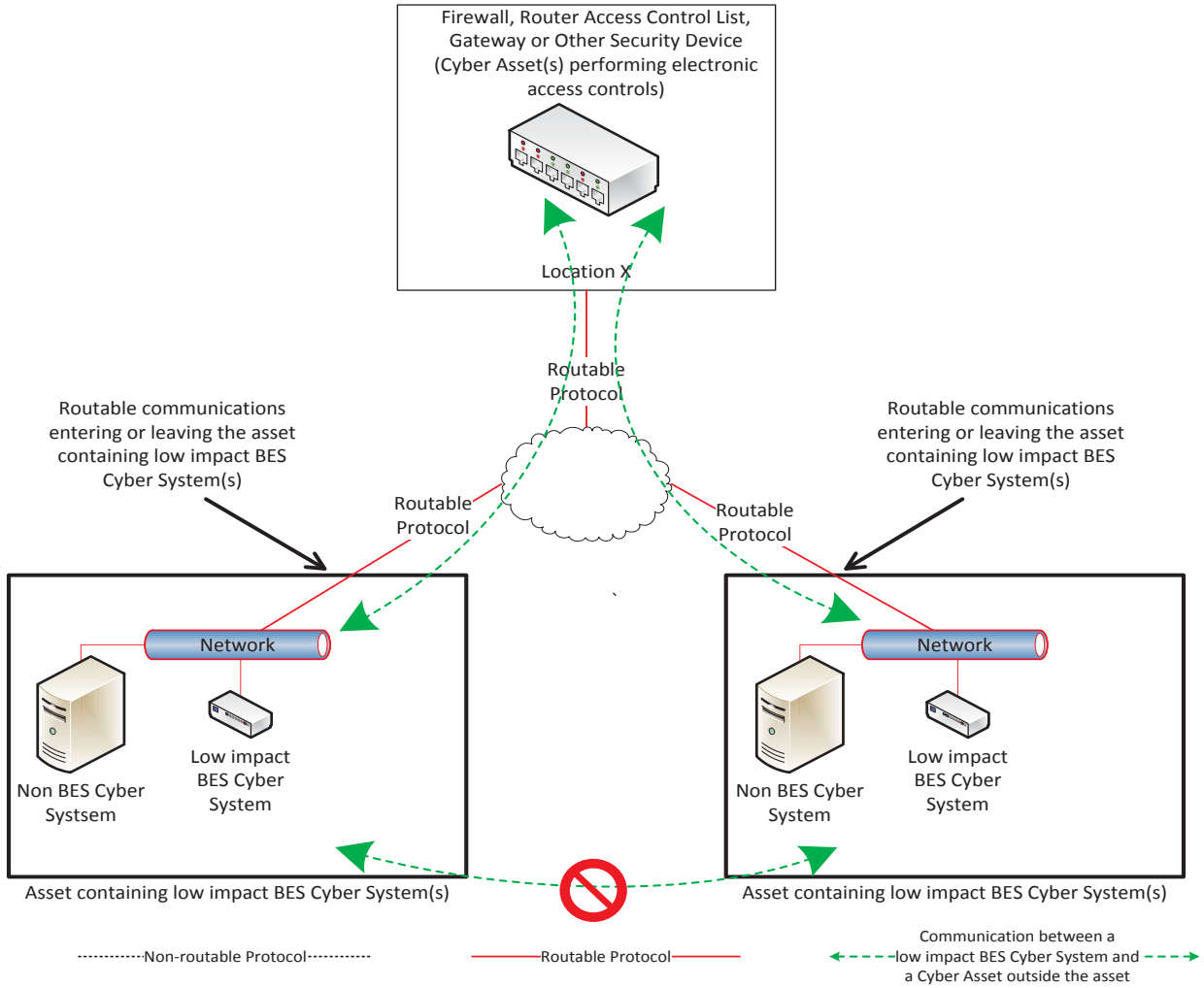
The Responsible Entity may choose to use a security device that permits only necessary inbound and outbound electronic access to the low impact BES Cyber System(s) within the asset containing the low impact BES Cyber System(s). In this example, two low impact BES Cyber Systems are accessed using the routable protocol that is entering or leaving the asset containing the low impact BES Cyber System(s). The IP/Serial converter is continuing the same communications session from the Cyber Asset(s) that are outside the asset to the low impact BES Cyber System(s). The security device provides the electronic access controls to permit only necessary inbound and outbound routable protocol access to the low impact BES Cyber System(s). When permitting the inbound and outbound electronic access permissions using access control lists, the Responsible Entity could restrict communication(s) using source and destination addresses or ranges of addresses. Responsible Entities could also restrict communication(s) using ports or services based on the capability of the electronic access control, the low impact BES Cyber System(s), or the application(s).



Reference Model 2

Reference Model 3 – Centralized Network-based Inbound & Outbound Access Permissions

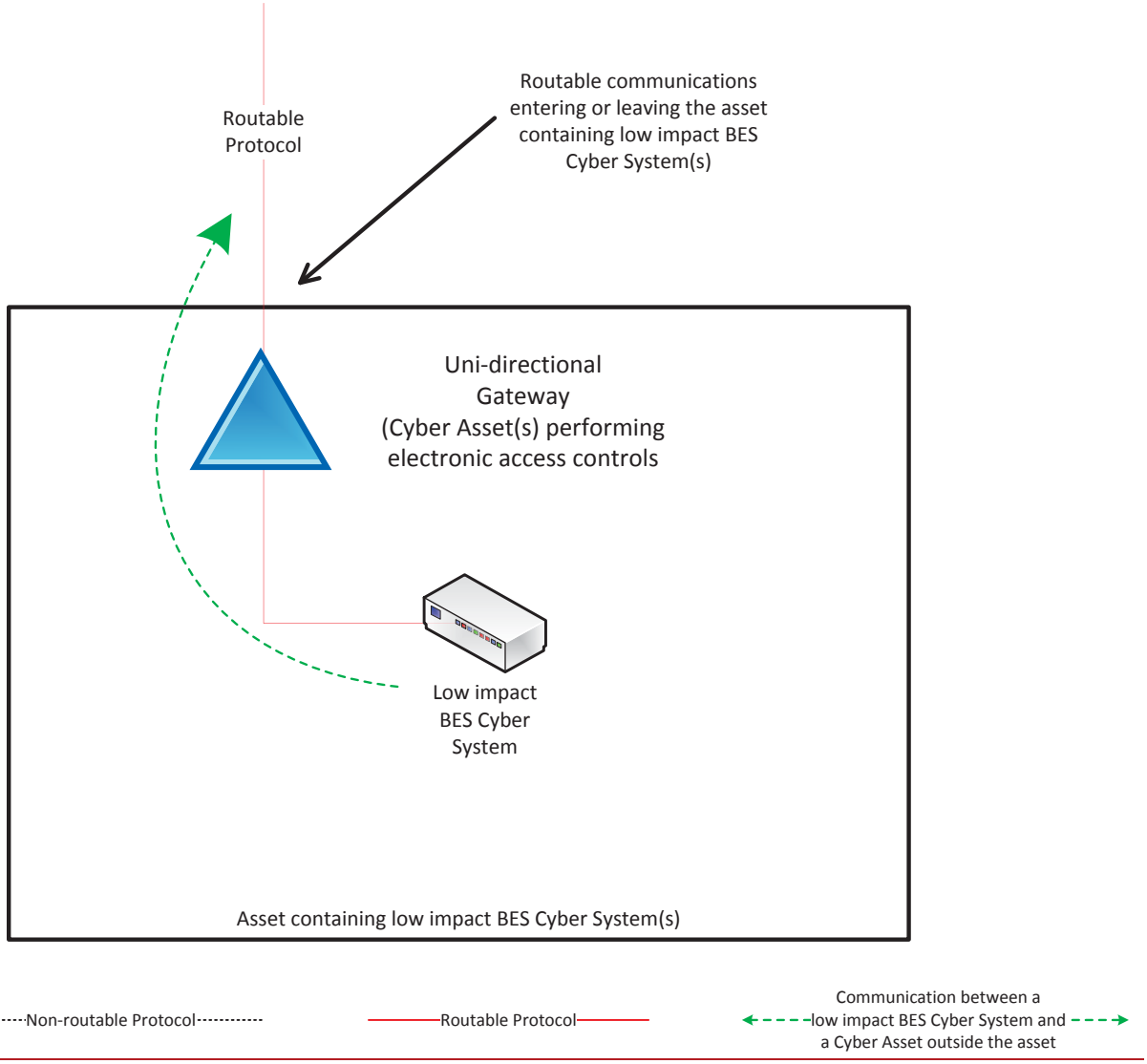
The Responsible Entity may choose to utilize a security device at a centralized location that may or may not be at another asset containing low impact BES Cyber System(s). The electronic access control(s) do not necessarily have to reside inside the asset containing the low impact BES Cyber System(s). A security device is in place at "Location X" to act as the electronic access control and permit only necessary inbound and outbound routable protocol access between the low impact BES Cyber System(s) and the Cyber Asset(s) outside each asset containing low impact BES Cyber System(s). Care should be taken that electronic access to or between each asset is through the Cyber Asset(s) determined by the Responsible Entity to be performing electronic access controls at the centralized location. When permitting the inbound and outbound electronic access permissions using access control lists, the Responsible Entity could restrict communication(s) using source and destination addresses or ranges of addresses. Responsible Entities could also restrict communication(s) using ports or services based on the capability of the electronic access control, the low impact BES Cyber System(s), or the application(s).



Reference Model 3

Reference Model 4 – Uni-directional Gateway

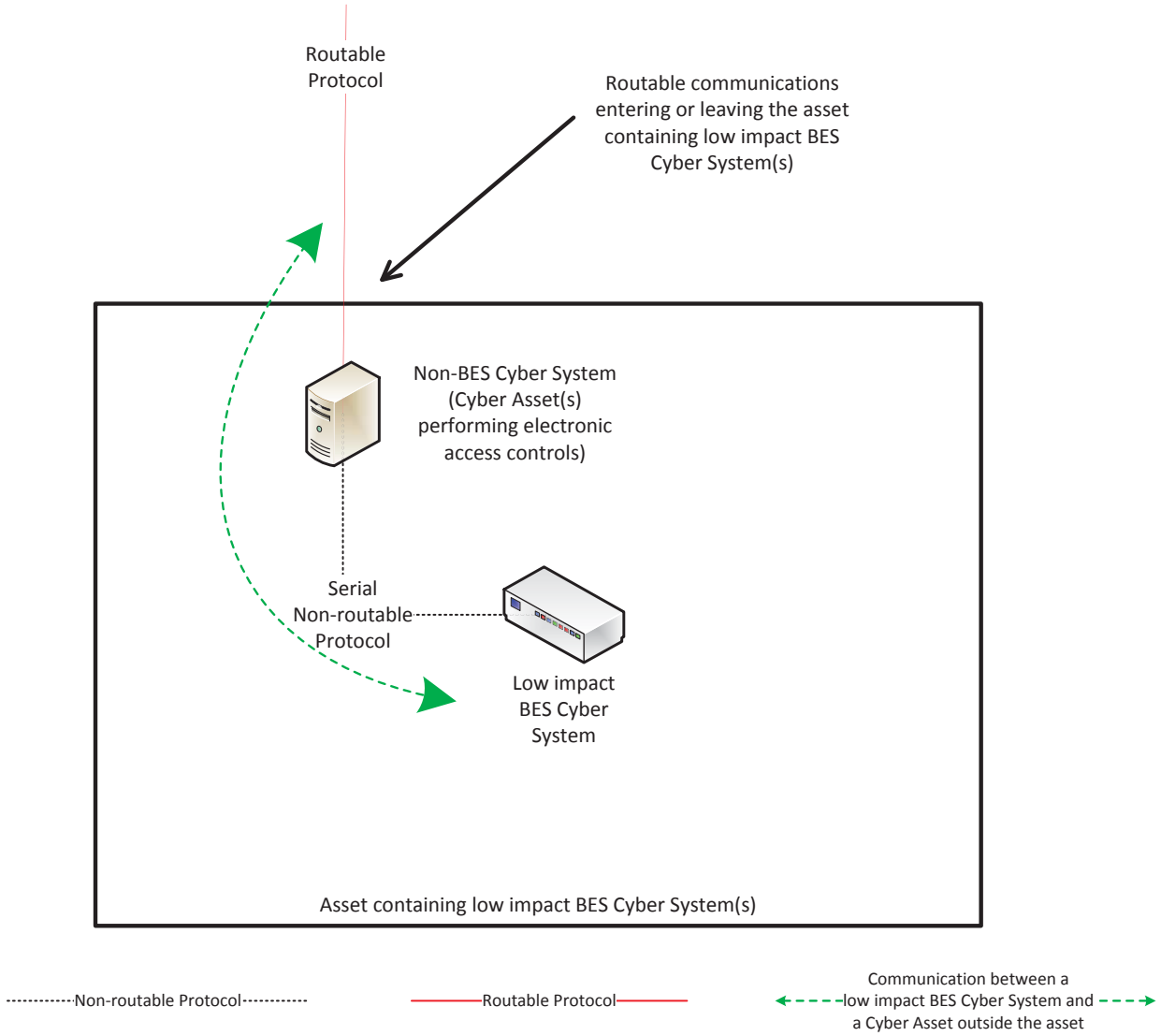
The Responsible Entity may choose to utilize a uni-directional gateway as the electronic access control. The low impact BES Cyber System(s) is not accessible (data cannot flow into the low impact BES Cyber System) using the routable protocol entering the asset due to the implementation of a "one-way" (uni-directional) path for data to flow. The uni-directional gateway is configured to permit only the necessary outbound communications using the routable protocol communication leaving the asset.



Reference Model 4 ~~*Systems using a single end-to-end bi-directional routable protocol session. Additionally, for "device-to-*~~

Reference Model 5 – User Authentication

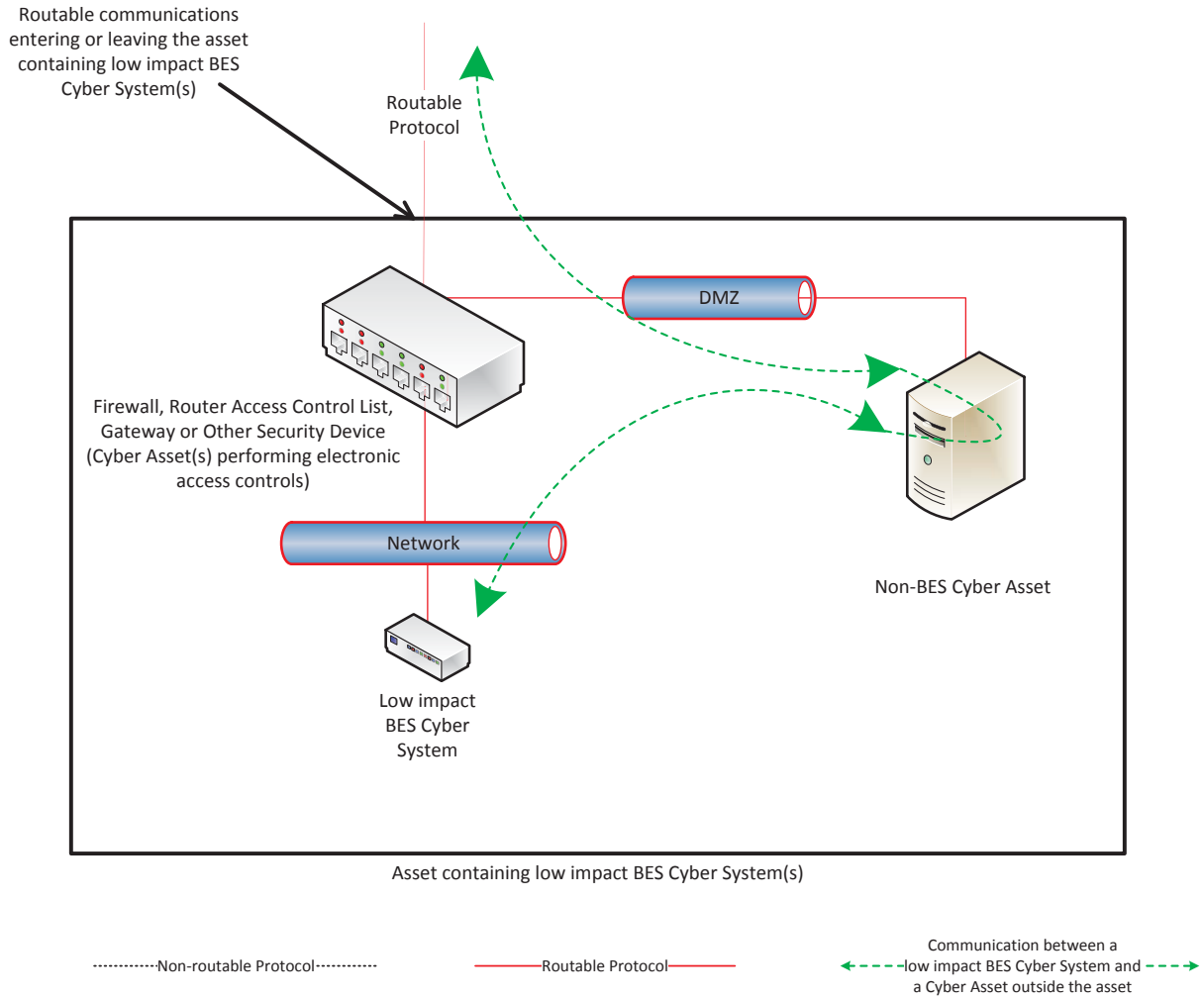
This reference model demonstrates that Responsible Entities have flexibility in choosing electronic access controls so long as the security objective of the requirement is met. The Responsible Entity may choose to utilize a non-BES Cyber Asset located at the asset containing the low impact BES Cyber System that requires authentication for communication from the Cyber Asset(s) outside the asset. This non-BES Cyber System performing the authentication permits only authenticated communication to connect to the low impact BES Cyber System(s), meeting the first half of the security objective to permit only necessary inbound electronic access. Additionally, the non-BES Cyber System performing authentication is configured such that it permits only necessary outbound communication meeting the second half of the security objective. Often, the outbound communications would be controlled in this network architecture by permitting no communication to be initiated from the low impact BES Cyber System. This configuration may be beneficial when the only communication to a device is for user-initiated interactive access.



Reference Model 5

Reference Model 6 – Indirect Access

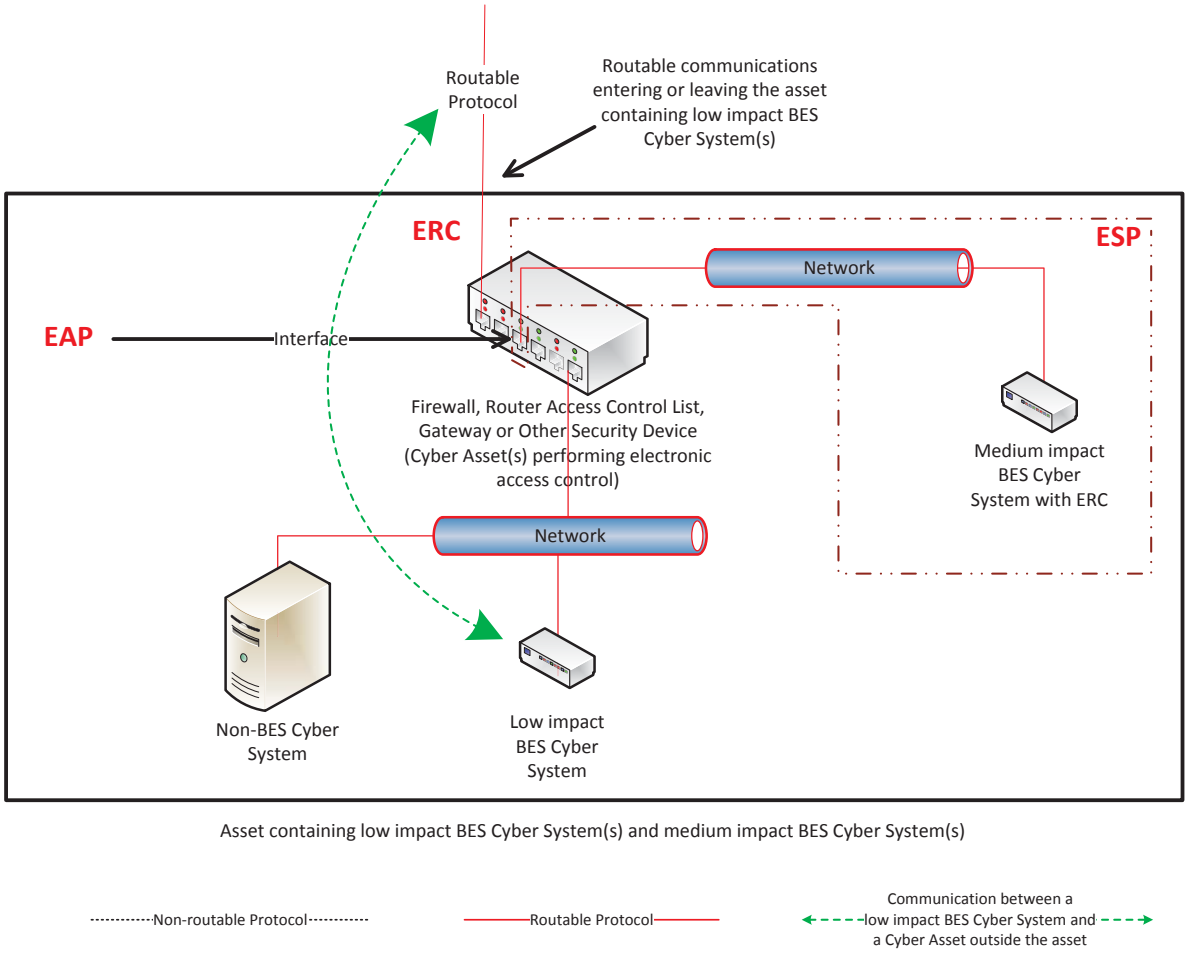
In implementing its electronic access controls, the Responsible Entity may identify that it has indirect access between the low impact BES Cyber System and a Cyber Asset outside the asset containing the low impact BES Cyber System through a non-BES Cyber Asset located within the asset. This indirect access meets the criteria of having communication between the low impact BES Cyber System and a Cyber Asset outside the asset containing the low impact BES Cyber System. In this reference model, it is intended that the Responsible Entity implement electronic access controls that permit only necessary inbound and outbound electronic access to the low impact BES Cyber System. Consistent with the other reference models provided, the electronic access in this reference model is controlled using the security device ~~connection," LERC exists if the Responsible Entity has devices outside of the asset containing the low impact BES Cyber System sending or receiving bi-directional routable communication to or from the low impact BES Cyber System.~~ that is restricting the communication that is entering or leaving the asset.



Reference Model 6

Reference Model 7 – Electronic Access Controls at assets containing low impact BES Cyber Systems and ERC

In this reference model, there is both a routable protocol entering and leaving the asset containing the low impact BES Cyber System(s) that is used by Cyber Asset(s) outside the asset and External Routable Connectivity because there is at least one medium impact BES Cyber System and one low impact BES Cyber System within the asset using the routable protocol communications. The Responsible Entity may choose to leverage an interface on the medium impact Electronic Access Control or Monitoring Systems (EACMS) to provide electronic access controls for purposes of CIP-003. The EACMS is therefore performing multiple functions – as a medium impact EACMS and as implementing electronic access controls for an asset containing low impact BES Cyber Systems.

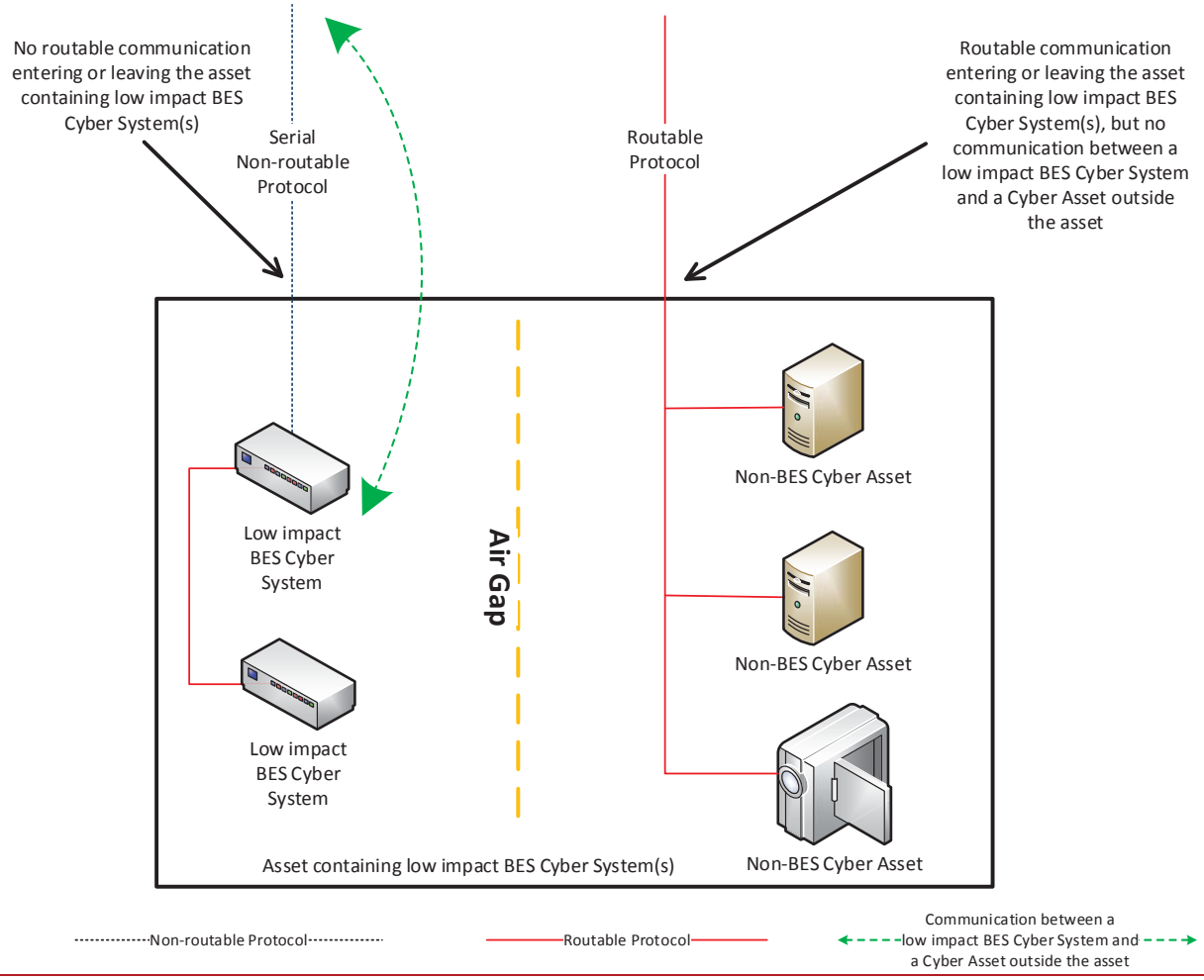


Reference Model 7

Reference Model 8 – Physical Isolation and Serial Non-routable Communications – No Electronic Access Controls Required

In this reference model, the criteria from Attachment 1, Section 3.1 requiring the implementation of electronic access controls are not met. This reference model demonstrates three concepts:

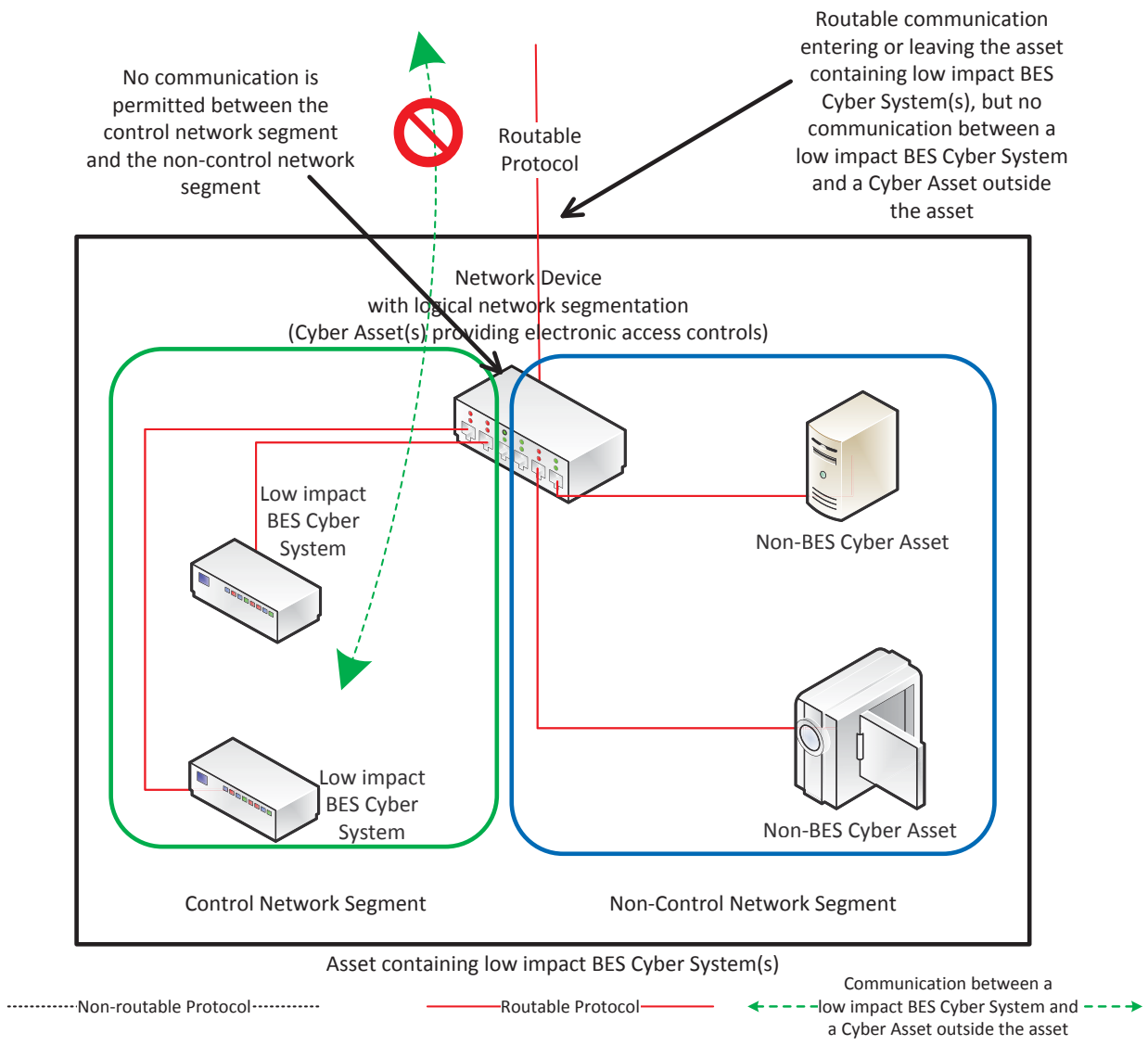
1) The physical isolation of the low impact BES Cyber System(s) from the routable protocol communication entering or leaving the asset containing the low impact BES Cyber System(s), commonly referred to as an 'air gap', mitigates the need to implement the required electronic access controls;
2) The communication to the low impact BES Cyber System from a Cyber Asset outside the asset containing the low impact BES Cyber System(s) using only a serial non-routable protocol where such communication is entering or leaving the asset mitigates the need to implement the required electronic access controls.
3) The routable protocol communication between the low impact BES Cyber System(s) and other Cyber Asset(s), such as the second low impact BES Cyber System depicted, may exist without needing to implement the required electronic access controls so long as the routable protocol communications never leaves the asset containing the low impact BES Cyber System(s).



Reference Model 8

Reference Model 9 – Logical Isolation - No Electronic Access Controls Required

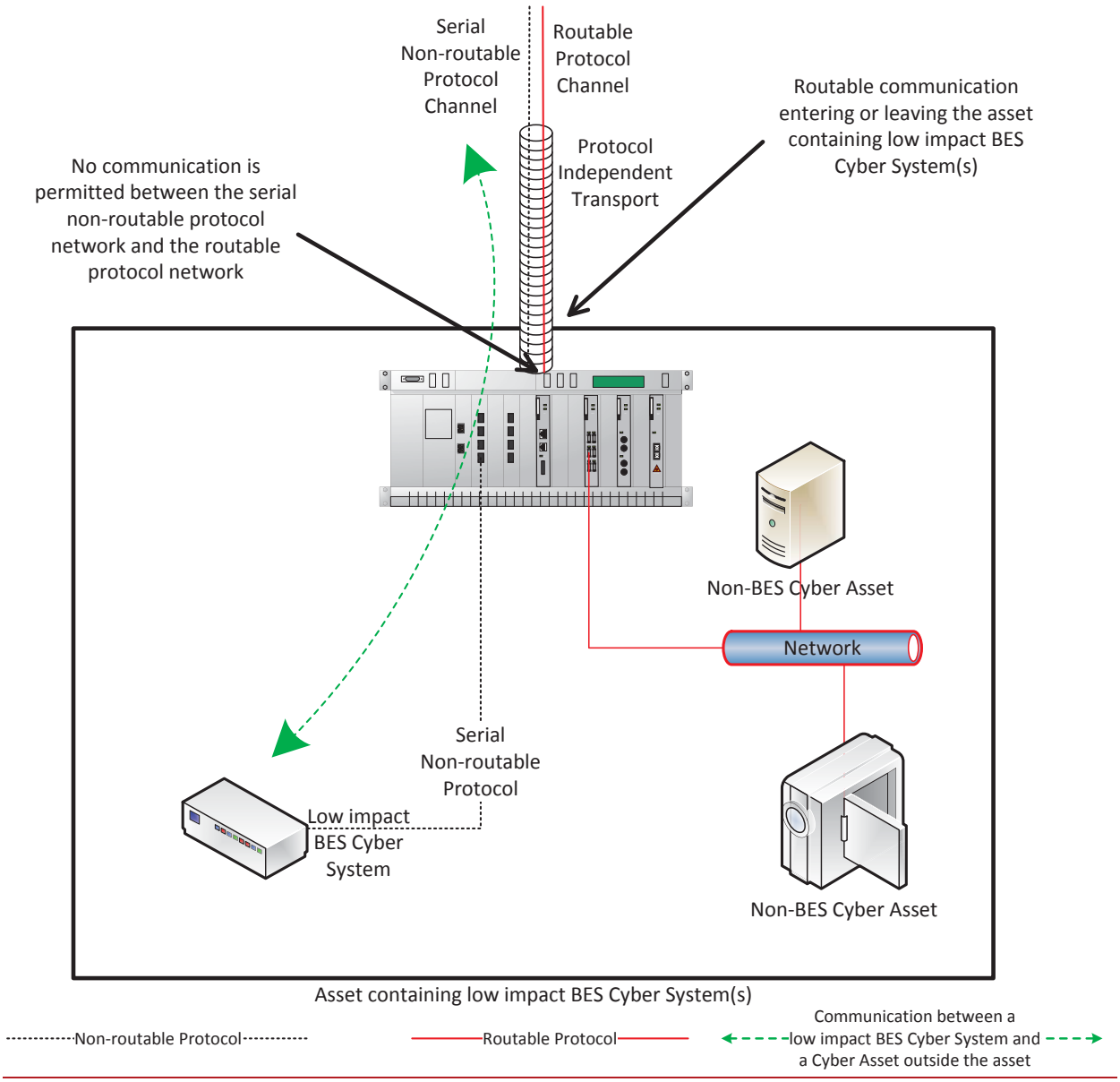
In this reference model, the criteria from Attachment 1, Section 3.1 requiring the implementation of electronic access controls are not met. The Responsible Entity has logically isolated the low impact BES Cyber System(s) from the routable protocol communication entering or leaving the asset containing low impact BES Cyber System(s). The logical network segmentation in this reference model permits no communication between a low impact BES Cyber System and a Cyber Asset outside the asset. Additionally, no indirect access exists because those non-BES Cyber Assets that are able to communicate outside the asset are strictly prohibited from communicating to the low impact BES Cyber System(s). The low impact BES Cyber System(s) is on an isolated network segment with logical controls preventing routable protocol communication into or out of the network containing the low impact BES Cyber System(s) and these communications never leave the asset using a routable protocol.



Reference Model 9

Reference Model 10 - Serial Non-routable Communications Traversing an Isolated Channel on a Non-routable Transport Network – No Electronic Access Controls Required

In this reference model, the criteria from Attachment 1, Section 3.1 requiring the implementation of electronic access controls are not met. This reference model depicts communication between a low impact BES Cyber System and a Cyber Asset outside the asset containing the low impact BES Cyber System over a serial non-routable protocol which is transported across a wide-area network using a protocol independent transport that may carry routable and non-routable communication such as a Time-Division Multiplexing (TDM) network, a Synchronous Optical Network (SONET), or a Multiprotocol Label Switching (MPLS) network. While there is routable protocol communication entering or leaving the asset containing low impact BES Cyber Systems(s) and there is communication between a low impact BES Cyber System and a Cyber Asset outside the asset, the communication between the low impact BES Cyber System and the Cyber Asset outside the asset is not using the routable protocol communication. This model is related to Reference Model 9 in that it relies on logical isolation to prohibit the communication between a low impact BES Cyber System and a Cyber Asset outside the asset from using a routable protocol.



Reference Model 10

Dial-up Connectivity

When identifying a LEAP, Responsible Entities are provided flexibility in the selection of the interface on a Cyber Asset that controls the LERC. Examples include, but are not limited to, the internal (facing the low impact BES Cyber Systems) interface on an external or host-based firewall, the internal interface on a router that has implemented an access control list (ACL), or other security device. The entity also has flexibility with respect to the location of the LEAP. LEAPs are not required to reside at the asset containing the low impact BES Cyber Systems. Furthermore, the entity is not required to establish a unique physical LEAP per asset containing low impact BES Cyber Systems. Responsible Entities can have a single Cyber Asset containing multiple LEAPs that controls the LERC for more than one asset containing low impact BES Cyber Systems. Locating the Cyber Asset with multiple LEAPs at an external location with multiple assets containing low impact BES Cyber Systems "behind" it, however, should not allow uncontrolled access to assets containing low impact BES Cyber Systems sharing a Cyber Asset containing the LEAP(s).

In Reference Model 4, the communication flows through an IP/Serial converter. LERC is correctly identified in this Reference Model because the IP/Serial converter in this instance is doing nothing more than extending the communication between the low impact BES Cyber System and the Cyber Asset outside the asset containing the low impact BES Cyber System. In contrast, Reference Model 6 has placed a Cyber Asset that performs a complete break or interruption that does not allow the user or device data flow to directly communicate with the low impact BES Cyber System. The Cyber Asset in Reference Model 6 is preventing extending access to the low impact BES Cyber System from the Cyber Asset outside the asset containing the low impact BES Cyber System. The intent is that if the IP/Serial converter that is deployed only does a "pass-through" of the data flow communication, then that "pass-through" data flow communication is LERC and a LEAP is required. However, if that IP/Serial converter performs some type of authentication in the data flow at the asset containing the low impact BES Cyber System before the communication can be sent to the low impact BES Cyber System, then that type of IP/Serial converter implementation is not LERC.

A Cyber Asset that contains interface(s) that only perform the function of a LEAP does not meet the definition of Electronic Access Control or Monitoring System (EACMS) associated with medium or high impact BES Cyber Systems and is not subject to the requirements applicable to an EACMS. However, a Cyber Asset may contain some interfaces that function as a LEAP and other interfaces that function as an EAP for high or medium impact BES Cyber Systems. In this case, the Cyber Asset would also be subject to the requirements applicable to the EACMS associated with the medium or high impact BES Cyber Systems.

Examples of sufficient access controls may include:

- Any LERC for the asset passes through a LEAP with explicit inbound and outbound access permissions defined, or equivalent method by which both inbound and outbound connections are confined to only those that the Responsible Entity deems necessary (e.g., IP addresses, ports, or services).
- As shown in Reference Model 1 below, the low impact BES Cyber System has a host-based firewall that is controlling the inbound and outbound access. In this

~~model, it is also possible that the host-based firewall could be on a non-BES Cyber Asset. The intent is that the host-based firewall controls the inbound and outbound access between the low impact BES Cyber System and the Cyber Asset in the business network.~~

- ~~As shown in Reference Model 5 below, a non-BES Cyber Asset has been placed between the low impact BES Cyber System on the substation network and the Cyber Asset in the business network. The expectation is that the non-BES Cyber Asset has provided a "protocol break" so that access to the low impact BES Cyber System is only from the non-BES Cyber Asset that is located within the asset containing the low impact BES Cyber System.~~

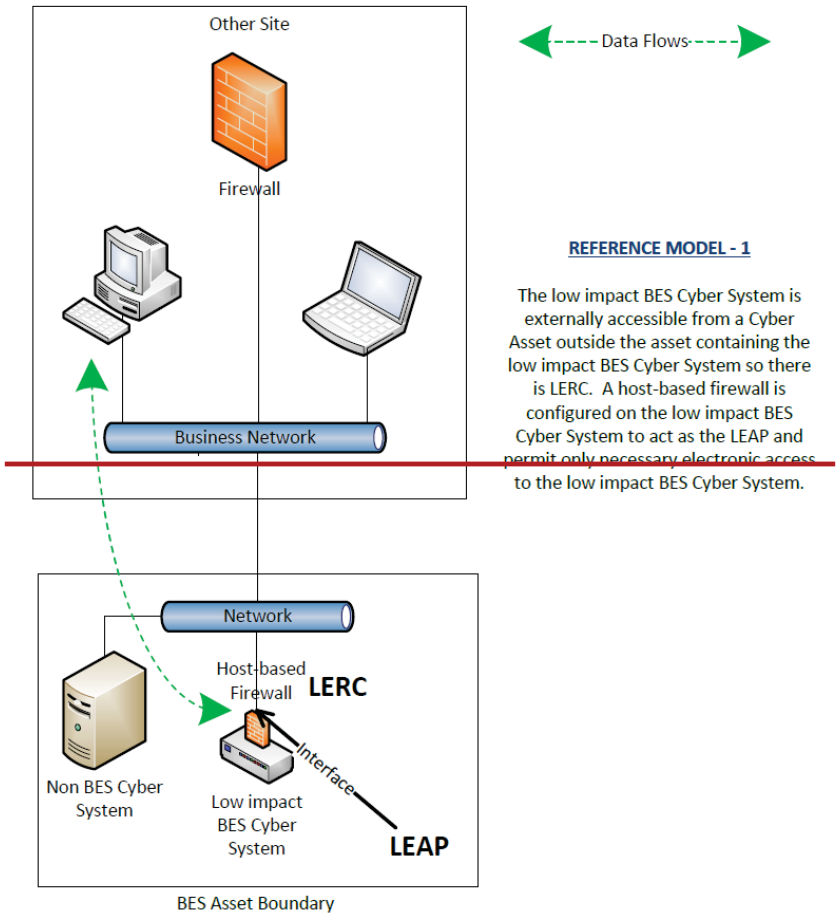
Dial-up Connectivity to a low impact BES Cyber System is set to dial out only (no auto-answer) to a preprogrammed number to deliver data. Incoming Dial-up Connectivity is to a dialback modem, a modem that must be remotely controlled by the control center or control room, has some form of access control, or the low impact BES Cyber System has access control.

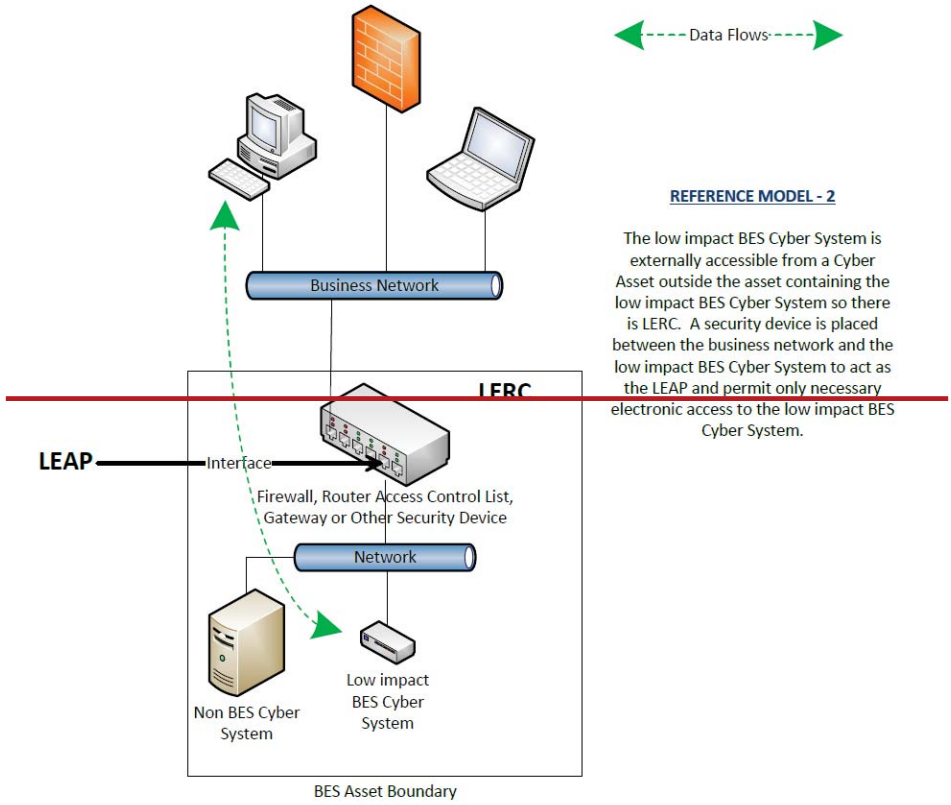
Insufficient Access Controls

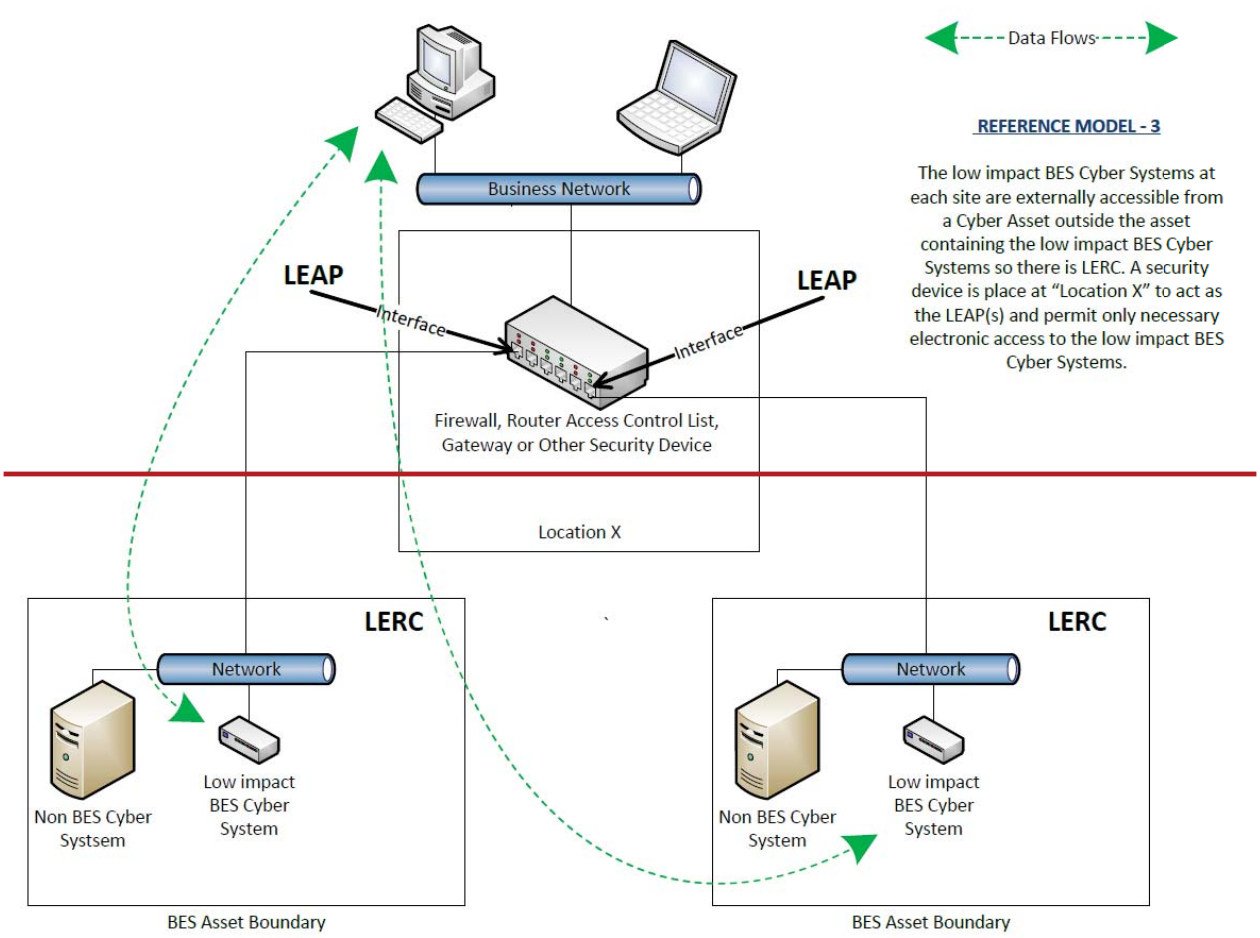
Some examples of situations that would lack sufficient access controls to meet the intent of this requirement include:

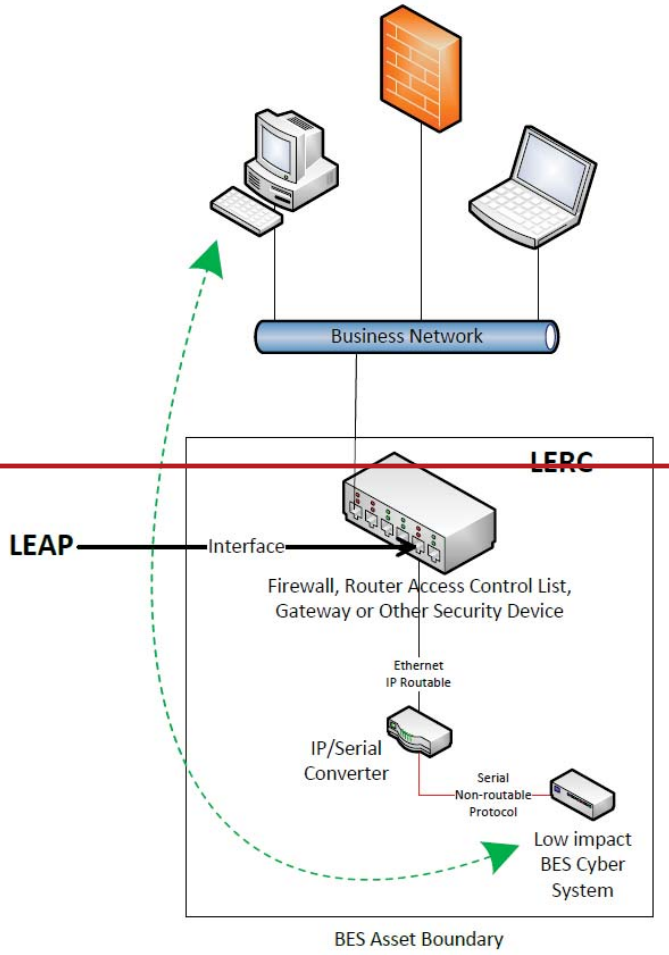
- An asset has Dial-up Connectivity and a low impact BES Cyber System is reachable via an auto-answer modem that connects any caller to the Cyber Asset that has a default password. There is no practical access control in this instance.
- ~~An asset has LERC due to a~~A low impact BES Cyber System ~~within it having~~has a wireless card on a public carrier that allows the BES Cyber System to be reachable via a public IP address. In essence, low impact BES Cyber Systems should not be accessible from the Internet and search engines such as Shodan.
- ~~In Reference Model 5, using just dual~~Dual-homing or multiple-network interface cards without disabling IP forwarding in the non-BES Cyber Asset within the DMZ to provide separation between the low impact BES Cyber System(s) and the ~~business~~external network would not meet the intent of "controlling" inbound and outbound electronic access assuming there was no other host-based firewall or other security ~~device~~devices on ~~that~~the non-BES Cyber Asset.

~~The following diagrams provide reference examples intended to illustrate how to determine whether there is LERC and for implementing a LEAP. While these diagrams identify several possible configurations, Responsible Entities may have additional configurations not identified below.~~


Other Site
Data Flows
Firewall
Business Network
REFERENCE MODEL - 1
The low impact BES Cyber System is externally accessible from a Cyber Asset outside the asset containing the low impact BES Cyber System so there is LERC. A host-based firewall is configured on the low impact BES Cyber System to act as the LEAP and permit only necessary electronic access to the low impact BES Cyber System.
Network
Host-based Firewall
LERC
Interface
Non BES Cyber System
Low impact BES Cyber System
LEAP
BES Asset Boundary


Data Flows
REFERENCE MODEL - 2
The low impact BES Cyber System is externally accessible from a Cyber Asset outside the asset containing the low impact BES Cyber System so there is LERC. A security device is placed between the business network and the low impact BES Cyber System to act as the LEAP and permit only necessary electronic access to the low impact BES Cyber System.
Business Network
LERC
LEAP
Interface
Firewall, Router Access Control List, Gateway or Other Security Device
Network
Non BES Cyber System
Low impact BES Cyber System
BES Asset Boundary

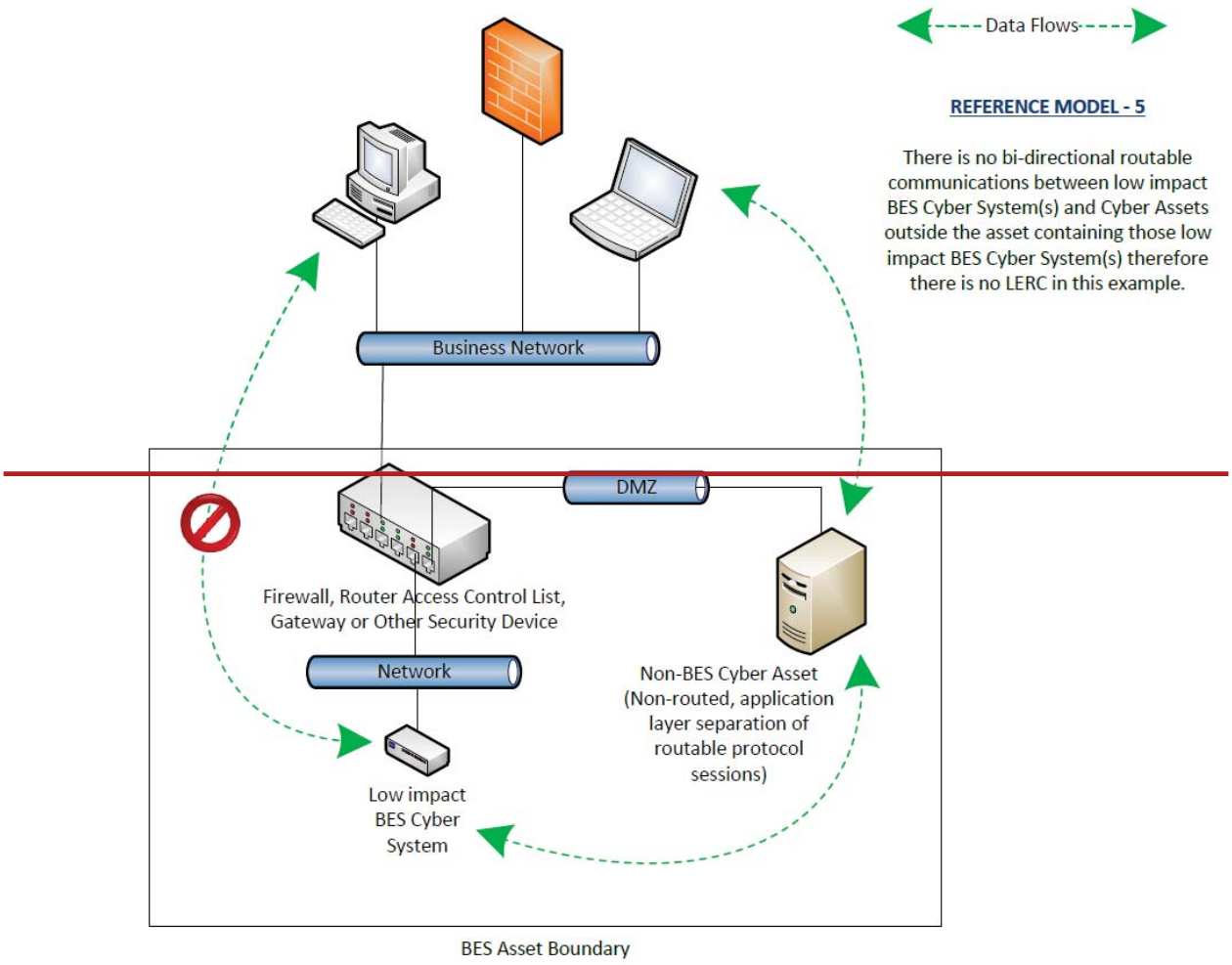

Data Flows
REFERENCE MODEL - 3
The low impact BES Cyber Systems at each site are externally accessible from a Cyber Asset outside the asset containing the low impact BES Cyber Systems so there is LERC. A security device is place at "Location X" to act as the LEAP(s) and permit only necessary electronic access to the low impact BES Cyber Systems.
Business Network
LEAP
Interface
LEAP
Interface
Firewall, Router Access Control List, Gateway or Other Security Device
Location X
LERC
Network
Non BES Cyber Systsem
Low impact BES Cyber System
BES Asset Boundary
LERC
Network
Non BES Cyber System
Low impact BES Cyber System
BES Asset Boundary

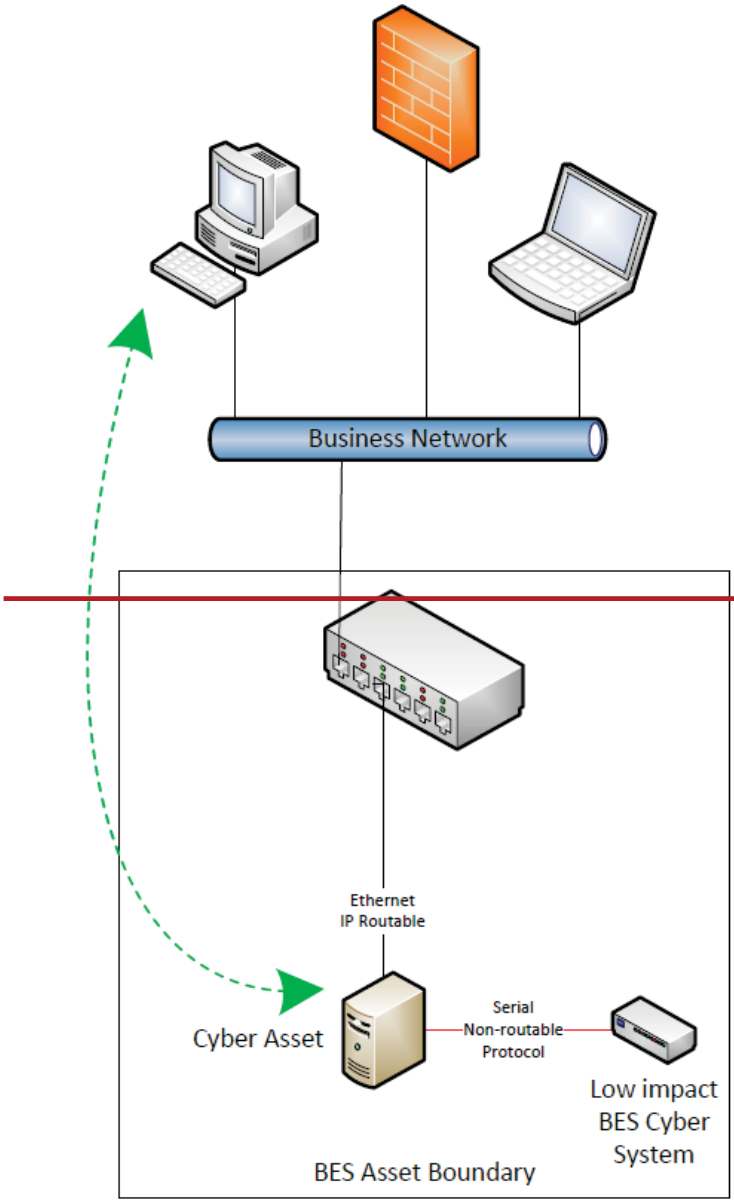


Data Flows

REFERENCE MODEL - 4

The low impact BES Cyber System is externally accessible from a Cyber Asset outside the asset containing the low impact BES Cyber System. There is LERC because the IP/Serial converter is extending the communication between the business network Cyber Asset and the low impact BES Cyber System is directly addressable from outside the asset. A security device is placed between the business network and the low impact BES Cyber System to permit only necessary electronic access to the low impact BES Cyber System.

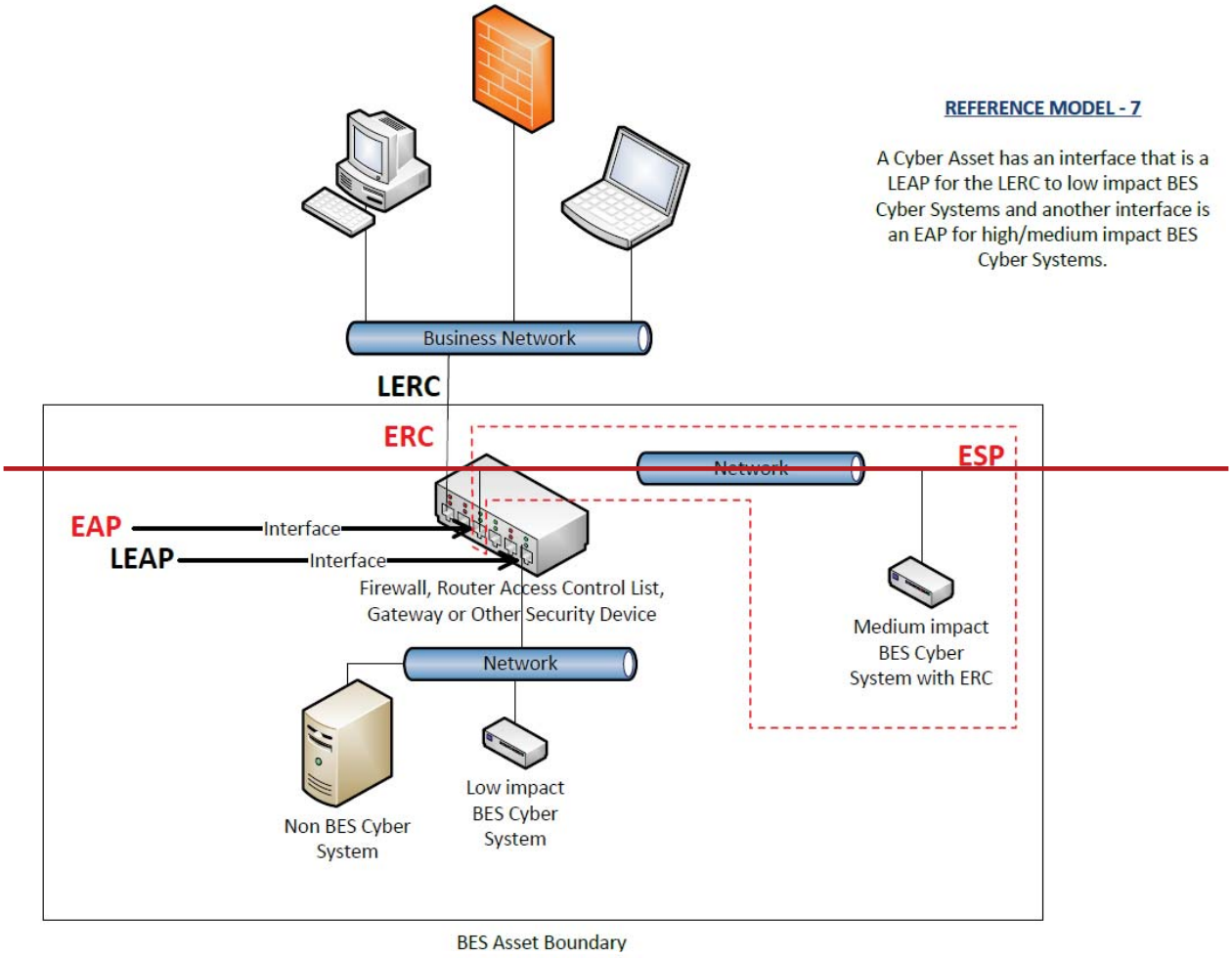

Data Flows
REFERENCE MODEL - 5
There is no bi-directional routable communications between low impact BES Cyber System(s) and Cyber Assets outside the asset containing those low impact BES Cyber System(s) therefore there is no LERC in this example.
Business Network
DMZ
Firewall, Router Access Control List, Gateway or Other Security Device
Network
Non-BES Cyber Asset (Non-routed, application layer separation of routable protocol sessions)
Low impact BES Cyber System
BES Asset Boundary



Data Flows

REFERENCE MODEL - 6

In this example, a Cyber Asset stops the direct access to the low impact BES Cyber System. There is a layer 7 application layer break or the Cyber Asset requires authentication and then establishes a new connection to the low impact BES Cyber System. There is no LERC in this example.



Requirement R2, Attachment 1, Section 4 – Cyber Security Incident Response

The entity should have one or more documented Cyber Security Incident response plan(s) that include each of the topics listed in Section 4. If, in the normal course of business, suspicious activities are noted at an asset containing low impact BES Cyber ~~Systems,~~System(s), the intent is for the entity to implement a Cyber Security Incident response plan that will guide the entity in responding to the incident and reporting the incident if it rises to the level of a Reportable Cyber Security Incident.

Entities are provided the flexibility to develop their Attachment 1, Section 4 Cyber Security Incident response plan(s) by asset or group of assets. The plans do not need to be on a per asset site or per low impact BES Cyber System basis. Entities can choose to use a single enterprise-wide plan to fulfill the obligations for low impact BES Cyber Systems.

The plan(s) must be tested once every 36 months. This is not an exercise per low impact BES Cyber Asset or per type of BES Cyber Asset but rather is an exercise of each incident response plan the entity created to meet this requirement. An actual Reportable Cyber Security Incident

counts as an exercise as do other forms of tabletop exercises or drills. NERC-led exercises such as GridEx participation would also count as an exercise provided the entity's response plan is followed. The intent of the requirement is for entities to keep the Cyber Security Incident response plan(s) current, which includes updating the plan(s), if needed, within 180 days following a test or an actual incident.

For low impact BES Cyber Systems, the only portion of the definition of Cyber Security Incident that would apply is, "A malicious act or suspicious event that disrupts, or was an attempt to disrupt, the operation of a BES Cyber System." The other portion of that definition is not to be used to require ESPs and PSPs for low impact BES Cyber Systems.

Requirement R2, Attachment 1, Section 5 – Transient Cyber Assets and Removable Media Malicious Code Risk Mitigation

Most BES Cyber Assets and BES Cyber Systems are isolated from external public or untrusted networks, and therefore Transient Cyber Assets and Removable Media are needed to transport files to and from secure areas to maintain, monitor, or troubleshoot critical systems. Transient Cyber Assets and Removable Media are a potential means for cyber-attack. To protect the BES Cyber Assets and BES Cyber Systems, CIP-003 Requirement R2, Attachment 1, Section 5 requires Responsible Entities to document and implement a plan for how they will mitigate the risk of malicious code introduction to low impact BES Cyber Systems from Transient Cyber Assets and Removable Media. The approach of defining a plan allows the Responsible Entity to document processes that are supportable within its organization and in alignment with its change management processes.

Transient Cyber Assets can be one of many types of devices from a specially-designed device for maintaining equipment in support of the BES to a platform such as a laptop, desktop, or tablet that may interface with or run applications that support BES Cyber Systems and is capable of transmitting executable code to the BES Cyber Asset(s) or BES Cyber System(s). Note: Cyber Assets connected to a BES Cyber System for less than 30 days due to an unplanned removal, such as premature failure, are not intended to be identified as Transient Cyber Assets. Removable Media subject to this requirement include, among others, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.

Examples of these temporarily connected devices include, but are not limited to:

- Diagnostic test equipment;
- Equipment used for BES Cyber System maintenance; or
- Equipment used for BES Cyber System configuration.

To meet the objective of mitigating risks associated with the introduction of malicious code at low impact BES Cyber Systems, Section 5 specifies the capabilities and possible security methods available to Responsible Entities based upon asset type and ownership.

With the list of options provided in Attachment 1, the entity has the discretion to use the option(s) that is most appropriate. This includes documenting its approach for how and when the entity reviews the Transient Cyber Asset under its control or under the control of parties

other than the Responsible Entity. The entity should avoid implementing a security function that jeopardizes reliability by taking actions that would negatively impact the performance or support of the Transient Cyber Asset or BES Cyber Asset.

Malicious Code Risk Mitigation

The terms "mitigate", "mitigating", and "mitigation" are used in Section 5 in Attachment 1 to address the risks posed by malicious code when connecting Transient Cyber Assets and Removable Media to BES Cyber Systems. Mitigation is intended to mean that entities reduce security risks presented by connecting the Transient Cyber Asset or Removable Media. When determining the method(s) to mitigate the introduction of malicious code, it is not intended for entities to perform and document a formal risk assessment associated with the introduction of malicious code.

Per Transient Cyber Asset Capability

As with other CIP standards, the requirements are intended for an entity to use the method(s) that the system is capable of performing. The use of "per Transient Cyber Asset capability" is to eliminate the need for a Technical Feasibility Exception when it is understood that the device cannot use a method(s). For example, for malicious code, many types of appliances are not capable of implementing antivirus software; therefore, because it is not a capability of those types of devices, implementation of the antivirus software would not be required for those devices.

Requirement R2, Attachment 1, Section 5.1 - Transient Cyber Asset(s) Managed by the Responsible Entity

For Transient Cyber Assets and Removable Media that are connected to both low impact and medium/high impact BES Cyber Systems, entities must be aware of the differing levels of requirements and manage these assets under the program that matches the highest impact level to which they will connect.

Section 5.1: Entities are to document and implement their plan(s) to mitigate malicious code through the use of one or more of the protective measures listed, based on the capability of the Transient Cyber Asset.

The Responsible Entity has the flexibility to apply the selected method(s) to meet the objective of mitigating the introductions of malicious code either in an on-going or in an on-demand manner. An example of managing a device in an on-going manner is having the antivirus solution for the device managed as part of an end-point security solution with current signature or pattern updates, regularly scheduled systems scans, etc. In contrast, for devices that are used infrequently and the signatures or patterns are not kept current, the entity may manage those devices in an on-demand manner by requiring an update to the signatures or patterns and a scan of the device before the device is connected to ensure that it is free of malicious code.

Selecting management in an on-going or on-demand manner is not intended to imply that the control has to be verified at every single connection. For example, if the device is managed in an on-demand manner, but will be used to perform maintenance on several BES Cyber Asset(s), the Responsible Entity may choose to document that the Transient Cyber Asset has been updated before being connected as a Transient Cyber Asset for the first use of that maintenance work. The intent is not to require a log documenting each connection of a Transient Cyber Asset to a BES Cyber Asset.

The following is additional discussion of the methods to mitigate the introduction of malicious code.

- Antivirus software, including manual or managed updates of signatures or patterns, provides flexibility to manage Transient Cyber Asset(s) by deploying antivirus or endpoint security tools that maintain a scheduled update of the signatures or patterns. Also, for devices that do not regularly connect to receive scheduled updates, entities may choose to update the signatures or patterns and scan the Transient Cyber Asset prior to connection to ensure no malicious software is present.
- Application whitelisting is a method of authorizing only the applications and processes that are necessary on the Transient Cyber Asset. This reduces the risk that malicious software could execute on the Transient Cyber Asset and impact the BES Cyber Asset or BES Cyber System.
- When using methods other than those listed, entities need to document how the other method(s) meet the objective of mitigating the risk of the introduction of malicious code.

If malicious code is discovered on the Transient Cyber Asset, it must be mitigated prior to connection to a BES Cyber System to prevent the malicious code from being introduced into the BES Cyber System. An entity may choose to not connect the Transient Cyber Asset to a BES Cyber System to prevent the malicious code from being introduced into the BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber Security Incident.

Requirement R2, Attachment 1, Section 5.2 - Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity

Section 5 also recognizes the lack of direct control over Transient Cyber Assets that are managed by parties other than the Responsible Entity. This lack of control, however, does not obviate the Responsible Entity's responsibility to ensure that methods have been deployed to mitigate the introduction of malicious code to low impact BES Cyber System(s) from Transient Cyber Assets it does not manage. Section 5 requires entities to review the other party's security practices with respect to Transient Cyber Assets to help meet the objective of the requirement. The use of "prior to connecting the Transient Cyber Assets" is intended to ensure that the Responsible Entity conducts the review before the first connection of the Transient Cyber Asset to help meet the objective to mitigate the introduction of malicious code. The SDT does not intend for the Responsible Entity to conduct a review for every single connection of that Transient Cyber Asset once the Responsible Entity has established the Transient Cyber Asset is meeting the security objective. The intent is to not require a log documenting each connection of a Transient Cyber Asset to a BES Cyber Asset.

To facilitate these controls, Responsible Entities may execute agreements with other parties to provide support services to BES Cyber Systems and BES Cyber Assets that may involve the use of Transient Cyber Assets. Entities may consider using the Department of Energy Cybersecurity Procurement Language for Energy Delivery dated April 2014.[1] Procurement language may unify

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

the other party and entity actions supporting the BES Cyber Systems and BES Cyber Assets. CIP program attributes may be considered including roles and responsibilities, access controls, monitoring, logging, vulnerability, and patch management along with incident response and back up recovery may be part of the other party's support. Entities may consider the "General Cybersecurity Procurement Language" and "The Supplier's Life Cycle Security Program" when drafting Master Service Agreements, Contracts, and the CIP program processes and controls.

Section 5.2: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more of the protective measures listed.

- Review the use of antivirus software and signature or pattern levels to ensure that the level is adequate to the Responsible Entity to mitigate the risk of malicious software being introduced to an applicable system.
- Review the antivirus or endpoint security processes of the other party to ensure that their processes are adequate to the Responsible Entity to mitigate the risk of introducing malicious software to an applicable system.
- Review the use of application whitelisting used by the other party to mitigate the risk of introducing malicious software to an applicable system.
- Review the use of live operating systems or software executable only from read-only media to ensure that the media is free from malicious software itself. Entities should review the processes to build the read-only media as well as the media itself.
- Review system hardening practices used by the other party to ensure that unnecessary ports, services, applications, etc. have been disabled or removed. This method intends to reduce the attack surface on the Transient Cyber Asset and reduce the avenues by which malicious software could be introduced.

Requirement R2, Attachment 1, Section 5.3 - Removable Media

Entities have a high level of control for Removable Media that are going to be connected to their BES Cyber Assets.

Section 5.3: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more method(s) to detect malicious code on the Removable Media before it is connected to a BES Cyber Asset. When using the method(s) to detect malicious code, it is expected to occur from a system that is not part of the BES Cyber System to reduce the risk of propagating malicious code into the BES Cyber System network or onto one of the BES Cyber Assets. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber Security Incident. Frequency and timing of the methods used to detect malicious code were intentionally excluded from the requirement because there are multiple timing scenarios that

can be incorporated into a plan to mitigate the risk of malicious code. The SDT does not intend to obligate a Responsible Entity to conduct a review for every single connection of Removable Media, but rather to implement its plan(s) in a manner that protects all BES Cyber Systems where Removable Media may be used. The intent is to not require a log documenting each connection of Removable Media to a BES Cyber Asset.

As a method to detect malicious code, entities may choose to use Removable Media with on-board malicious code detection tools. For these tools, the Removable Media are still used in conjunction with a Cyber Asset to perform the detection. For Section 5.3.1, the Cyber Asset used to perform the malicious code detection must be outside of the BES Cyber System.

Requirement R3:

The intent of CIP-003-~~6~~7, Requirement R3 is effectively unchanged since prior versions of the standard. The specific description of the CIP Senior Manager has now been included as a defined term rather than clarified in the Reliability Standard itself to prevent any unnecessary cross-reference to this standard. It is expected that the CIP Senior Manager will play a key role in ensuring proper strategic planning, executive/board-level awareness, and overall program governance.

Requirement R4:

As indicated in the rationale for CIP-003-~~6~~7, Requirement R4, this requirement is intended to demonstrate a clear line of authority and ownership for security matters. The intent of the SDT was not to impose any particular organizational structure, but, rather, the intent is to afford the Responsible Entity significant flexibility to adapt this requirement to its existing organizational structure. A Responsible Entity may satisfy this requirement through a single delegation document or through multiple delegation documents. The Responsible Entity can make use of the delegation of the delegation authority itself to increase the flexibility in how this applies to its organization. In such a case, delegations may exist in numerous documentation records as long as the collection of these documentation records shows a clear line of authority back to the CIP Senior Manager. In addition, the CIP Senior Manager could also choose not to delegate any authority and meet this requirement without such delegation documentation.

The Responsible Entity must keep its documentation of the CIP Senior Manager and any delegations up-to-date. This is to ensure that individuals do not assume any undocumented authority. However, delegations do not have to be re-instated if the individual who delegated the task changes roles or the individual is replaced. For instance, assume that John Doe is named the CIP Senior Manager and he delegates a specific task to the Substation Maintenance Manager. If John Doe is replaced as the CIP Senior Manager, the CIP Senior Manager documentation must be updated within the specified timeframe, but the existing delegation to the Substation Maintenance Manager remains in effect as approved by the previous CIP Senior Manager, John Doe.

Rationale:
During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for Requirement R1:
One or more security policies enable effective implementation of the requirements of the cyber security Reliability Standards. The purpose of policies is to provide a management and governance foundation for all requirements that apply to a Responsible Entity's BES Cyber Systems. The Responsible Entity can demonstrate through its policies that its management supports the accountability and responsibility necessary for effective implementation of the requirements.

Annual review and approval of the cyber security policies ensures that the policies are kept-up-to-date and periodically reaffirms management's commitment to the protection of its BES Cyber Systems.

Rationale for Requirement R2:
In response to FERC Order No. 791, Requirement R2 requires entities to develop and implement cyber security plans to meet specific security control objectives for assets containing low impact BES Cyber ~~Systems.~~System(s). The cyber security plan(s) covers ~~four~~five subject matter areas: (1) cyber security awareness; (2) physical security controls; (3) electronic access controls; ~~and~~ (4) Cyber Security Incident response; and (5) Transient Cyber Asset and Removable Media Malicious Code Risk Mitigation. This plan(s), along with the cyber security policies required under Requirement R1, Part 1.2, provides a framework for operational, procedural, and technical safeguards for low impact BES Cyber Systems.

Considering the varied types of low impact BES Cyber Systems across the BES, Attachment 1 provides Responsible Entities flexibility on how to apply the security controls to meet the security objectives. Additionally, because many Responsible Entities have multiple-impact rated BES Cyber Systems, nothing in the requirement prohibits entities from using their high and medium impact BES Cyber System policies, procedures, and processes to implement security controls required for low impact BES Cyber Systems, as detailed in Requirement R2, Attachment 1.

Responsible Entities will use their identified assets containing low impact BES Cyber System(s) (developed pursuant to CIP-002) to substantiate the sites or locations associated with low impact BES Cyber ~~Systems.~~System(s). However, there is no requirement or compliance expectation for Responsible Entities to maintain a list(s) of individual low impact BES Cyber ~~Systems~~System(s) and their associated cyber assets or to maintain a list of authorized users.

Rationale for Modifications to Sections 2 and 3 of Attachment 1 (Requirement R2):
Requirement R2 mandates that entities develop and implement one or more cyber security plan(s) to meet specific security objectives for assets containing low impact BES Cyber System(s). In Paragraph 73 of FERC Order No. 822, the Commission directed NERC to modify "…the Low Impact External Routable Connectivity definition to reflect the commentary in the Guidelines and Technical Basis section of CIP-003-6…to provide needed clarity to the definition

and eliminate ambiguity surrounding the term 'direct' as it is used in the proposed definition…within one year of the effective date of this Final Rule."

The revisions to Section 3 incorporate select language from the LERC definition into Attachment 1 and focus the requirement on implementing electronic access controls for asset(s) containing low impact BES Cyber System(s). This change requires the Responsible Entity to permit only necessary inbound and outbound electronic access when using a routable protocol entering or leaving the asset between low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber system(s). When this communication is present, Responsible Entities are required to implement electronic access controls unless that communication meets the following exclusion language (previously in the definition of LERC) contained in romanette (iii): "not used for time-sensitive protection or control functions between intelligent electronic devices (e.g. communications using protocol IEC TR-61850-90-5 R-GOOSE)".

The revisions to Section 2 of Attachment 1 complement the revisions to Section 3; consequently, the requirement now mandates the Responsible Entity control physical access to "the Cyber Asset(s), as specified by the Responsible Entity, that provide electronic access control(s) implemented for Section 3.1, if any." The focus on electronic access controls rather than on the Low Impact BES Cyber System Electronic Access Points (LEAPs) eliminates the need for LEAPs.

Given these revisions to Sections 2 and 3, the NERC Glossary terms: Low Impact External Routable Connectivity (LERC) and Low Impact BES Cyber System Electronic Access Point (LEAP) will be retired.

Rationale for Section 5 of Attachment 1 (Requirement R2):
Requirement R2 mandates that entities develop and implement one or more cyber security plan(s) to meet specific security objectives for assets containing low impact BES Cyber System(s). In Paragraph 32 of FERC Order No. 822, the Commission directed NERC to "…provide mandatory protection for transient devices used at Low Impact BES Cyber Systems based on the risk posed to bulk electric system reliability." Transient devices are potential vehicles for introducing malicious code into low impact BES Cyber Systems. Section 5 of Attachment 1 is intended to mitigate the risk of malware propagation to the BES through low impact BES Cyber Systems by requiring entities to develop and implement one or more plan(s) to address the risk. The cyber security plan(s) along with the cyber security policies required under Requirement R1, Part 1.2, provide a framework for operational, procedural, and technical safeguards for low impact BES Cyber Systems.

Rationale for Requirement R3:
The identification and documentation of the single CIP Senior Manager ensures that there is clear authority and ownership for the CIP program within an organization, as called for in Blackout Report Recommendation 43. The language that identifies CIP Senior Manager responsibilities is included in the Glossary of Terms used in NERC Reliability Standards so that it may be used across the body of CIP standards without an explicit cross-reference.

FERC Order No. 706, Paragraph 296, requests consideration of whether the single senior manager should be a corporate officer or equivalent. As implicated through the defined term, the senior manager has "the overall authority and responsibility for leading and managing implementation of the requirements within this set of standards" which ensures that the senior manager is of sufficient position in the Responsible Entity to ensure that cyber security receives the prominence that is necessary. In addition, given the range of business models for responsible entities, from municipal, cooperative, federal agencies, investor owned utilities, privately owned utilities, and everything in between, the SDT believes that requiring the CIP Senior Manager to be a "corporate officer or equivalent" would be extremely difficult to interpret and enforce on a consistent basis.

Rationale for Requirement R4:

The intent of the requirement is to ensure clear accountability within an organization for certain security matters. It also ensures that delegations are kept up-to-date and that individuals do not assume undocumented authority.

In FERC Order No. 706, Paragraphs 379 and 381, the Commission notes that Recommendation 43 of the 2003 Blackout Report calls for "clear lines of authority and ownership for security matters." With this in mind, the Standard Drafting Team has sought to provide clarity in the requirement for delegations so that this line of authority is clear and apparent from the documented delegations.