« *Technical Rationale and Justification for Reliability Standard* » (Justification technique) et « *Implementation Guidance* » (Guide d'application) (version française)

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

VERSION PRÉLIMINAIRE

Cybersécurité – Périmètres de sécurité électronique

Justification technique de la norme de fiabilité CIP-005-7

Octobre 2020

FIABILITÉ | RÉSILIENCE | SÉCURITÉ

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table des matières

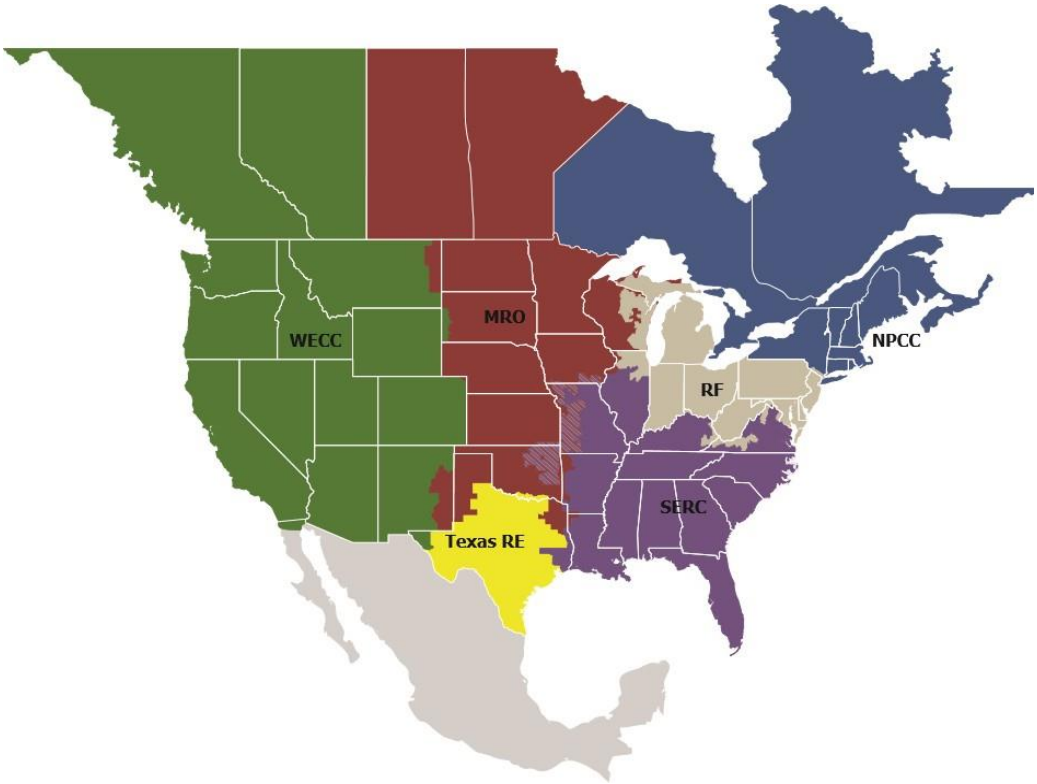
Préface iii
Introduction iv
Termes nouveaux ou modifiés utilisés dans les normes de fiabilité de la NERC 6
Exigence E1 7
Remarques générales sur l'exigence E1 7
Exigence 1 8
Exigence E2 10
Remarques générales sur l'exigence E2 10
Exigence E3 12
Alinéas 3.1 et 3.2 – Gestion des accès distants des fournisseurs pour les *EACMS* et les *PACS* 12
Justification technique de la norme de fiabilité CIP-005-6 0
Section 4 – Portée de l'applicabilité des normes CIP sur la cybersécurié 0
Exigence E1 0
Exigence E2 2
Justification 2
Justifications pour E1 2
Justifications pour E2 3

Préface

L'électricité est un élément essentiel du tissu de nos sociétés modernes, et l'organisme de fiabilité électrique (ERO) a pour mission de renforcer ce tissu. L'ERO, qui regroupe la North American Electric Reliability Corporation (NERC) et les six entités régionales, veille à maximiser la fiabilité et la sécurité du *système électrique interconnecté* (*BPS*) de l'Amérique du Nord. Nous travaillons en permanence à réduire de manière efficace et efficiente les risques pour la fiabilité et la sécurité du réseau électrique.

Fiabilité | Résilience | Sécurité
Parce que près de 400 millions de citoyens en Amérique du Nord comptent sur nous

Le *système électrique interconnecté* de l'Amérique du Nord est divisé en six territoires d'entités régionales, comme le montrent la carte et le tableau ci-dessous. Les zones combinant deux couleurs indiquent des chevauchements, car certains *responsables de l'approvisionnement* sont actifs dans une région alors que les *propriétaires d'installation de transport* et les *exploitants de réseau de transport* associés sont actifs dans une autre région.



MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst Corporation
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

Introduction

Ce document expose la justification technique de la norme de fiabilité CIP-005-7 proposée. Il vise à guider les parties prenantes ainsi que l'ERO dans la compréhension des enjeux technologiques et des exigences techniques de cette norme de fiabilité. Le présent document, *Justification technique de la norme de fiabilité CIP-005-7*, n'est pas une norme de fiabilité et son contenu ne doit donc pas être considéré comme obligatoire et exécutoire.

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

La section 4.1 (Entités fonctionnelles) présente la liste des entités fonctionnelles de la NERC auxquelles s'applique la norme. Si une 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. Il est à noter que la section 4.1 limite l'applicabilité de la norme, dans le cas des *distributeurs*, à ceux qui détiennent certains types de systèmes et d'équipements énumérés à la section 4.2.

En outre, la section 4.2 (*Installations*) définit la portée des *installations*, systèmes et équipements détenus par les entités responsables désignées à la section 4.1 comme étant visées par la norme. Comme il est indiqué à la section d'exemption 4.2.3.5, la norme ne s'applique pas aux entités responsables qui n'ont pas de *systèmes électroniques BES* à impact élevé ou moyen selon la catégorisation de la norme CIP-002. 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 la définition du terme « *installations* » dans le glossaire de la NERC indique déjà l'appartenance au *BES*, l'utilisation additionnelle du terme « *BES* » vise ici à renforcer la portée d'applicabilité pour ces *installations*, en particulier dans cette section sur l'applicabilité de la norme. Cela établit quels sont les systèmes, *installations* et équipements visés par les normes.

Les mises à jour du présent document reflètent maintenant les intentions de l'équipe de rédaction de la norme *Cybersécurité – Gestion des risques dans la chaîne d'approvisionnement* (projet 2019-03) quant aux changements à apporter aux exigences.

Le 18 octobre 2018, la Federal Energy Regulatory Commission (FERC) publiait l'Ordonnance 850, dans laquelle elle demandait de modifier les différentes normes sur la chaîne d'approvisionnement afin d'étendre leur portée aux *systèmes de contrôle ou de surveillance des accès électroniques* (*EACMS*), plus spécifiquement ceux qui assurent le contrôle ou la surveillance des accès électroniques à des *systèmes électroniques BES* à impact élevé ou moyen. Par ailleurs, dans son rapport du 17 mai 2019 sur les risques de cybersécurité dans la chaîne d'approvisionnement, la NERC recommandait de modifier les normes sur la chaîne d'approvisionnement afin d'étendre leur portée aux *systèmes de contrôle des accès physiques* (*PACS*) qui assurent le contrôle des accès physiques à des *systèmes électroniques BES* à impact élevé ou moyen.

L'équipe de rédaction du projet 2019-03 a donc formulé la norme de fiabilité CIP-005-7 de manière à exiger des entités responsables qu'elles respectent les prescriptions de l'Ordonnance 850 de la FERC et du rapport de la NERC sur les risques de cybersécurité dans la chaîne d'approvisionnement.

En outre, l'équipe de rédaction du projet 2019-03 a supprimé la mention « *coordonnateur des échanges ou responsable des échanges* », cette fonction ayant été retirée du Registre des entités visées.

Termes nouveaux ou modifiés utilisés dans les normes de fiabilité de la NERC

La norme CIP-005-7 utilise la ou les définitions suivantes, qui sont reproduites ci-après pour référence au cours de la lecture de la justification technique qui suit.

Termes modifiés proposés : aucun.

Nouveaux termes proposés : aucun.

Exigence E1

Remarques générales sur l'exigence E1

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

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

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

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

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

Justification des modifications : (alinéa 1.1)
Affirmation claire du fait que les *actifs électroniques BES* reliés au moyen d'un protocole routable doivent se situer à l'intérieur d'un *périmètre de sécurité électronique*.

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

Justification des modifications : (alinéa 1.2)
Utilisation des termes définis *point d'accès électronique* et *système électronique BES*.

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

Justification des modifications : (alinéa 1.3)
Utilisation du terme défini *point d'accès électronique* (*EAP*) et insistance sur le fait que l'entité doit connaître les accès entrants et sortants via l'*EAP* qu'elle autorise et que les raisons pour lesquelles elle autorise ces accès sont justifiées.

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

Justification des modifications apportées : (alinéa 1.4)
Explication plus claire du fait que la connectivité par lien commuté doit assurer l'authentification afin de rendre impossible l'accès direct au *système électronique BES* à l'aide d'un simple numéro de téléphone.

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

Justification des modifications : (alinéa 1.5)

Conformité avec l'Ordonnance 706 de la FERC, alinéas 496-503, en vertu de laquelle il faut prévoir deux dispositifs de sécurité distincts pour les *ESP* afin de préserver le périmètre de protection des *actifs électroniques* advenant une défaillance ou un défaut de configuration de l'un ou l'autre de ces dispositifs. L'Ordonnance indique clairement qu'il ne s'agit pas simplement d'assurer une redondance des pare-feu ; l'équipe de rédaction a donc décidé d'ajouter l'exigence liée à la mise en œuvre de moyens de détection des communications malveillantes pour les *ESP*.

Exigence 1

L'exigence E1 de la norme CIP-005-5 exige l'isolation des *systèmes électroniques BES* des autres systèmes de degrés de confiance différents en exigeant des *points d'accès électroniques* contrôlés entre les différentes zones de confiance. Les *périmètres de sécurité électronique* sont également utilisés comme première couche de défense pour certains *systèmes électroniques BES* qui ne disposent pas intrinsèquement d'une protection électronique suffisante, notamment les dispositifs qui n'ont pas de fonction d'authentification.

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

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

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

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

Lorsqu'un *actif électronique* est accessible par connectivité routable à travers l'*ESP*, les données qui entrent dans l'*ESP* ou en sortent doivent être contrôlées par un *point d'accès électronique* (*EAP*).

L'*EAP* doit contrôler les échanges tant entrants que sortants. La norme exige dorénavant le contrôle des échanges sortants puisque celui-ci constitue un premier indicateur de compromission et un mécanisme de défense de premier niveau contre les attaques de vulnérabilité du jour zéro. Si des *actifs électroniques* à l'intérieur de l'*ESP* sont compromis et tentent de communiquer avec des hôtes inconnus à l'extérieur de l'*ESP* (il s'agit habituellement d'hôtes de « commande et contrôle », sur Internet, ou d'hôtes de rebond compromis au sein d'autres réseaux de l'entité responsable et qui agissent comme intermédiaires), l'*EAP* doit agir comme mécanisme de défense de premier niveau pour rompre la communication. L'intention de l'équipe de rédaction est de faire en sorte que l'entité responsable connaisse les autres *actifs électroniques* ou plages d'adresses avec lesquels le *système électronique BES* a besoin de communiquer et qu'elle limite les communications à ces actifs et adresses connus. L'objectif de l'équipe de rédaction n'est pas de faire en sorte que l'entité responsable documente les activités internes des pare-feu dynamiques, où les connexions amorcées dans un sens sont autorisées dans l'autre sens. L'objectif est plutôt que l'entité responsable connaisse et documente les systèmes ou groupes de systèmes qui peuvent communiquer entre eux de part et d'autre de l'*EAP* afin que les connexions indésirables puissent être détectées et bloquées.

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

Dans le cas de la connectivité par lien commuté, l'intention de l'équipe de rédaction est de prévenir les situations où il serait possible d'établir une liaison directe avec un *actif électronique BES* au moyen d'un numéro de téléphone uniquement. Si un modem est configuré de manière à simplement répondre au téléphone et à établir la liaison avec l'*actif électronique BES* demandé sans authentifier le demandeur, il rend vulnérable le *système électronique BES*. En vertu de cette exigence, le modem doit authentifier le demandeur avant d'établir la communication avec le *système électronique BES*. L'exigence E2 s'applique également dans le cas d'une connectivité par lien commuté utilisée pour un *accès distant interactif*.

La norme ajoute une exigence pour les *centres de contrôle* concernant la détection des communications malveillantes. Il s'agit d'une réponse à l'Ordonnance 706 de la FERC, alinéas 496-503, stipulant qu'il faut prévoir deux dispositifs de sécurité distincts pour les *ESP* afin de préserver le périmètre de protection des *systèmes électroniques BES* advenant une défaillance ou un défaut de configuration de l'un ou l'autre de ces dispositifs. L'ordonnance indique clairement qu'il ne s'agit pas simplement d'assurer une redondance des pare-feu ; l'équipe de rédaction a donc décidé d'ajouter l'exigence liée à la mise en œuvre de moyens de détection des communications malveillantes pour les *ESP*.

Exigence E2

Remarques générales sur l'exigence E2

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

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

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

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

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

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

Référence à une version précédente : (alinéa 2.1) Nouveau

Justification des modifications apportées : (alinéa 2.1)

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

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

Justification des modifications apportées : (alinéa 2.2)
Nouvelle exigence visant à poursuivre les efforts de l'équipe d'intervention rapide affectée au projet 2010-15 (révision accélérée de la norme CIP-005-3). Cette exigence vise à protéger la confidentialité et l'intégrité de chaque session d'*accès distant interactif*.

Justification des modifications apportées : (alinéa 2.3)
Nouvelle exigence visant à poursuivre les efforts de l'équipe d'intervention rapide affectée au projet 2010-15 (révision accélérée de la norme CIP-005-3). Les méthodes d'authentification multifactorielle sont décrites dans le document *Homeland Security Presidential Directive 12* (HSPD-12) du 12 août 2007.

Exigence E3

Alinéas 3.1 et 3.2 – Gestion des accès distants des fournisseurs pour les *EACMS* et les *PACS*

L'équipe de rédaction du projet 2019-03 a créé une nouvelle exigence E3 afin de réunir les dispositions relatives à la gestion de tous les types d'accès distant des fournisseurs (accès de système à système ou d'utilisateur à système) pour les *EACMS* et les *PACS*. Les *EACMS* ont été incorporés à cette exigence en réponse au paragraphe 5 de l'Ordonnance 850 de la FERC, dans lequel celle-ci ordonne à la NERC de mettre sur pied une équipe de rédaction pour étendre la portée de la norme à ces dispositifs. L'ajout des *EACMS* est justifié par les risques signalés par la FERC au paragraphe 4 de l'ordonnance précitée ; il y est indiqué qu'une équipe d'intervention d'urgence en cybersécurité des systèmes de commande industrielle (ICS-CERT) du département de la Sécurité intérieure des États-Unis (DHS) a déclaré que les pare-feu (normalement définis comme des *EACMS*) constituent « la première ligne de défense dans l'environnement réseau d'un système de commande industrielle ». La compromission de ces dispositifs, qui commandent la gestion des accès, pourrait fournir à un intrus « la clé de la porte principale » d'un *ESP* dans lequel résident des *systèmes électroniques BES*. Avec cette clé, un intrus aurait tout loisir de s'introduire dans l'*ESP* ou de modifier les contrôles d'accès afin de permettre à des tiers de contourner le système d'autorisation.

Aux alinéas 3.1 et 3.2 de l'exigence E3, le mot « connexion » désigne le mécanisme par lequel un utilisateur ou un système interagit avec un *EACMS* ou un *PACS* aux fins d'authentification.

Aux alinéas 3.1 et 3.2 de l'exigence E3, le mot « authentifié » renvoie au mécanisme par lequel l'*EACMS* ou le *PACS* identifie l'utilisateur ou le dispositif. Il s'agit de permettre à l'*EACMS* ou au *PACS* de remplir d'abord sa fonction de validation de l'utilisateur ou du dispositif qui demande une connexion ; l'entité peut ensuite distinguer, parmi les connexions par accès distant, celles qui sont commandées par des fournisseurs. Ces nouveaux alinéas n'ont pas un caractère prescriptif quant à la manière dont doit se dérouler l'authentification, de même que pour les méthodes administratives et techniques utilisées.

À l'alinéa 3.2 de l'exigence E3, le mot « contrôler » offre à l'entité la latitude voulue pour permettre au fournisseur de se reconnecter en présence d'un ensemble particulier de critères établis par l'entité, dans la mesure où la reconnexion est nécessaire au maintien des opérations critiques de l'entité. Si l'entité détermine qu'elle ne veut pas permettre ou n'a pas besoin de permettre une reconnexion, elle peut utiliser le moyen de son choix pour bloquer toute reconnexion.

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

Étant donné que si un *PACS* est compromis à distance, une présence physique est tout de même nécessaire pour exploiter la vulnérabilité de *systèmes électroniques BES*, l'équipe de rédaction s'est livrée à un sérieux travail de consultation et de réflexion relativement à l'inclusion des *PACS* dans la portée des exigences. L'équipe a conclu que le risque pour la fiabilité du *BES* que représente un *PACS* compromis, mal utilisé, endommagé ou indisponible justifie l'inclusion des *PACS* parmi les catégories d'*actifs électroniques* visées. En outre, l'inclusion des *PACS* :

1. répond à la préoccupation énoncée par la FERC au paragraphe 6 de l'Ordonnance 850, où elle rappelle que « l'exclusion de ces éléments peut constituer une lacune dans les normes de fiabilité sur la gestion des risques dans la chaîne d'approvisionnement » ;

2. répond au souhait formulé au paragraphe 24 de l'Ordonnance 850, où la FERC propose de « demander que la NERC évalue les risques de cybersécurité dans la chaîne d'approvisionnement associés aux *PACS* et aux *PCA* dans le cadre de l'étude des risques de cybersécurité dans la chaîne d'approvisionnement demandée par le Conseil d'administration de la NERC dans ses résolutions du 10 août 2017 » ; et

3. répond directement à la recommandation d'inclusion des *PACS* formulée par la NERC dans son rapport final sur les risques de cybersécurité dans la chaîne d'approvisionnement[1].

À la page 4 du rapport final de la NERC sur les risques de cybersécurité dans la chaîne d'approvisionnement, on peut lire : « Les normes de fiabilité CIP de la NERC établissent une démarche de défense en profondeur axée sur les risques, visant à sécuriser le *BES* contre les menaces de cybersécurité et de sécurité physique. » Les *PACS* ont pour fonction de gérer les menaces physiques à l'endroit des *systèmes électroniques BES*, afin de protéger ceux-ci contre les compromissions qui pourraient entraîner un fonctionnement incorrect ou des instabilités dans le *BES*.

On peut également lire à la page 15 du rapport final de la NERC sur les risques de cybersécurité dans la chaîne d'approvisionnement : « En outre, un auteur de menace doit être physiquement présent sur les lieux de l'installation afin d'exploiter la vulnérabilité qui réside dans un *PACS* compromis. Un auteur de menace pourrait aussi devoir contourner plusieurs autres mesures de contrôle ou de surveillance des accès physiques qui n'auraient pas été compromises afin d'obtenir l'accès souhaité. » Bien que la compromission d'un *PACS* puisse ne pas elle-même permettre de produire un effet nuisible immédiat (délai de 15 minutes) pour la fiabilité du *BES*, elle pourrait signaler l'intention d'un auteur de menace d'obtenir un accès électronique non autorisé.

Bien que d'autres normes de fiabilité visent à atténuer certains risques pour la sécurité relatifs aux *PACS*, aucune ne concerne les risques dans la chaîne d'approvisionnement. C'est pourquoi l'équipe de rédaction a ajouté les *PACS* à la section *Systèmes visés* des alinéas 3.1 et 3.2 de l'exigence.

L'équipe de rédaction a pris en compte un aspect supplémentaire du rapport de la NERC sur les risques de cybersécurité dans la chaîne d'approvisionnement : le risque associé aux fonctions de contrôle d'accès – distinctes des fonctions de surveillance des accès – tant pour les *EACMS* que pour les *PACS*. Ces deux types de systèmes, selon leur définition actuelle, sont chargés de diverses activités fonctionnelles ; le rapport de la NERC, de son côté, souligne

1. NERC, *Cyber Security Supply Chain Risks, Staff Report and Recommended Actions*, 17 mai 2019. https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf

le risque accru associé aux fonctions de contrôle des accès plutôt qu'aux fonctions de surveillance des accès. L'équipe de rédaction a envisagé de limiter la portée des exigences aux seules fonctions de contrôle, mais a finalement décidé de s'en tenir aux définitions approuvées des termes *EACMS* et *PACS*, considérant que cela entraînerait moins de confusion. Du reste, le fait de vouloir modifier les définitions des termes *EACMS* et *PACS* outrepasserait les limites de la demande SAR 2019-03.

Les entités ont le choix d'autoriser ou d'interdire les accès distants à l'un ou l'autre de leurs systèmes (*systèmes électroniques BES*, *EACMS* ou *PACS*) ; si toutefois les accès distants sont autorisés, il est nécessaire d'avoir des moyens pour identifier les connexions à distance et aussi pour les désactiver.

Justification technique de la norme de fiabilité CIP-005-6

Cette section reproduit l'essentiel du texte de la section *Principes directeurs et fondements techniques* de la norme CIP-005-6, à titre de référence historique. Par ailleurs, le contenu de cette même section qui donne des indications sur la conformité est repris dans un Guide d'application distinct pour la présente norme.

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

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

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

La section 4.2. *Installations* définit la portée des *installations,* systèmes et équipements détenus par l'entité responsable désignée à la section 4.1, qui est visée par les exigences de la norme. Comme il est indiqué à la section d'exemption 4.2.3.5, la présente norme ne s'applique pas aux entités responsables qui n'ont pas de *systèmes électroniques BES* à impact élevé ou moyen selon la catégorisation de la norme CIP-002-5. Outre l'ensemble des *installations* du *BES*, des *centres de contrôle* et des autres systèmes et équipements, la liste comprend l'ensemble des systèmes et équipements détenus par les *distributeurs*. Bien que le terme « *installations* » dans le glossaire de la NERC indique déjà l'appartenance au *BES*, l'utilisation additionnelle du terme « *BES* » vise ici à renforcer la portée d'applicabilité pour ces *installations*, en particulier dans cette section sur l'applicabilité. Cela établit quels sont les *installations*, systèmes et équipements visés par les normes.

Exigence E1

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

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

- l'étendue des « *actifs électroniques protégés* (*PCA*) associés » qui doivent également répondre à certaines exigences CIP, et

- la frontière à l'intérieur de laquelle tous les *actifs électroniques* doivent répondre aux exigences qui s'appliquent au *système électronique BES* ayant l'impact le plus élevé à l'intérieur de la zone (seuil de protection).

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

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

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

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

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

Dans le cas de la connectivité par lien commuté, l'intention de la SDT est de prévenir les situations où il serait possible d'établir une liaison directe avec un *actif électronique BES* au moyen d'un numéro de téléphone uniquement. Si un modem est configuré de manière à simplement répondre au téléphone et à établir la liaison avec l'*actif électronique BES* demandé sans authentifier le demandeur, il rend vulnérable le *système électronique BES*. En vertu de cette exigence, le modem doit authentifier le demandeur avant d'établir la communication avec le *système électronique BES*. […] L'exigence E2 s'applique également dans le cas d'une connectivité par lien commuté utilisée pour un *accès distant interactif*.

La norme ajoute une exigence pour les *centres de contrôle* concernant la détection des communications malveillantes. Ceci est en réponse à l'ordonnance 706 de la FERC, alinéas 496-503, stipulant qu'il faut prévoir deux dispositifs de sécurité distincts pour les *ESP* afin de préserver le périmètre de protection des *systèmes électroniques BES* advenant une défaillance ou un défaut de configuration de l'un ou l'autre de ces dispositifs. L'ordonnance indique clairement qu'il ne s'agit pas simplement d'assurer une redondance des pare-feu ; la SDT a donc décidé d'ajouter l'exigence liée à la mise en œuvre de moyens de détection des communications malveillantes pour les *ESP*. […]

Exigence E2

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

Justification

Pendant l'élaboration de la présente 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.

Justifications pour E1

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

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

L'exigence à l'alinéa 1.2 de la norme CIP-005 (versions 1 à 4) a été supprimée de la version 5. Cette exigence avait un caractère définitoire et servait à inclure les modems commutés utilisant

des protocoles non routables dans le domaine d'application de la norme CIP-005. L'exclusion liée aux protocoles non routables n'existant plus en tant que critère spécifique d'applicabilité (norme CIP-002) dans la version 5, cette exigence est dorénavant inutile.

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

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

Justification des modifications : (alinéa 1.1)

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

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

Justification des modifications : (alinéa 1.2)

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

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

Justification des modifications : (alinéa 1.3)

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

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

Justification des modifications apportées : (alinéa 1.4)

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

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

Justification des modifications : (alinéa 1.5)

Conformité avec l'Ordonnance 706 de la FERC, alinéas 496-503, en vertu de laquelle il faut prévoir deux dispositifs de sécurité distincts pour les *ESP* afin de préserver le périmètre de protection des *actifs électroniques* advenant une défaillance ou un défaut de configuration de l'un ou l'autre de ces dispositifs. L'Ordonnance indique clairement qu'il ne s'agit pas simplement d'assurer une redondance des pare-feu ; la SDT a donc décidé d'ajouter l'exigence liée à la mise en œuvre de moyens de détection des communications malveillantes pour les *ESP*.

Justifications pour E2

Les entités inscrites utilisent l'*accès distant interactif* pour accéder aux *actifs électroniques* en vue d'assurer le soutien et la maintenance des réseaux de systèmes de commande. La détection et le signalement des vulnérabilités dans les technologies et les méthodes d'accès distant, que l'on croyait sécurisées et qui étaient utilisées par des entités du secteur électrique, nécessitent que l'on apporte des modifications aux normes de contrôle de la sécurité au sein de l'industrie. Actuellement, aucune exigence n'oblige les gestionnaires d'un accès distant sécurisé

à des *actifs électroniques* à se doter des mesures de protection mentionnées dans les normes CIP de la NERC. Des dispositifs de protection inadéquats peuvent permettre un accès non autorisé au réseau de l'organisation, ce qui pourrait entraîner des conséquences graves. Le document ***Guidance for Secure Interactive Remote Access***, publié par la NERC en juillet 2011, renferme davantage de renseignements à cet égard.

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

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

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

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

[…]

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

Référence à une version précédente : (alinéa 2.1) Nouveau

Justification des modifications apportées : (alinéa 2.1)

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

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

Justification des modifications apportées : (alinéa 2.2)

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

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

Justification des modifications apportées : (alinéa 2.3)

Nouvelle exigence visant à poursuivre les efforts de l'équipe d'intervention rapide affectée au projet 2010-15 (révision accélérée de la norme CIP-005-3). Les méthodes d'authentification multifactorielle sont décrites dans la Homeland Security Presidential Directive 12 (HSPD-12) du 12 août 2007.

Justification des modifications apportées : (alinéas 2.4 et 2.5)

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

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

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

VERSION PRÉLIMINAIRE

Cybersécurité – Gestion des changements de configuration et analyses de vulnérabilité

Justification technique de la norme de fiabilité CIP-010-4

Octobre 2020

FIABILITÉ | RÉSILIENCE | SÉCURITÉ

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table des matières

Préface iv
Introduction v
Termes nouveaux ou modifiés utilisés dans les normes de fiabilité de la NERC 6
Exigence E1 7
Remarques générales sur l'exigence E1 7
Justification de l'exigence 1 7
Configuration de référence 9
Mécanismes de cybersécurité 9
Environnement d'essai 10
Vérification des logiciels 10
Exigence E2 11
Justification de l'exigence E2 11
Surveillance des configurations de référence 11
Exigence E3 12
Justification de l'exigence E3 12
Analyses de vulnérabilité 12
Exigence E4 13
Justification de l'exigence E4 13
Résumé des changements 13
Actifs électroniques temporaires et *supports de stockage amovibles* 13
Atténuation du risque lié aux vulnérabilités 14
Prise en compte des capacités de l'*actif électronique temporaire* 14
Annexe 1 16
Exigence E4, section 1 de l'annexe 1 – *Actifs électroniques temporaires* gérés par l'entité responsable 16
Exigence E4, section 2 de l'annexe 1 – *Actifs électroniques temporaires* gérés par une tierce partie autre que l'entité responsable 16
Exigence E4, section 3 de l'annexe 1 – *Supports de stockage amovibles* 16
Justification technique de la norme de fiabilité CIP-010-3 18
Section 4 – Portée de l'applicabilité des normes CIP sur la cybersécurité 18
Exigence E1 18
Configuration de référence 18
Mécanismes de cybersécurité 19
Environnement d'essai 19
Vérification des logiciels 19
Exigence E2 20

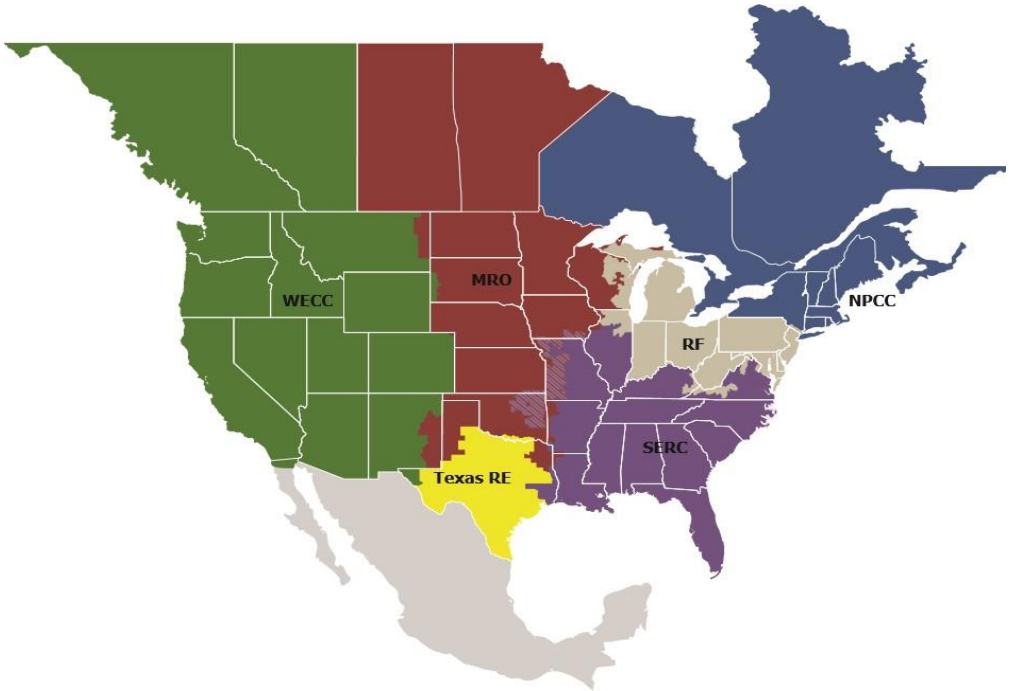
Exigence E3.....20
Exigence E4.....20
Exigence E4, section 1 de l'annexe 1 – *Actifs électroniques temporaires* gérés par l'entité responsable 21
Exigence E4, section 2 de l'annexe 1 – *Actifs électroniques temporaires* gérés par une tierce partie autre que l'entité responsable.....24
Exigence E4, section 3 de l'annexe 1 – *Supports de stockage amovibles*.....25
Justification 27
Justification de l'exigence E1.....27
Justification de l'exigence E2.....27
Justification de l'exigence E3.....27
Justification de l'exigence E4.....27
Résumé des changements.....27

Préface

L'électricité est un élément essentiel du tissu de nos sociétés modernes, et l'organisme de fiabilité électrique (ERO) a pour mission de renforcer ce tissu. L'ERO, qui regroupe la North American Electric Reliability Corporation (NERC) et les six entités régionales, veille à maximiser la fiabilité et la sécurité du *système électrique interconnecté* (*BPS*) de l'Amérique du Nord. Nous travaillons en permanence à réduire de manière efficace et efficiente les risques pour la fiabilité et la sécurité du réseau électrique.

Fiabilité | Résilience | Sécurité
Parce que près de 400 millions de citoyens en Amérique du Nord comptent sur nous

Le *système électrique interconnecté* de l'Amérique du Nord est divisé en six territoires d'entités régionales, comme le montrent la carte et le tableau ci-dessous. Les zones combinant deux couleurs indiquent des chevauchements, car certains *responsables de l'approvisionnement* sont actifs dans une région alors que les *propriétaires d'installation de transport* et les *exploitants de réseau de transport* associés sont actifs dans une autre région.



MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst Corporation
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

Introduction

Ce document expose la justification technique de la norme de fiabilité CIP-010-4 proposée. Il vise à guider les parties prenantes ainsi que l'ERO dans la compréhension des enjeux technologiques et des exigences techniques de cette norme de fiabilité. Le présent document, *Justification technique de la norme de fiabilité CIP-010-4*, n'est pas une norme de fiabilité et son contenu ne doit donc pas être considéré comme obligatoire et exécutoire.

Le 18 octobre 2018, la Federal Energy Regulatory Commission (FERC) publiait l'Ordonnance 850[1] dans laquelle elle demandait de modifier les différentes normes concernant la chaîne d'approvisionnement. Le sommaire à la page 1 de ce document stipule ce qui suit : « …la Commission demande à la NERC d'élaborer et de soumettre des modifications aux normes de fiabilité sur la gestion des risques dans la chaîne d'approvisionnement de manière à étendre la portée de ces normes aux *systèmes de contrôle ou de surveillance des accès électroniques* ». Par ailleurs, dans son rapport du 17 mai 2019 sur les risques de cybersécurité dans la chaîne d'approvisionnement[2], la NERC recommandait de modifier les normes sur la chaîne d'approvisionnement afin d'étendre leur portée aux *systèmes de contrôle des accès physiques* (*PACS*) qui assurent le contrôle des accès physiques à des *systèmes électroniques BES* à impact moyen ou élevé.

L'équipe de rédaction du projet 2019-03 a donc formulé la norme de fiabilité CIP-010-4 de manière à exiger des entités responsables qu'elles respectent les prescriptions de l'Ordonnance 850 de la FERC et du rapport de la NERC sur les risques de cybersécurité dans la chaîne d'approvisionnement.

1. https://www.nerc.com/FilingsOrders/us/FERCOrdersRules/Order%20No.%20850%20Supply%20Chain%20Risk%20Management%20Reliability%20Standards.pdf
2. NERC, *Cyber Security Supply Chain Risks, Staff Report and Recommended Actions*, 17 mai 2019. https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf

Termes nouveaux ou modifiés utilisés dans les normes de fiabilité de la NERC

La norme CIP-010-4 utilise la ou les définitions suivantes, qui sont reproduites ci-après pour référence au cours de la lecture de la justification technique qui suit.

Termes modifiés proposés : aucun.

Nouveaux termes proposés : aucun.

Exigence E1

Remarques générales sur l'exigence E1

Les paragraphes 5 et 30 de l'Ordonnance 850 de la FERC demandent de modifier l'exigence E1 de la norme de fiabilité CIP-010-3 de manière à étendre la gestion des risques dans la chaîne d'approvisionnement aux *systèmes de contrôle ou de surveillance des accès électroniques* (*EACMS*) associés aux *systèmes électroniques BES* à impact élevé ou moyen. Par ailleurs, la NERC recommande de modifier les normes sur la chaîne d'approvisionnement afin d'étendre leur portée aux *systèmes de contrôle des accès physiques* (*PACS*) qui assurent le contrôle des accès physiques (à l'exclusion des fonctions d'alarme et de consignation) à des *systèmes électroniques BES* à impact élevé ou moyen ; l'équipe de rédaction des normes du projet 2019-03 a mis en œuvre ces prescriptions.

Justification de l'exigence 1

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

L'alinéa 1.6 de l'exigence E1 répond au paragraphe 48 de l'Ordonnance 829 de la FERC, qui demande de vérifier l'intégrité et l'authenticité des logiciels avant leur installation dans les *systèmes électroniques BES*. L'exigence de vérifier l'intégrité et l'authenticité des logiciels vise à ce que les logiciels installés dans les *systèmes électroniques BES* n'aient pas été modifiés à l'insu de leur fournisseur, et qu'ils ne soient pas contrefaits.

L'alinéa 1.6 de l'exigence E1 répond aux paragraphes 5 et 30 de l'Ordonnance 850 de la FERC, qui demande de vérifier l'intégrité et l'authenticité des logiciels avant leur installation dans les *EACMS* ; cette vérification vise aussi les *PACS*, selon la recommandation du rapport de la NERC sur les risques de cybersécurité dans la chaîne d'approvisionnement[3]. L'exigence de vérifier l'intégrité et l'authenticité des logiciels vise à ce que les logiciels installés dans les *EACMS* et les *PACS* n'aient pas été modifiés à l'insu de leur fournisseur avant l'installation, et qu'ils ne soient pas contrefaits.

Étant donné la nature des *PACS* et le besoin potentiel d'une présence physique, l'équipe de rédaction s'est livrée à un sérieux travail de consultation et de réflexion relativement à l'inclusion des *PACS* dans la portée des exigences. L'équipe de rédaction a finalement conclu que le risque que représente un *PACS* compromis, mal utilisé, endommagé ou indisponible pour la fiabilité du *BES* justifie l'inclusion des *PACS* parmi les catégories d'*actifs électroniques* visées par les contrôles de sécurité axés sur la gestion des risques dans la chaîne d'approvisionnement. En outre, l'inclusion des *PACS* :

1. répond à la préoccupation énoncée par la FERC au paragraphe 6 de l'Ordonnance 850, où elle rappelle que « l'exclusion de ces éléments peut constituer une lacune dans les normes de fiabilité sur la gestion des risques dans la chaîne d'approvisionnement » ;

2. répond au souhait formulé au paragraphe 24 de l'Ordonnance 850, où la FERC propose de « demander que la NERC évalue les risques de cybersécurité dans la chaîne

3. NERC, *Cyber Security Supply Chain Risks, Staff Report and Recommended Actions*, 17 mai 2019. https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf

d'approvisionnement associés aux *PACS* et aux *PCA* (*actifs électroniques protégés*) dans le cadre de l'étude des risques de cybersécurité dans la chaîne d'approvisionnement demandée par le Conseil d'administration de la NERC dans ses résolutions du 10 août 2017 ; et

3. répond directement à la recommandation d'inclusion des *PACS* formulée par la NERC dans son rapport final sur les risques de cybersécurité dans la chaîne d'approvisionnement[4].

Autre argument à l'appui de la décision de l'équipe de rédaction d'étendre aux *PACS* la portée de la norme, on peut lire à la page 4 du rapport final de la NERC sur les risques de cybersécurité dans la chaîne d'approvisionnement : « Les normes de fiabilité CIP de la NERC établissent une démarche de défense en profondeur axée sur les risques, visant à sécuriser le *BES* contre les menaces de cybersécurité et de sécurité physique. » Cette phrase est tirée d'un contexte qui concerne les *EACMS*, mais elle mentionne bel et bien la sécurité physique ; par conséquent, le principe est transférable et applicable aux *PACS*, qui font partie intégrante d'une stratégie de déploiement de couches successives de mécanismes de détection et de prévention. Les *PACS* ont pour fonction de gérer les accès physiques aux *systèmes électroniques BES* afin de protéger ceux-ci contre les compromissions qui pourraient entraîner un fonctionnement incorrect ou des instabilités dans le *BES*, et ils sont mis en place expressément pour protéger les *systèmes électroniques BES*.

On peut également lire à la page 15 du rapport final de la NERC sur les risques de cybersécurité dans la chaîne d'approvisionnement : « En outre, un auteur de menace doit être physiquement présent sur les lieux de l'installation afin d'exploiter la vulnérabilité qui réside dans un *PACS* compromis. Un auteur de menace pourrait aussi devoir contourner plusieurs autres mesures de contrôle ou de surveillance des accès physiques qui n'auraient pas été compromises afin d'obtenir l'accès souhaité. » Certes, la compromission d'un *PACS* peut ne pas elle-même permettre de produire un effet nuisible immédiat (délai de 15 minutes) pour la fiabilité du *BES* ; cependant, il est évident que l'intention d'un auteur de menace d'obtenir un accès électronique non autorisé à un *PACS* indique qu'il s'agit d'une manœuvre initiale intentionnelle 1) en vue d'activités de reconnaissance clandestines, et 2) menant à une compromission méthodique permettant d'attaquer par la suite les *systèmes électroniques BES* que le *PACS* est censé protéger.

Par ailleurs, il existe un précédent à l'alinéa 1.5 de l'exigence E1 de la norme CIP-006-6, qui témoigne de l'importance accordée aux *PACS*, à leurs fonctions ainsi qu'aux délais liés à l'information transmise par ces systèmes en exigeant le déclenchement d'une alarme ou d'une alerte en réponse à la détection d'un accès non autorisé à un point d'accès physique d'un *périmètre de sécurité physique* (*PSP*), à l'intention du personnel d'intervention, dans les 15 minutes suivant la détection. Ce délai impérieux souligne l'imminence de la menace que la compromission de la sécurité physique représente pour le *système électronique BES* associé et pour l'exploitation fiable des *installations* de *BES* qu'il dessert.

L'équipe de rédaction convient que la NERC renvoie à juste titre à diverses normes de fiabilité qui atténuent certains risques pour la sécurité relativement aux *PACS* ; cependant, l'équipe de rédaction soutient que ces exigences existantes ne couvrent pas les risques associés à la chaîne d'approvisionnement, et qu'elles n'atténuent donc pas suffisamment ces risques.

4. NERC, *Cyber Security Supply Chain Risks, Staff Report and Recommended Actions*, 17 mai 2019. https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf

L'équipe de rédaction a pris en considération un autre aspect du rapport de la NERC sur les risques de cybersécurité dans la chaîne d'approvisionnement : il s'agit du risque associé aux différentes fonctions des *EACMS* et des *PACS*. Le rapport de la NERC soulignait un risque accru pour la partie contrôle des *EACMS* et des *PACS*, et l'équipe de rédaction a envisagé de limiter la portée des exigences aux seuls *EACMS* et *PACS* assurant des fonctions de contrôle. Cependant, comme les définitions actuellement en vigueur spécifient le contrôle et la surveillance pour les *EACMS*, et le contrôle, le signalement et la consignation pour les *PACS*, l'équipe de rédaction a conclu que l'emploi de termes faisant autorité entraînerait moins de confusion. L'équipe de rédaction n'a pas voulu modifier les définitions, considérant l'utilisation très répandue des termes *EACMS* et *PACS* dans toutes les normes, et aussi que la demande SAR ne l'autorisait pas à aller modifier toutes ces normes.

Configuration de référence

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

Les configurations de référence dans la norme CIP-010 comportent cinq éléments : le système d'exploitation ou le système embarqué ; les logiciels commerciaux ou les logiciels libres ; les logiciels personnalisés ; les ports logiques accessibles par le réseau ; et les correctifs de sécurité. L'information sur le système d'exploitation précise le nom et la version du logiciel en cours d'utilisation dans l'*actif électronique*. En l'absence de système d'exploitation indépendant (par exemple pour un relais de protection), l'information sur le système embarqué devrait être précisée. Les logiciels commerciaux ou les logiciels libres sont ceux qui ont été installés intentionnellement dans l'*actif électronique*. L'utilisation du mot « intentionnellement » vise à préciser que seuls les logiciels jugés nécessaires pour les *actifs électroniques* doivent être inclus dans la configuration de référence. L'équipe de rédaction ne souhaite pas que soient inclus dans cette configuration les calepins, les calculettes, les DLL, les pilotes de périphérique ou d'autres applications compris dans un système d'exploitation commercial ou distribués à titre de logiciel libre. Les logiciels personnalisés installés peuvent comprendre des scripts programmés pour des fonctions locales de l'entité ou d'autres programmes créés en vue d'une tâche ou fonction spécifique à l'entité. Dans le cas d'un logiciel supplémentaire qui a été installé intentionnellement et qui n'est ni un logiciel commercial ni un logiciel libre, ce logiciel pourrait être considéré comme un logiciel personnalisé. Si un dispositif a besoin de communiquer avec un autre dispositif à l'extérieur du réseau, les communications doivent être limitées aux seuls dispositifs qui doivent communiquer, conformément à la norme CIP-007-6. Les ports accessibles doivent être indiqués dans la configuration de référence. Les correctifs de sécurité appliqués doivent comprendre tous les correctifs antérieurs et courants appliqués sur l'*actif électronique*. Alors que l'alinéa 2.1 de l'exigence E2 de la norme CIP-007-6 stipule que les entités doivent se tenir informées des correctifs de sécurité, les évaluer et les appliquer, l'alinéa 1.1.5 de l'exigence E1 de la norme CIP-010 stipule que les entités doivent consigner tous les correctifs appliqués, antérieurs et courants.

Mécanismes de cybersécurité

Les mécanismes de cybersécurité dont il est question renvoient spécifiquement aux mécanismes des normes CIP-005 et CIP-007. Les alinéas pertinents de l'exigence E1 de la norme CIP-010 stipulent que l'entité doit déterminer et analyser les mécanismes des normes CIP-005 et CIP-007 qui pourraient être touchés par un changement par rapport à la configuration de référence existante. L'équipe de rédaction ne souhaite pas obliger l'entité

responsable à passer en revue tous les mécanismes de cybersécurité des normes CIP-005 et CIP-007 pour chaque changement, mais seulement le ou les mécanismes susceptibles d'être touchés par le changement en question. Par exemple, les changements relatifs aux ports logiques concernent seulement l'exigence E1 de la norme CIP-007 (ports et services), tandis que les changements relatifs aux correctifs de sécurité concernent seulement l'exigence E2 de la norme CIP-007 (gestion des correctifs de sécurité). L'équipe de rédaction a choisi de ne pas préciser les exigences des normes CIP-005 et CIP-007 dans le texte de la norme CIP-010, étant donné que n'importe lequel des mécanismes de cybersécurité de ces normes peut être touché par suite d'un changement dans la configuration de référence. L'équipe de rédaction considère qu'il est possible que toutes les exigences des normes CIP-005 et CIP-007 soient touchées par un changement important dans la configuration de référence, et c'est pourquoi les normes CIP-005 et CIP-007 sont citées dans leur globalité plutôt qu'à l'échelon de leurs exigences individuelles.

Environnement d'essai

La formulation relative à l'utilisation d'un environnement d'essai servant à déterminer tout écart par rapport à la configuration de référence a été choisie expressément pour les cas où il serait impossible de dupliquer certains éléments de *système électronique BES* d'un *centre de contrôle*.

Vérification des logiciels

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

Exigence E2

Justification de l'exigence E2

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

Surveillance des configurations de référence

L'idée maîtresse de l'exigence E2 est la surveillance automatisée du *système électronique BES*. Cependant, l'équipe de rédaction reconnaît que certains *actifs électroniques* se prêtent mal à une surveillance automatisée.

Exigence E3

Justification de l’exigence E3

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

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

Analyses de vulnérabilité

L’entité responsable doit prendre note que l’exigence d’analyse de vulnérabilité fait une distinction entre analyse sur papier et analyse active. Cette distinction s’appuie sur l’Ordonnance 706 de la FERC et la proposition réglementaire (Notice of Proposed Rulemaking) connexe.

Exigence E4

Justification de l'exigence E4

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

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

L'exigence E4 intègre les concepts d'autres exigences des normes CIP-010-2 et CIP-007-6 afin d'aider à définir les exigences applicables aux *actifs électroniques temporaires* et aux *supports de stockage amovibles*.

Résumé des changements

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

Actifs électroniques temporaires et *supports de stockage amovibles*

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

Les *actifs électroniques temporaires* et les *supports de stockage amovibles* sont des dispositifs connectés temporairement : 1) à un *actif électronique BES*, 2) à un réseau à l'intérieur d'un *périmètre de sécurité électronique* ou 3) à un *actif électronique protégé*. Les *actifs électroniques*

temporaires et les *supports de stockage amovibles* n'assurent pas de services liés à la fiabilité du *BES* et ne font pas partie de l'*actif électronique BES* auquel ils sont connectés.

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

Bien que les définitions d'*actif électronique temporaire* et de *support de stockage amovible* comprennent une condition qui limite à 30 jours leur durée de connexion, la section 1.1 de l'annexe 1 permet à l'entité responsable d'incorporer à son plan des traitements appliqués en permanence ou à la demande ainsi que des mesures indépendantes de l'état de connexion ou de déconnexion. Il est à noter qu'un traitement à la demande n'est à appliquer que lorsqu'on s'apprête à connecter l'*actif électronique temporaire* ou le *support de stockage amovible* à un *système électronique BES* ou à un *actif électronique protégé* ; une fois l'*actif électronique temporaire* ou le *support de stockage amovible* déconnecté, les exigences présentées ici cessent de s'appliquer tant qu'on ne s'apprête pas de nouveau à le connecter à l'*actif électronique BES* ou à l'*actif électronique protégé*.

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

À partir de la liste d'options présentée à l'annexe 1 pour chacun des thèmes de cybersécurité, l'entité responsable est libre de choisir le ou les moyens qui lui conviennent le mieux. L'entité responsable est invitée à documenter comment et quand elle entend gérer les *actifs électroniques temporaires* sous son contrôle ou examiner ceux placés sous le contrôle d'autres entités.

Atténuation du risque lié aux vulnérabilités

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

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

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

capacité de faire fonctionner un logiciel antivirus ; par conséquent, la mise en œuvre d'un logiciel antivirus ne serait pas exigée pour ces dispositifs.

Annexe 1

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

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

Section 1.2 – Les entités doivent documenter et mettre en œuvre leurs processus d'autorisation pour l'utilisation des *actifs électroniques temporaires* qu'ils gèrent directement. Les *actifs électroniques temporaires* peuvent être désignés individuellement ou par type d'actifs.

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

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

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

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

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

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

doivent procéder à la détection des programmes malveillants sur les *supports de stockage amovibles* avant qu'ils soient connectés à un *actif électronique BES*. Un choix judicieux du moment des interventions de détection, documenté dans le plan de l'entité, devrait réduire le risque d'introduction de programmes malveillants dans l'*actif électronique BES* ou l'*actif électronique protégé*.

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

Justification technique de la norme de fiabilité CIP-010-3

Cette section reproduit l'essentiel du texte de la section *Principes directeurs et fondements techniques* de la norme CIP-010-3, à titre de référence historique. Par ailleurs, le contenu de cette même section qui donne des indications sur la conformité est repris dans un Guide d'application distinct pour la présente norme.

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

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

La section 4.1 (Entités fonctionnelles) présente la liste des entités fonctionnelles de la NERC auxquelles s'applique la norme. Si l'entité est enregistrée au titre d'une ou de plusieurs des entités fonctionnelles énumérées à la section 4.1, les normes CIP sur la cybersécurité de la NERC s'y appliquent. Il est à noter qu'en ce qui concerne les *distributeurs*, la section 4.1 limite l'applicabilité à ceux qui détiennent certains types de systèmes et d'équipements énumérés à la section 4.2.

La section 4.2 (Installations) définit la portée des *installations*, systèmes et équipements détenus par l'entité responsable qui, selon la section 4.1, est visée par les exigences de la norme. Comme il est indiqué à la section d'exemption 4.2.3.5, la présente norme ne s'applique pas aux entités responsables qui n'ont pas de *systèmes électroniques BES* à impact élevé ou moyen selon la catégorisation de la norme CIP-002-5.1. Outre l'ensemble des *installations* du *BES*, des *centres de contrôle* et des autres systèmes et équipements, la liste comprend l'ensemble des systèmes et équipements détenus par les *distributeurs*. Bien que le terme « *installations* » dans le glossaire de la NERC indique déjà qu'il s'agit d'*éléments* du *BES*, l'utilisation additionnelle du terme « *BES* » vise ici à renforcer la portée d'applicabilité pour ces *installations*, en particulier dans cette section sur l'applicabilité. Cela aide à clarifier quels sont les *installations*, systèmes et équipements visés par les normes.

Exigence E1

Configuration de référence

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

Les configurations de référence dans la norme CIP-010 comportent cinq éléments : le système d'exploitation ou le système embarqué ; les logiciels commerciaux ou les logiciels libres ; les logiciels personnalisés ; les ports logiques accessibles par le réseau ; et les correctifs de sécurité. L'information sur le système d'exploitation précise le nom et la version du logiciel en cours d'utilisation dans l'*actif électronique*. En l'absence de système d'exploitation indépendant (par exemple pour un relais de protection), l'information sur le système embarqué devrait être précisée. Les logiciels commerciaux ou les logiciels libres sont ceux qui ont été installés intentionnellement dans l'actif électronique. L'utilisation du mot « intentionnellement » vise à préciser que seuls les logiciels jugés nécessaires pour les *actifs électroniques* doivent être inclus dans la configuration de référence. La SDT ne souhaite pas que soient inclus dans cette configuration les calepins, calculettes, les DLL, les pilotes de périphérique ou d'autres

applications compris dans un système d'exploitation commercial ou distribués à titre de logiciel libre. Les logiciels personnalisés installés peuvent comprendre des scripts programmés pour des fonctions locales de l'entité ou d'autres programmes créés en vue d'une tâche ou fonction spécifique à l'entité. Dans le cas d'un logiciel supplémentaire qui a été installé intentionnellement et qui n'est ni un logiciel commercial ni un logiciel libre, ce logiciel pourrait être considéré comme un logiciel personnalisé. Si un dispositif a besoin de communiquer avec un autre dispositif à l'extérieur du réseau, les communications doivent être limitées aux seuls dispositifs qui doivent communiquer, conformément à la norme CIP-007-6. Les ports accessibles doivent être indiqués dans la configuration de référence. Les correctifs de sécurité appliqués doivent comprendre tous les correctifs antérieurs et courants appliqués sur l'actif électronique. Alors que l'alinéa 2.1 de l'exigence E2 de la norme CIP-007-6 stipule que les entités doivent se tenir informées des correctifs de sécurité, les évaluer et les appliquer, l'alinéa 1.1.5 de l'exigence E1 de la norme CIP-010 stipule que les entités doivent consigner tous les correctifs appliqués, antérieurs et courants.

[…]

Mécanismes de cybersécurité

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

Environnement d'essai

L'environnement d'essai du *centre de contrôle* (ou l'environnement de production dans lequel l'essai est effectué d'une manière qui réduit au minimum les effets dommageables) doit simuler la configuration de référence, mais peut le faire au moyen de composants différents. […]

En outre, l'entité responsable doit prendre note que, lorsqu'il est question d'un environnement d'essai (ou d'un environnement de production dans lequel l'essai est effectué d'une manière qui réduit au minimum les effets dommageables), il s'agit bien de « simuler » la configuration de référence, et non de la reproduire à l'identique. Cette formulation a été choisie expressément pour les cas où il serait impossible de dupliquer certains éléments de *système électronique BES* d'un *centre de contrôle*. […]

Vérification des logiciels

Le concept de vérification des logiciels (validation de l'identité de la source d'un logiciel et de l'intégrité du logiciel obtenu de cette source) est une mesure de contrôle essentielle pour prévenir l'introduction de maliciels ou de logiciels contrefaits. Cet objectif vise à réduire la

probabilité qu'un assaillant puisse exploiter les processus de gestion des correctifs de fournisseurs légitimes pour infiltrer dans un *système électronique BES* des mises à jour ou des correctifs de logiciel compromis. L'équipe de rédaction entend amener les entités responsables à établir des mesures pour vérifier les éléments de configuration de référence qui sont mis à jour par les fournisseurs. Soulignons que cette exigence n'est pas limitée aux correctifs de sécurité.

[…]

Exigence E2

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

Exigence E3

L'entité responsable doit prendre note que l'exigence d'analyse de vulnérabilité fait une distinction entre analyse sur papier et analyse active. Cette distinction s'appuie sur l'Ordonnance 706 de la FERC et la proposition réglementaire (*Notice of Proposed Rulemaking*) connexe.

[…]

Exigence E4

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

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

[…]

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

Bien que les définitions d'*actif électronique temporaire* et de *support de stockage amovible* comprennent une condition qui limite à 30 jours leur durée de connexion, la section 1.1 de l'annexe 1 permet à l'entité responsable d'incorporer à son plan des traitements appliqués en permanence ou à la demande ainsi que des mesures indépendantes de l'état de connexion ou de déconnexion. Il est à noter qu'un traitement à la demande n'est à appliquer que lorsqu'on s'apprête à connecter l'*actif électronique temporaire* ou le *support de stockage amovible* à un *système électronique BES* ou à un *actif électronique protégé* ; une fois l'*actif électronique temporaire* ou le *support de stockage amovible* déconnecté, les exigences présentées ici cessent de s'appliquer tant qu'on ne s'apprête pas de nouveau à le connecter à l'*actif électronique BES* ou à l'*actif électronique protégé*.

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

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

Atténuation du risque lié aux vulnérabilités

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

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

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

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

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

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

1.2.1 Les utilisateurs (individuellement, par groupe ou par rôle) autorisés à utiliser les *actifs électroniques temporaires*. On peut inscrire à cette fin le nom de la personne, le nom d'un service ou le titre d'un poste. Attention : il faut déterminer si ces utilisateurs doivent aussi avoir un accès électronique autorisé au système pertinent conformément à la norme CIP-004.

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

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

[…]

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

- L'application de correctifs, avec mises à jour manuelles ou systématiques, offre à l'entité responsable une certaine latitude quant à l'utilisation de ses *actifs électroniques temporaires*. L'entité peut décider de mettre en place pour ses *actifs électroniques temporaires* un processus normalisé d'application de correctifs de sécurité selon un calendrier régulier, ou plutôt d'appliquer les correctifs de sécurité nécessaires à un *actif électronique temporaire* avant de le connecter à un *actif électronique* visé. Contrairement à l'exigence E2 de la norme CIP-007, l'entité n'a pas à élaborer de plans d'atténuation datés ou d'autres documents au-delà de ce qui est nécessaire pour déterminer que l'*actif électronique temporaire* reçoit les correctifs de sécurité appropriés.
- L'utilisation de systèmes d'exploitation et de logiciels exécutables uniquement à partir de supports non inscriptibles permet d'avoir un système d'exploitation protégé qui ne peut être modifié de manière à transmettre des programmes malveillants. Lorsqu'une entité crée un système d'exploitation personnalisé sur support externe, elle doit vérifier l'image pendant sa création afin de s'assurer que l'image ne contient aucun programme malveillant.
- Le renforcement du système d'exploitation consiste à éliminer tous les logiciels et utilitaires non essentiels et à n'installer que le minimum indispensable au fonctionnement de l'ordinateur, ce qui aide à réduire les vulnérabilités. Les programmes

supplémentaires peuvent offrir des fonctionnalités utiles, mais ils peuvent aussi receler des « portes dérobées » d'accès au système ; leur élimination a pour effet de renforcer le système.

- Si elle opte pour des moyens autres que ceux qui sont suggérés pour atténuer le risque lié aux vulnérabilités logicielles, l'entité doit établir une documentation qui indique comment ces moyens réalisent l'objectif d'atténuer le risque en question.

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

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

Section 1.5 : Les entités doivent documenter et mettre en œuvre leurs processus de protection et d'évaluation des *actifs électroniques temporaires* visant à atténuer le risque qu'une utilisation non autorisée de ceux-ci peut présenter pour les *systèmes électroniques BES*. La préoccupation à laquelle répond cette section est la possibilité qu'un *actif électronique temporaire* puisse être manipulé de façon inappropriée ou être exposé à des logiciels malveillants pendant qu'il n'est pas utilisé aux fins prévues par une personne autorisée. La sécurité physique de l'*actif électronique temporaire* est assurément une mesure qui atténue ce

risque, mais d'autres outils et techniques sont aussi envisageables. La liste d'exemples ci-après présente différentes possibilités suggérées.

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

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

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

[…]

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

- Procéder à un examen de l'*actif électronique temporaire* géré par une tierce partie autre que l'entité responsable afin de déterminer si la version des correctifs de sécurité du dispositif atténue adéquatement le risque de vulnérabilités logicielles avant la connexion de l'actif *électronique temporaire* à un système visé.

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

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

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

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

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

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

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

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

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

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

Justification

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

Justification de l'exigence E1

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

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

Justification de l'exigence E2

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

Justification de l'exigence E3

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

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

Justification de l'exigence E4

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

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

L'exigence E4 intègre les concepts d'autres exigences des normes CIP-010-2 et CIP-007-6 afin d'aider à définir les exigences applicables aux *actifs électroniques temporaires* et aux *supports de stockage amovibles*.

Résumé des changements

Toutes les exigences relatives aux *actifs électroniques temporaires* et aux *supports de stockage amovibles* sont regroupées dans la norme CIP-010. En raison de la nouveauté de la définition

de ces types d'actifs et des exigences qui s'y appliquent, la SDT a jugé que le regroupement de ces exigences dans une seule et même norme aiderait les entités à reconnaître rapidement les exigences applicables à ces types d'actifs. La création d'une norme séparée pour ces exigences a été envisagée ; cependant, la SDT a déterminé que l'utilisation de ces types d'actifs est connexe aux processus de gestion des changements et d'analyse de vulnérabilité, et qu'il est en somme préférable de regrouper le tout dans la norme qui encadre déjà ces processus.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

VERSION PRÉLIMINAIRE

Cybersécurité – Gestion des risques dans la chaîne d'approvisionnement

Justification technique de la norme de fiabilité CIP-013-2

Octobre 2020

FIABILITÉ | RÉSILIENCE | SÉCURITÉ

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table des matières

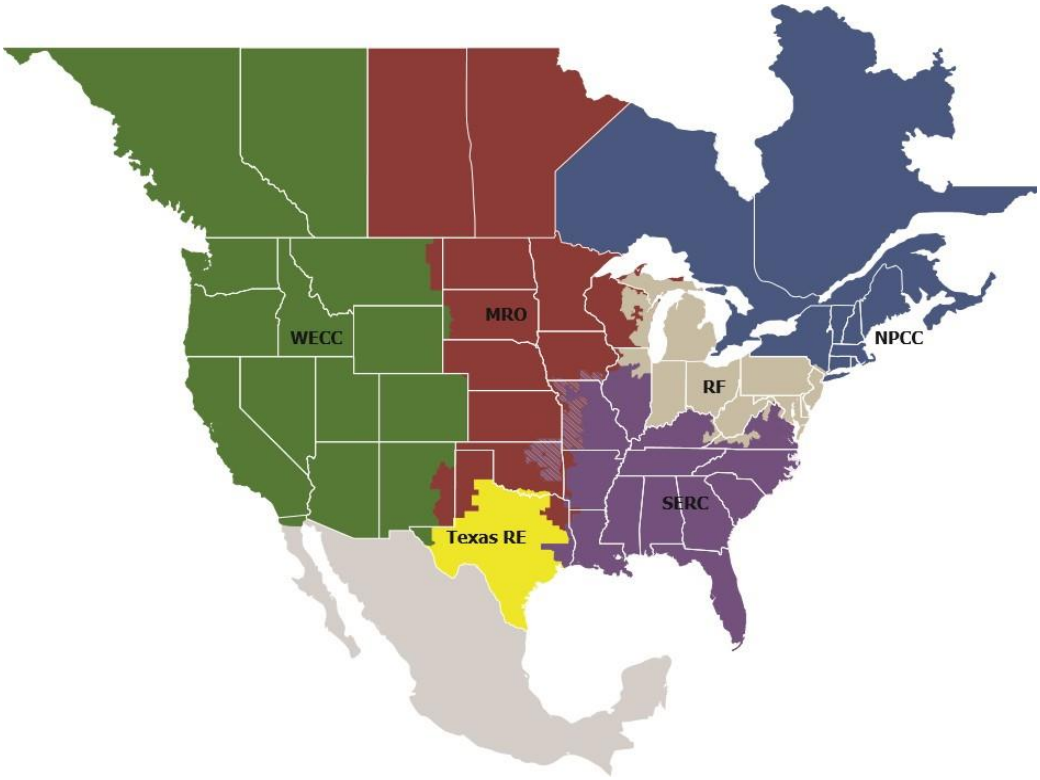
Préface iii
Introduction iv
Termes nouveaux ou modifiés utilisés dans les normes de fiabilité de la NERC 5
Exigences E1 et E2 6
Remarques générales sur les exigences E1 et E2 6
Justification des exigences E1 et E2 8
Exigence E3 10
Remarques générales sur l'exigence E3 10
Justification technique de la norme de fiabilité CIP-013-1 11

Préface

L'électricité est un élément essentiel du tissu de nos sociétés modernes, et l'organisme de fiabilité électrique (ERO) a pour mission de renforcer ce tissu. L'ERO, qui regroupe la North American Electric Reliability Corporation (NERC) et les six entités régionales, veille à maximiser la fiabilité et la sécurité du *système électrique interconnecté* (*BPS*) de l'Amérique du Nord. Nous travaillons en permanence à réduire de manière efficace et efficiente les risques pour la fiabilité et la sécurité du réseau électrique.

Fiabilité | Résilience | Sécurité
Parce que près de 400 millions de citoyens en Amérique du Nord comptent sur nous

Le *système électrique interconnecté* de l'Amérique du Nord est divisé en six territoires d'entités régionales, comme le montrent la carte et le tableau ci-dessous. Les zones combinant deux couleurs indiquent des chevauchements, car certains responsables de l'approvisionnement sont actifs dans une région alors que les *propriétaires d'installation de transport* et les *exploitants de réseau de transport* associés sont actifs dans une autre région.



MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst Corporation
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

Introduction

Ce document expose la justification technique de la norme de fiabilité CIP-013-2 proposée. Il vise à guider les parties prenantes ainsi que l'ERO dans la compréhension des enjeux technologiques et des exigences techniques de cette norme de fiabilité. Il présente aussi des précisions quant aux intentions de l'équipe de rédaction de la norme *Cybersécurité – Gestion des risques dans la chaîne d'approvisionnement* (projet 2019-03). Le présent document, *Justification technique de la norme de fiabilité CIP-013-2*, n'est pas une norme de fiabilité et son contenu ne doit donc pas être considéré comme obligatoire et exécutoire.

Le 18 octobre 2018, la Federal Energy Regulatory Commission (FERC) publiait l'Ordonnance 850, dans laquelle elle demandait de modifier les différentes normes sur la chaîne d'approvisionnement afin d'étendre leur portée aux *systèmes de contrôle ou de surveillance des accès électroniques* (*EACMS*), plus spécifiquement ceux qui assurent le contrôle ou la surveillance des accès électroniques à des *systèmes électroniques BES* à impact élevé ou moyen. Par ailleurs, dans son rapport du 17 mai 2019 sur les risques de cybersécurité dans la chaîne d'approvisionnement, la NERC recommandait de modifier les normes sur la chaîne d'approvisionnement afin d'étendre leur portée aux *systèmes de contrôle des accès physiques* (*PACS*) qui assurent le contrôle des accès physiques à des *systèmes électroniques BES* à impact élevé ou moyen.

L'équipe de rédaction du projet 2019-03 a donc formulé la norme de fiabilité CIP-013-2 de manière à exiger des entités responsables qu'elles respectent les prescriptions de l'Ordonnance 850 de la FERC et du rapport de la NERC sur les risques de cybersécurité dans la chaîne d'approvisionnement.

Termes nouveaux ou modifiés utilisés dans les normes de fiabilité de la NERC

La norme CIP-013-2 utilise la ou les définitions suivantes, qui sont reproduites ci-après pour référence au cours de la lecture de la justification technique qui suit.

Termes modifiés proposés : aucun.

Nouveaux termes proposés : aucun.

Exigences E1 et E2

Remarques générales sur les exigences E1 et E2

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

1) intégrité et authenticité des logiciels ;
2) accès distant par les fournisseurs ;
3) planification des systèmes d'information ; et
4) gestion des risques liés aux fournisseurs et contrôles d'approvisionnement.

Le ou les plans de gestion des risques de cybersécurité prescrits à l'exigence E1 s'appliquent aux *systèmes électroniques BES* à impact élevé ou moyen. Les paragraphes 5 et 30 de l'Ordonnance 850 de la FERC demandent de modifier les normes de fiabilité de manière à étendre la portée des normes sur la gestion des risques dans la chaîne d'approvisionnement aux *EACMS* associés aux *systèmes électroniques BES* à impact élevé ou moyen. De son côté, la NERC a aussi recommandé, dans son rapport du 17 mai 2019 sur les risques de cybersécurité dans la chaîne d'approvisionnement[1] (chapitre 3, pages 12 à 15), de modifier les normes sur la chaîne d'approvisionnement afin d'étendre leur portée aux *PACS* qui assurent le contrôle des accès physiques à des *systèmes électroniques BES* à impact élevé ou moyen.

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

Étant donné la nature des *PACS* et le besoin potentiel d'une présence physique, l'équipe de rédaction s'est livrée à un sérieux travail de consultation et de réflexion relativement à l'inclusion des *PACS* dans la portée des exigences. L'équipe de rédaction a finalement conclu que le risque pour la fiabilité du *BES* que représente un *PACS* compromis, mal utilisé, endommagé ou indisponible justifie l'inclusion des *PACS* parmi les catégories d'*actifs électroniques* visées par les contrôles de sécurité axés sur la gestion des risques dans la chaîne d'approvisionnement.

En outre, l'inclusion des *PACS* :

1. répond à la préoccupation énoncée par la FERC au paragraphe 6 de son Ordonnance 850, où elle rappelle que « l'exclusion de ces éléments peut constituer une lacune dans les normes de fiabilité sur la gestion des risques dans la chaîne d'approvisionnement » ;

2. répond au souhait formulé au paragraphe 24 de l'Ordonnance 850, où la FERC propose de « demander que la NERC évalue les risques de cybersécurité dans la chaîne d'approvisionnement associés aux *PACS* et aux *PCA* [(*actifs électroniques protégés*)] dans le cadre de l'étude des risques de cybersécurité dans la chaîne d'approvisionnement

1. NERC, *Cyber Security Supply Chain Risks, Staff Report and Recommended Actions*, 17 mai 2019. https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf

demandée par le Conseil d'administration de la NERC dans ses résolutions du 10 août 2017 » ; et

3. répond directement à la recommandation d'inclusion des *PACS* formulée par la NERC dans son rapport final sur les risques de cybersécurité dans la chaîne d'approvisionnement[2].

Autre argument à l'appui de la décision de l'équipe de rédaction d'étendre aux *PACS* la portée de la norme, on peut lire à la page 4 du rapport final de la NERC sur les risques de cybersécurité dans la chaîne d'approvisionnement : « Les normes de fiabilité CIP de la NERC établissent une démarche de défense en profondeur axée sur les risques, visant à sécuriser le *BES* contre les menaces de cybersécurité et de sécurité physique. » Cette phrase est tirée d'un contexte qui concerne les *EACMS*, mais elle mentionne bel et bien la sécurité physique ; par conséquent, le principe est transférable et applicable aux *PACS*, qui font partie intégrante d'une stratégie de déploiement de couches successives de mécanismes de détection et de prévention. Les *PACS* ont pour fonction de gérer les accès physiques aux *systèmes électroniques BES* afin de protéger ceux-ci contre les compromissions qui pourraient entraîner un fonctionnement incorrect ou des instabilités dans le *BES*, et ils sont mis en place expressément pour protéger les *systèmes électroniques BES*.

On peut également lire à la page 15 du rapport final de la NERC sur les risques de cybersécurité dans la chaîne d'approvisionnement : « En outre, un auteur de menace doit être physiquement présent sur les lieux de l'installation afin d'exploiter la vulnérabilité qui réside dans un *PACS* compromis. Un auteur de menace pourrait aussi devoir contourner plusieurs autres mesures de contrôle ou de surveillance des accès physiques qui n'auraient pas été compromises afin d'obtenir l'accès souhaité. » Bien que la compromission d'un *PACS* puisse ne pas elle-même permettre de produire un effet nuisible immédiat (délai de 15 minutes) pour la fiabilité du *BES*, elle pourrait signaler l'intention d'un auteur de menace d'obtenir un accès électronique non autorisé. Un accès électronique au *PACS* peut constituer une manœuvre initiale en vue d'activités de reconnaissance et de nuisance à des *systèmes électroniques BES*.

Par ailleurs, il existe un précédent à l'alinéa 1.5 de l'exigence E1 de la norme CIP-006-6, qui témoigne de l'importance accordée aux *PACS*, à leurs fonctions ainsi qu'aux délais liés à l'information transmise par ces systèmes en exigeant le déclenchement d'une alarme ou d'une alerte en réponse à la détection d'un accès non autorisé à un point d'accès physique d'un *périmètre de sécurité physique*, à l'intention du personnel d'intervention, dans les 15 minutes suivant la détection. Ce délai impérieux souligne l'imminence de la menace que la compromission de la sécurité physique représente pour le *système électronique BES* associé et pour l'exploitation fiable des *installations* de *BES* qu'il dessert.

L'équipe de rédaction convient que la NERC renvoie à juste titre à diverses normes de fiabilité qui atténuent certains risques pour la sécurité relativement aux *PACS* ; cependant, l'équipe de rédaction soutient que ces exigences existantes ne couvrent pas les risques associés à la chaîne d'approvisionnement, et qu'elles n'atténuent donc pas suffisamment ces risques.

Enfin, l'équipe de rédaction a pris en considération un autre aspect du rapport de la NERC sur les risques de cybersécurité dans la chaîne d'approvisionnement, concernant le risque associé aux différents aspects des *EACMS* et des *PACS*. Ces deux types de systèmes, selon leur définition actuelle, sont chargés de diverses activités fonctionnelles ; le rapport de la NERC, de son côté, souligne le risque accru associé à la fonction de contrôle. L'équipe de rédaction a

2. NERC, *Cyber Security Supply Chain Risks, Staff Report and Recommended Actions*, 17 mai 2019. https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf

envisagé de limiter la portée des exigences aux seules fonctions de contrôle, mais a finalement décidé de s'en tenir aux définitions approuvées des termes *EACMS* et *PACS*, considérant que cela entraînerait moins de confusion. Du reste, le fait de vouloir modifier les définitions des termes *EACMS* et *PACS* outrepasserait les limites de la demande SAR 2019-03.

Justification des exigences E1 et E2

L'alinéa 1.1 de l'exigence E1 met en œuvre les prescriptions du paragraphe 56 de l'Ordonnance 829 et du paragraphe 5 de l'Ordonnance 850 de la FERC, qui demandent de déterminer et de documenter les risques de cybersécurité associés aux processus de planification et de préparation en amont de l'acquisition de *systèmes électroniques BES* à impact élevé ou moyen, ainsi que des *EACMS* et des *PACS* associés. L'objectif de sécurité est d'une part d'amener les entités à envisager les risques de cybersécurité pour le *BES* liés aux produits et services de fournisseurs, résultant : i) de l'acquisition et de l'installation d'équipements et de logiciels de fournisseurs ; et ii) d'une transition entre fournisseurs. D'autre part, les entités doivent être amenées à envisager les moyens d'atténuer ces risques à l'étape de planification des *systèmes électroniques BES*.

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

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

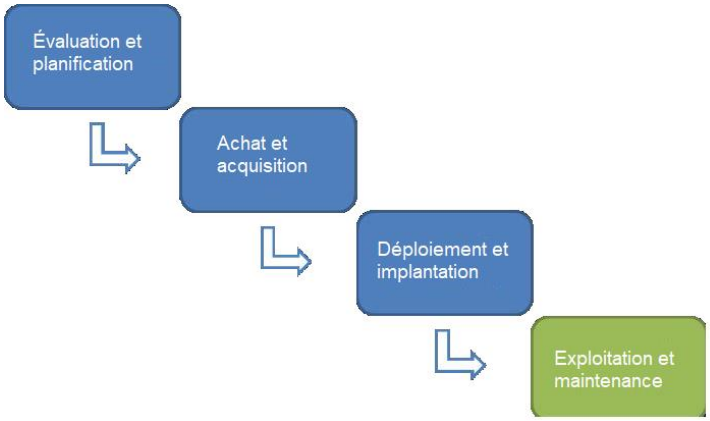
Les accès distants dont il est question à l'alinéa 1.2.6 comprennent les accès distants avec authentification commandés par un fournisseur et les accès distants par l'entremise de systèmes de fournisseur pour les *EACMS* et les *PACS* ; ils comprennent aussi les *accès distants interactifs* commandés par un fournisseur et les accès par l'entremise de systèmes de fournisseur à des *systèmes électroniques BES* et à des *PCA*.

Le terme « fournisseur » utilisé dans cette norme désigne uniquement les personnes, entreprises ou autres organisations avec lesquelles l'entité responsable, ou une organisation affiliée, est en relation contractuelle en vue de la fourniture de *systèmes électroniques BES* et de services connexes. Ce terme exclut les autres entités inscrites auprès de la NERC qui

fournissent des services de fiabilité (par exemple, des services de *responsable de l'équilibrage* ou de *coordonnateur de la fiabilité* dans le cadre des normes de fiabilité de la NERC). Un fournisseur, selon l'emploi de ce terme dans la norme, peut comprendre : i) des créateurs de logiciels ou de systèmes d'information, des fabricants de composants de système ou des prestataires de services informatiques ; ii) des revendeurs de produits ; ou iii) des intégrateurs de systèmes.

Collectivement, les dispositions de la norme CIP-013-2 concernent les contrôles d'une entité visant à gérer les risques de cybersécurité pour les *systèmes électroniques BES* pendant les phases de planification, d'acquisition et de déploiement du cycle de vie du système, selon le schéma ci-après.

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



Exigence E3

Remarques générales sur l'exigence E3

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

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

- de la NERC ou de l'E-ISAC ;
- de l'ICS-CERT ;
- du Centre canadien pour la cybersécurité (CCC).

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

Justification technique de la norme de fiabilité CIP-013-1

Cette section reproduit tel quel le texte de la section Compléments de la norme CIP-013-1, à titre de référence historique. Par ailleurs, le contenu de cette même section qui donne des indications sur la conformité est repris dans un Guide d'application distinct pour la présente norme.

Justification

Exigence E1

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

1) intégrité et authenticité des logiciels ;
2) accès distant par les fournisseurs ;
3) planification des systèmes d'information ; et
4) gestion des risques liés aux fournisseurs et contrôles d'approvisionnement.

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

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

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

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

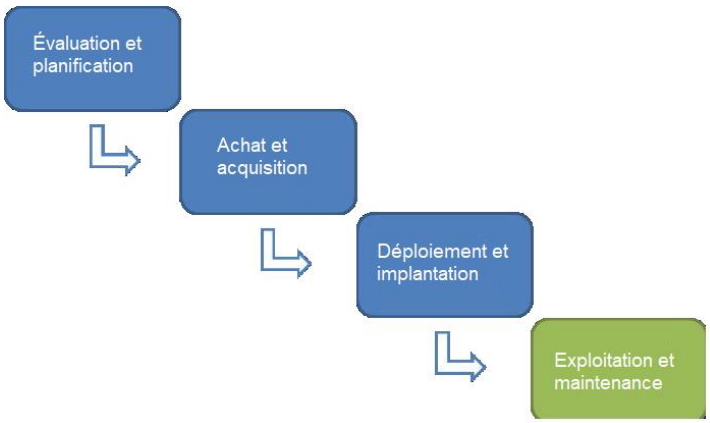
bien qu'on s'attende à ce que l'entité responsable veille à faire respecter les dispositions contractuelles relatives à la sécurité, la mise en exécution du contrat et le respect de celui-ci par le fournisseur ne sont pas visés par cette norme de fiabilité.

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

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

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

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



Exigence E2

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

Ces réévaluations périodiques permettent aux entités de tenir leurs plans à jour et de répondre aux inquiétudes et aux vulnérabilités, existantes ou émergentes, concernant la chaîne

d'approvisionnement. Les entités peuvent, par exemple, prendre en compte les directives ou autres informations provenant :

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

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

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

VERSION PRÉLIMINAIRE du Guide d'application en attente de la présentation à l'ERO pour approbation

VERSION PRÉLIMINAIRE

Cybersécurité – Périmètres de sécurité électronique

Guide d'application de la norme de fiabilité CIP-005-7

Octobre 2020

FIABILITÉ | RÉSILIENCE | SÉCURITÉ

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table des matières

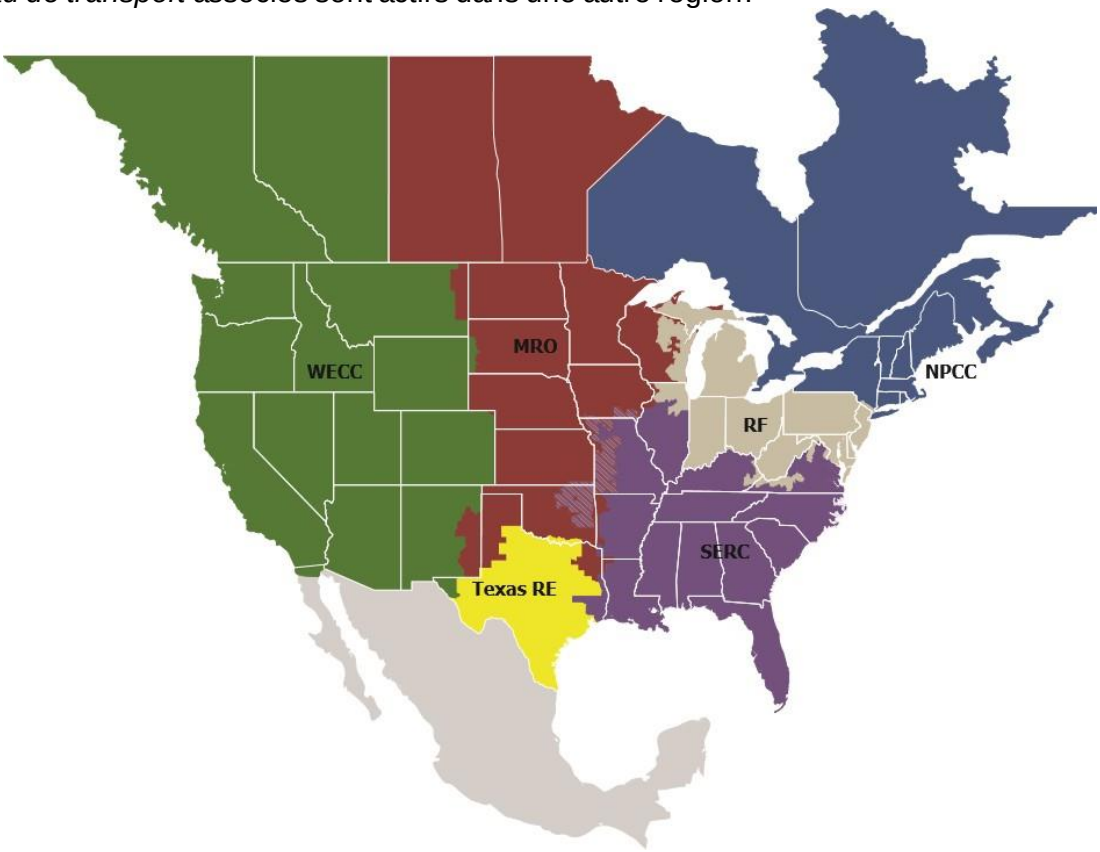
Preface.....1
Introduction 2
Requirement R3 3
Implementation Guidance for CIP-005-6.....5
Section 4 – Scope of Applicability of the CIP Cyber Security Standards**Erreur ! Signet non défini.**
Requirement R1: 5

Préface

L'électricité est un élément essentiel du tissu de nos sociétés modernes, et l'organisme de fiabilité électrique (ERO) a pour mission de renforcer ce tissu. L'ERO, qui regroupe la North American Electric Reliability Corporation (NERC) et les six entités régionales, veille à maximiser la fiabilité et la sécurité du *système électrique interconnecté* (*BPS*) de l'Amérique du Nord. Nous travaillons en permanence à réduire de manière efficace et efficiente les risques pour la fiabilité et la sécurité du réseau électrique.

Fiabilité | Résilience | Sécurité
Parce que près de 400 millions de citoyens en Amérique du Nord comptent sur nous

Le *système électrique interconnecté* de l'Amérique du Nord est divisé en six territoires d'entités régionales, comme le montrent la carte et le tableau ci-dessous. Les zones combinant deux couleurs indiquent des chevauchements, car certains *responsables de l'approvisionnement* sont actifs dans une région alors que les *propriétaires d'installation de transport* et les *exploitants de réseau de transport* associés sont actifs dans une autre région.



MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst Corporation
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

Introduction

L'équipe de rédaction des normes sur les risques de cybersécurité dans la chaîne d'approvisionnement (projet 2019-03) a produit le présent Guide d'application afin de présenter des exemples de démarches de mise en conformité avec la norme CIP-005-7. Ce Guide d'application ne prescrit pas une seule et unique démarche possible, mais met de l'avant diverses manières de réaliser la conformité avec la norme. Il ne s'agit d'ailleurs que d'exemples, et les entités sont donc libres de choisir toute autre démarche plus adaptée à leur situation particulière[1]. Le présent *Guide d'application de la norme de fiabilité CIP-005-7* n'est pas une norme de fiabilité et son contenu ne doit donc pas être considéré comme obligatoire et exécutoire.

Les entités responsables pourront compléter utilement la lecture du présent Guide d'application en consultant l'information présentée par l'équipe de rédaction dans le document de justification technique des modifications de la norme CIP-005-7.

Le 18 octobre 2018, la Federal Energy Regulatory Commission (FERC) publiait l'Ordonnance 850, dans laquelle elle demandait de modifier les différentes normes sur la chaîne d'approvisionnement afin d'étendre leur portée aux *systèmes de contrôle ou de surveillance des accès électroniques* (*EACMS*), plus spécifiquement ceux qui assurent le contrôle ou la surveillance des accès électroniques à des *systèmes électroniques BES* à impact élevé ou moyen. Par ailleurs, dans son rapport du 17 mai 2019 sur les risques de cybersécurité dans la chaîne d'approvisionnement, la NERC recommandait de modifier les normes sur la chaîne d'approvisionnement afin d'étendre leur portée aux *systèmes de contrôle des accès physiques* (*PACS*) qui assurent le contrôle des accès physiques à des *systèmes électroniques BES* à impact élevé ou moyen.

L'équipe de rédaction du projet 2019-03 a donc formulé la norme de fiabilité CIP-005-7 de manière à exiger des entités responsables qu'elles respectent les prescriptions de l'Ordonnance 850 de la FERC et du rapport de la NERC sur les risques de cybersécurité dans la chaîne d'approvisionnement.

1. Politique de la NERC relative aux lignes directrices sur la conformité

Exigence E3

L'équipe de rédaction 2019-03 a ajouté l'exigence E3 portant sur la gestion des accès distants des fournisseurs pour les *EACMS* et les *PACS*, et créé les nouveaux alinéas 3.1 et 3.2 en réponse à l'Ordonnance 850 de la FERC et au rapport de la NERC sur les risques de cybersécurité dans la chaîne d'approvisionnement. Si une entité permet l'accès distant à ses *EACMS* et à ses *PACS*, la méthode utilisée pour déterminer les connexions à distance authentifiées commandées par des fournisseurs est documentée et une capacité de désactivation des accès distants est exigée. Par exemple, si une entité utilise sa solution d'accès distant d'entreprise pour autoriser les connexions à distance à ses *PACS*, il incombe à cette entité de documenter la méthode d'authentification des connexions à distance et de créer un processus pour interrompre ces connexions après authentification. Quelques exemples non limitatifs de moyens simples utilisables par une entité pour interrompre ces connexions : désactiver un jeton ou un certificat de sécurité de compte de fournisseur, suspendre ou supprimer des comptes de fournisseur dans Active Directory, bloquer une plage d'adresses IP de fournisseur, ou débrancher physiquement un câble réseau.

L'utilisation de *systèmes intermédiaires* (qui constituent un sous-ensemble des *EACMS*) n'est pas exigée pour l'accès distant à d'autres *EACMS*, ce qui réduit le potentiel de demandes récursives (« en cascade »). Cependant, si une entité utilise le même système (un *système intermédiaire* par exemple) pour des connexions à distance et pour l'accès tant à ses *systèmes électroniques BES* qu'à ses *EACMS* (à l'intérieur du *périmètre de sécurité électronique*), le processus d'interruption des connexions à distance commandées par des fournisseurs commence après que l'entité a déterminé, à partir d'une authentification, qu'une certaine tentative de connexion ne doit pas être autorisée. Pour cet exemple, supposons que l'entité utilise un hôte de rebond comme *système intermédiaire* avec authentification multifactorielle et Active Directory. Lorsque le fournisseur tente une connexion à distance, l'hôte de rebond présente l'écran de session Active Directory ainsi que le portail d'accès multifactoriel. L'entité pourrait choisir de désactiver le compte Active Directory, de désactiver le compte multifactoriel, ou les deux. L'une ou l'autre de ces méthodes enlève au fournisseur la capacité d'établir une connexion. Le fournisseur en accès distant tentera de se connecter à l'*EACMS*, mais après un échec d'authentification, la tentative de connexion sera interrompue. Ce scénario illustre une méthode permettant d'empêcher les connexions à distance par des fournisseurs tout en éliminant la problématique des demandes récursives (« en cascade »).

Si une entité interdit strictement les connexions distantes commandées par des fournisseurs au moyen d'une politique, l'entité devrait envisager les mesures suivantes pour obtenir une assurance raisonnable de conformité à cette politique, la politique elle-même pouvant devenir la méthode documentée.

1. Documenter si la politique prévoit la possibilité de dérogations en situation d'urgence, la marche à suivre pour évaluer ou approuver ces dérogations, ainsi que les modalités d'interruption d'une connexion distante commandée par un fournisseur en cas de besoin pendant les situations d'urgence en question.

2. Une entité pourrait établir des contrôles internes afin de vérifier périodiquement que les connexions à distance commandées par des fournisseurs sont interdites dans les configurations de système. Quelques exemples, non limitatifs :

a. Utiliser les examens périodiques des accès, prescrits à l'exigence E4 de la norme CIP-004-6 et à l'exigence E5 de la norme CIP-007-6, afin de maintenir une certitude raisonnable que les connexions à distance commandées par des fournisseurs sont interdites selon les modalités prévues.

b. Utiliser les examens périodiques d'inventaire possiblement associés à l'exigence E2 de la norme CIP-002-5.1a pour évaluer les classifications de *systèmes électroniques BES* et les topologies de réseau, afin de produire des documents attestant que les besoins et les configurations de connexions à distance commandées par des fournisseurs ont été revus et confirmés comme étant conformes aux attentes de la politique.

c. Utiliser les examens périodiques de configuration des ensembles de règles ou des listes d'accès qui peuvent être effectués dans le contexte de la norme CIP-005-7 ainsi que la vérification des contrôles en place pour les *points d'accès électroniques*, les *périmètres de sécurité électronique* et la mise en œuvre de *systèmes intermédiaires*, afin d'obtenir une assurance supplémentaire que les connexions à distance commandées par des fournisseurs sont interdites selon les modalités prévues.

d. Utiliser les examens périodiques de gestion des changements de configuration effectués en rapport avec l'exigence E2 de la norme CIP-010-4 pour évaluer les *systèmes électroniques BES* et les changements non prévus (ou potentiellement non autorisés) aux configurations de référence qui pourraient mener à l'ajout de connexions à distance commandées par des fournisseurs, afin d'obtenir une assurance supplémentaire que les connexions à distance commandées par des fournisseurs sont interdites selon les modalités prévues.

e. Utiliser les analyses périodiques de cybervulnérabilité effectuées en rapport avec l'exigence E3 de la norme CIP-010-4 pour évaluer les caractéristiques de connectivité des *systèmes électroniques BES*, leurs interfaces et leurs configurations de protocole, ainsi que les connexions physiques non prévues (ou potentiellement non autorisées), afin d'obtenir une assurance supplémentaire que les connexions à distance commandées par des fournisseurs sont interdites selon les modalités prévues.

f. Utiliser les dispositions dans le programme ou les processus de gestion des accès distants de l'entité responsable détaillant les contrôles internes et la technologie utilisée pour détecter les accès non autorisés afin d'obtenir une assurance supplémentaire que tout ajout de connexions à distance commandées par des fournisseurs pourrait être détecté et annulé en cas de non-conformité avec la politique.

Le recours à du personnel surnuméraire constitue un autre exemple d'accès distant par des fournisseurs ; cette méthode présente toutefois moins de risques que les autres formes d'accès distant par des fournisseurs. En effet, l'entité doit effectuer pour le fournisseur toutes les tâches prescrites à la norme CIP-004 avec la même rigueur que pour un employé (formation, évaluation des risques liés au personnel, etc.) et remettre au fournisseur un dispositif géré par l'entité pour faciliter l'accès distant. L'entité doit gérer ce type d'accès distant par un fournisseur de la même façon que les accès distants de ses employés.

Guide d'application de la norme CIP-005-6

Cette section reproduit certaines portions du texte de la section *Principes directeurs et fondements techniques* de la norme CIP-005-6, à titre de référence historique. Par ailleurs, le texte de cette même section qui donne des indications sur l'intention de l'équipe de rédaction et sur la justification technique est reproduit dans un document intitulé *Justification technique de la norme de fiabilité CIP-005-7*.

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

Exigence E1

Les entités responsables doivent savoir quelles données ont besoin de traverser l'*EAP*, et en justifier les raisons dans un document, afin de s'assurer que l'*EAP* limite les échanges aux communications nécessaires uniquement. Ces communications comprennent, sans s'y limiter, celles qui sont requises dans le cadre de l'exploitation normale, des interventions d'urgence, du soutien, de la maintenance et du dépannage.

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

(...) Il peut s'agir par exemple de modems à fonction de rappel, de modems activés ou mis sous tension à distance et de modems mis sous tension au besoin par le personnel sur place et mis hors tension après utilisation en vertu d'une politique bien établie.

(...) Les technologies qui répondent à cette exigence comprennent notamment les systèmes de détection ou de prévention des intrusions (IDS/IPS) et d'autres formes d'inspection en profondeur des paquets. Ces technologies vont plus loin que les ensembles de règles associant ports, sources et destinations, et constituent par le fait même un autre mécanisme de sécurité distinct mis en œuvre par l'*ESP*.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

VERSION PRÉLIMINAIRE du Guide d'application en attente de la présentation à l'ERO pour approbation

VERSION PRÉLIMINAIRE

Cybersécurité — Gestion des changements de configuration et analyses de vulnérabilité

Guide d'application de la norme de fiabilité CIP-010-4

Octobre 2020

FIABILITÉ | RÉSILIENCE | SÉCURITÉ

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table des matières

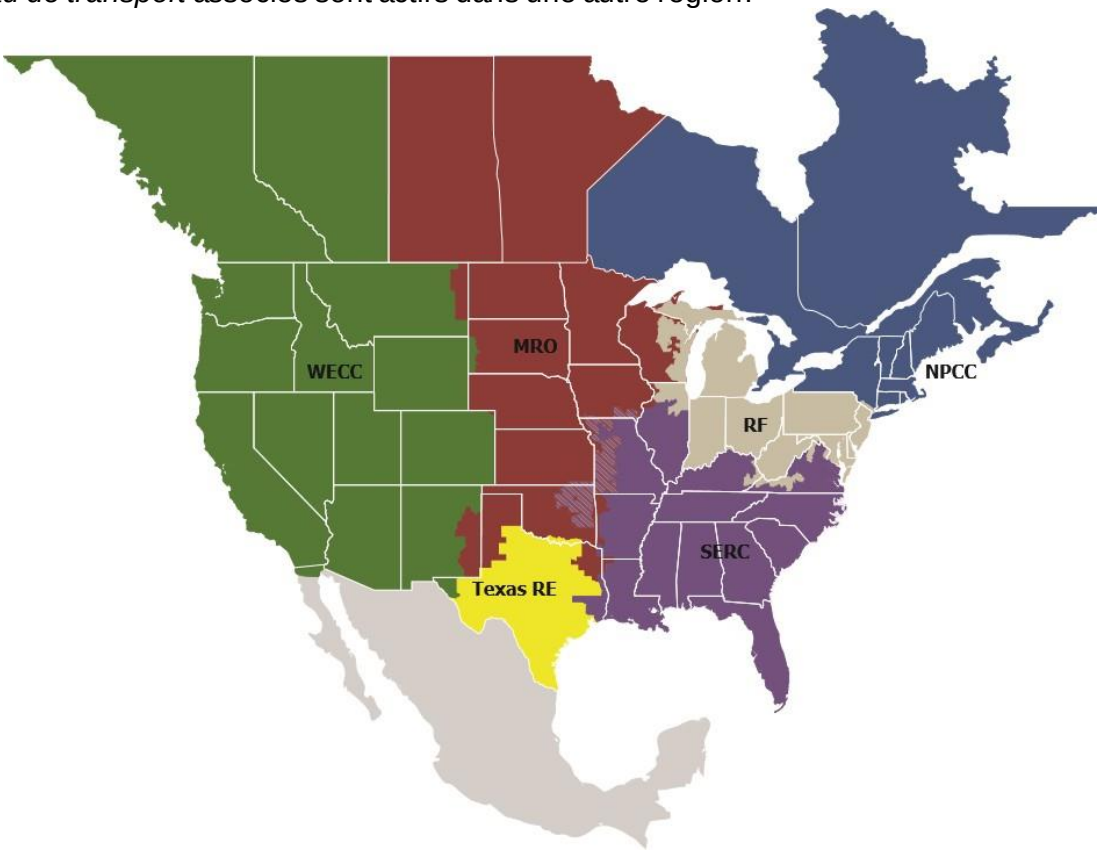
Préface iii
Introduction 5
Exigence E1 0
Remarques générales sur l'exigence E1 0
Guide de mise en œuvre de l'exigence E1 1
Directives d'application de la norme CIP-010-3 3
Section 4 – Portée de l'applicabilité des normes CIP sur la cybersécurité 3
Exigence E1 : 3
Exigence E2 5
Exigence E3 5
Exigence E4 6
Exigence E4, section 1 de l'annexe 1 – *Actifs électroniques temporaires* gérés par l'entité responsable 6
Exigence E4, section 2 de l'annexe 1 – *Actifs électroniques temporaires* gérés par une tierce partie autre que l'entité responsable 9
Exigence E4, section 3 de l'annexe 1 – *Supports de stockage amovibles* 10

Préface

L'électricité est un élément essentiel du tissu de nos sociétés modernes, et l'organisme de fiabilité électrique (ERO) a pour mission de renforcer ce tissu. L'ERO, qui regroupe la North American Electric Reliability Corporation (NERC) et les six entités régionales, veille à maximiser la fiabilité et la sécurité du *système électrique interconnecté* (*BPS*) de l'Amérique du Nord. Nous travaillons en permanence à réduire de manière efficace et efficiente les risques pour la fiabilité et la sécurité du réseau électrique.

Fiabilité | Résilience | Sécurité
Parce que près de 400 millions de citoyens en Amérique du Nord comptent sur nous

Le *système électrique interconnecté* de l'Amérique du Nord est divisé en six territoires d'entités régionales, comme le montrent la carte et le tableau ci-dessous. Les zones combinant deux couleurs indiquent des chevauchements, car certains *responsables de l'approvisionnement* sont actifs dans une région alors que les *propriétaires d'installation de transport* et les *exploitants de réseau de transport* associés sont actifs dans une autre région.



MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst Corporation
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

Introduction

Le présent Guide d'application a pour objet de présenter des exemples de démarches de mise en conformité avec la norme CIP-010-4. Il ne prescrit pas une seule et unique démarche possible, mais met de l'avant diverses manières de réaliser la conformité avec la norme. Il ne s'agit d'ailleurs que d'exemples, et les entités sont donc libres de choisir toute autre démarche plus adaptée à leur situation particulière[1]. Le présent *Guide d'application de la norme de fiabilité CIP-010-4* n'est pas une norme de fiabilité et son contenu ne doit donc pas être considéré comme obligatoire et exécutoire.

Les entités responsables pourront compléter utilement la lecture du présent Guide d'application en consultant l'information présentée par l'équipe de rédaction dans le document de justification technique des modifications de la norme CIP-010-4.

Ce document présente des démarches rédigées par les équipes de rédaction précédentes dans le contexte des versions précédentes de la norme CIP-010, ainsi que les ajouts de l'équipe de rédaction des normes sur les risques de cybersécurité dans la chaîne d'approvisionnement (projet 2019-03) en rapport avec les modifications récentes. Tout élément de texte pertinent à la version 4 de la présente norme et rédigé par les équipes de rédaction précédentes est inclus dans ce document.

Le projet 2019-03 a été entrepris à la suite de l'Ordonnance 850[2] de la Federal Energy Regulatory Commission (FERC) publiée le 18 octobre 2018, dont le sommaire à la page 1 stipule ce qui suit : « …la Commission demande à la NERC d'élaborer et de soumettre des modifications aux normes de fiabilité sur la gestion des risques dans la chaîne d'approvisionnement de manière à étendre la portée de ces normes aux *systèmes de contrôle ou de surveillance des accès électroniques*. » Par ailleurs, dans son rapport du 17 mai 2019 sur les risques de cybersécurité dans la chaîne d'approvisionnement[3], la NERC recommandait de modifier les normes sur la chaîne d'approvisionnement afin d'étendre leur portée aux *systèmes de contrôle des accès physiques* (*PACS*) qui assurent le contrôle des accès physiques à des *systèmes électroniques BES* à impact élevé ou moyen.

L'équipe de rédaction du projet 2019-03 a donc formulé la norme de fiabilité CIP-010-4 de manière à exiger des entités responsables qu'elles respectent les prescriptions de l'Ordonnance 850 de la FERC et du rapport de la NERC sur les risques de cybersécurité dans la chaîne d'approvisionnement.

1. Politique de la NERC relative aux lignes directrices sur la conformité
2. https://www.nerc.com/FilingsOrders/us/FERCOrdersRules/Order%20No.%20850%20Supply%20Chain%20Risk%20Management%20Reliability%20Standards.pdf
3. https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf

Exigence E1

Remarques générales sur l'exigence E1

Les paragraphes 5 et 30 de l'Ordonnance 850 de la FERC demandent de modifier l'exigence E1 de la norme de fiabilité CIP-010-3 de manière à étendre la gestion des risques dans la chaîne d'approvisionnement aux *systèmes de contrôle ou de surveillance des accès électroniques* (*EACMS*) associés aux *systèmes électroniques BES* à impact élevé ou moyen. Par ailleurs, la NERC recommande de modifier les normes sur la chaîne d'approvisionnement afin d'étendre leur portée aux *systèmes de contrôle des accès physiques* (*PACS*) qui assurent le contrôle des accès physiques (à l'exclusion des fonctions d'alarme et de consignation) à des *systèmes électroniques BES* à impact élevé ou moyen ; l'équipe de rédaction des normes du projet 2019-03 a mis en œuvre ces prescriptions.

Remarques générales sur l'alinéa 1.5 de l'exigence E1

Environnement d'essai

L'entité responsable doit prendre note que, lorsqu'il est question d'un environnement d'essai (ou d'un environnement de production dans lequel l'essai est effectué d'une manière qui réduit au minimum les effets dommageables), il s'agit bien de « simuler » la configuration de référence, et non de la reproduire à l'identique.

La formulation relative à l'utilisation d'un environnement d'essai servant à déterminer tout écart par rapport à la configuration de référence a été choisie expressément pour les cas où il serait impossible de dupliquer certains éléments de *système électronique BES* d'un *centre de contrôle* ; par exemple, un modèle ancien de pilote de tableau de visualisation, ou encore les nombreuses liaisons d'échange de données à partir des installations sur le terrain ou vers d'autres *centres de contrôle* (comme les liaisons ICCP).

Remarques générales sur l'alinéa 1.6 de l'exigence E1

Vérification des logiciels

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

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

- les processus de livraison des logiciels et les mesures permettant de vérifier l'identité de la source des logiciels et l'intégrité des logiciels livrés au moyen de ces processus. Dans la mesure où l'entité responsable utilise des systèmes automatisés – par exemple un service par abonnement – pour télécharger et diffuser les logiciels ainsi que leurs mises à jour, envisager d'intégrer à ces processus un mécanisme de vérification des logiciels ;
- la coordination des mesures de vérification des logiciels de l'entité responsable avec d'autres politiques et mesures de cybersécurité, notamment les processus de gestion des changements et des correctifs ainsi que les contrôles d'approvisionnement ;
- le stockage des logiciels dans un dépôt central, après validation de l'identité de la source et de l'intégrité des logiciels, afin d'éviter de devoir répéter ces vérifications avant chaque installation ;
- des mesures supplémentaires comme les exemples décrits à la section SI-7 sur l'intégrité des logiciels, des micrologiciels et de l'information (Software, Firmware, and Information Integrity) de la publication spéciale 800-53 révision 4 du NIST, ou dans d'autres documents d'encadrement semblables ;
- des mesures supplémentaires comme celles décrites dans les normes FIPS 140-2 et FIPS 180-4 ou d'autres documents d'encadrement semblables, visant à ce que les méthodes cryptographiques utilisées soient acceptables par l'entité responsable.

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

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

Même une fois la vérification effectuée, il est recommandé de mettre à l'essai les logiciels. Si les vérifications d'intégrité et d'authenticité sont effectuées uniquement au point d'origine chez le fournisseur, on ne peut pas être certain que le produit obtenu n'a pas été compromis avant qu'il devienne disponible au point d'origine. Les vérifications par le fournisseur ne détectent pas les programmes malveillants introduits dans le logiciel, le micrologiciel ou le correctif entre le contrôle d'intégrité par le fournisseur et la mise en œuvre du logiciel par l'*entité inscrite* dans un *système électronique BES* à impact moyen ou élevé et les *EACMS* ou *PACS* associés.

Guide de mise en œuvre de l'exigence E1

Un document d'encadrement entériné par l'ERO (CIP-010-3 R1.6 Software Integrity and Authenticity) donne des indications supplémentaires sur la mise en conformité, ainsi que des exemples.

Directives d’application de la norme CIP-010-3

Cette section reproduit textuellement des extraits de la section Éclaircissements et commentaires de la norme CIP-010-3, à titre de référence historique. Par ailleurs, des extraits de cette même section qui portent sur l’intention de l’équipe de rédaction et sur la justification technique sont présentés à part dans un document de justification technique pour la présente norme.

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

Néant

Exigence E1 :

Configuration de référence

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

Actif nº 051028 au poste électrique Alpha

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

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

Mécanismes de cybersécurité

Néant

Environnement d’essai

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

Cette formulation a été choisie expressément pour les cas où il serait impossible de dupliquer certains éléments de *système électronique BES* d’un *centre de contrôle* ; par exemple, un modèle ancien de pilote de tableau de visualisation, ou encore les nombreuses liaisons d’échange de données à partir des installations sur le terrain ou vers d’autres *centres de contrôle* (comme les liaisons ICCP).

Vérification des logiciels

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

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

- les processus de livraison des logiciels et les mesures permettant de vérifier l'identité de la source des logiciels et l'intégrité des logiciels livrés au moyen de ces processus. Dans la mesure où l'entité responsable utilise des systèmes automatisés – par exemple un service par abonnement – pour télécharger et diffuser les logiciels ainsi que leurs mises à jour, envisager d'intégrer à ces processus un mécanisme de vérification des logiciels ;
- la coordination des mesures de vérification des logiciels de l'entité responsable avec d'autres politiques et mesures de cybersécurité, notamment les processus de gestion des changements et des correctifs ainsi que les contrôles d'approvisionnement ;
- le stockage des logiciels dans un dépôt central, après validation de l'identité de la source et de l'intégrité des logiciels, afin d'évider de devoir répéter ces vérifications avant chaque installation ;
- des mesures supplémentaires comme les exemples décrits à la section SI-7 sur l'intégrité des logiciels, des micrologiciels et de l'information (*Software, Firmware, and Information Integrity*) de la publication spéciale 800-53 révision 4 du NIST, ou dans d'autres documents d'encadrement semblables ;
- des mesures supplémentaires comme celles décrites dans les normes FIPS 140-2 et FIPS 180-4 ou d'autres documents d'encadrement semblables, visant à ce que les méthodes cryptographiques utilisées soient acceptables par l'entité responsable.

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

- Vérifier que le logiciel porte une signature numérique, et valider cette signature pour s'assurer que l'intégrité du logiciel n'a pas été compromise.
- Utiliser une infrastructure de clés publiques (PKI) avec chiffrement, de façon que seuls les destinataires désignés puissent déchiffrer les logiciels, afin que ceux-ci ne puissent pas être modifiés en cours de transit.
- Demander aux sources de logiciels de fournir des empreintes électroniques ou des codes de hachage pour tous les logiciels, et vérifier ces valeurs avant l'installation dans un système électronique BES afin de confirmer l'intégrité du logiciel. Il est souhaitable de

recevoir les valeurs de vérification au moyen d'une méthode différente de celle utilisée pour recevoir le logiciel à partir de la source de logiciels.

- Utiliser des mécanismes de sécurisation pour la livraison et la diffusion afin de réduire les risques dans la chaîne d'approvisionnement (par exemple, exiger un emballage inviolable pour les logiciels pendant le transport.)

Exigence E2

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

Exigence E3

Dans l'élaboration de ses processus d'analyse de vulnérabilité, l'entité responsable est fortement encouragée à inclure à tout le moins les éléments suivants, dont plusieurs sont mentionnés dans les normes CIP-005 et CIP-007 :

Analyse de vulnérabilité sur papier :

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

Analyse de vulnérabilité active :

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

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

Exigence E4

Exemples non limitatifs de ces dispositifs connectés temporairement :

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

L'entité responsable doit éviter de mettre en place des fonctions de sécurité susceptibles d'affaiblir la fiabilité du réseau en agissant d'une manière qui nuirait au fonctionnement ou au soutien d'*actifs électroniques temporaires*, d'*actifs électroniques BES* ou d'*actifs électroniques protégés*.

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

Par exemple, dans le cas des programmes malveillants, bien des types de dispositifs n'ont pas la capacité de faire fonctionner un logiciel antivirus ; par conséquent, la mise en œuvre d'un logiciel antivirus ne serait pas exigée pour ces dispositifs.

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

Section 1.2 Afin de respecter cet élément de l'exigence, l'entité doit documenter les éléments suivants :

1.2.1 Les utilisateurs (individuellement, par groupe ou par rôle) autorisés à utiliser les *actifs électroniques temporaires*. On peut inscrire à cette fin le nom de la personne, le nom d'un service ou le titre d'un poste. Attention : il faut déterminer si ces utilisateurs doivent aussi avoir un accès électronique autorisé au système pertinent conformément à la norme CIP-004.

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

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

Les entités doivent se montrer prudentes dans l'utilisation d'*actifs électroniques temporaires* et s'assurer que ceux-ci n'ont pas de fonctions activées (par exemple la connectivité sans fil ou

Bluetooth) qui permettraient au dispositif de servir de relais entre un réseau extérieur et un système visé. Dans un tel cas, l'*actif électronique temporaire* deviendrait un *point d'accès électronique* non autorisé, en contravention avec l'exigence E1 de la norme CIP-005.

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

Section 1.3 Les options présentées laissent la porte ouverte à des solutions de rechange (technologies ou processus) qui atténueraient adéquatement le risque lié à ces vulnérabilités.

- L'application de correctifs, avec mises à jour manuelles ou systématiques, offre à l'entité responsable une certaine latitude quant à l'utilisation de ses *actifs électroniques temporaires*. L'entité peut décider de mettre en place pour ses *actifs électroniques temporaires* un processus normalisé d'application de correctifs de sécurité selon un calendrier régulier, ou plutôt d'appliquer les correctifs de sécurité nécessaires à un *actif électronique temporaire* avant de le connecter à un *actif électronique* visé. Contrairement à l'exigence E2 de la norme CIP-007, l'entité n'a pas à élaborer de plans d'atténuation datés ou d'autres documents au-delà de ce qui est nécessaire pour déterminer que l'*actif électronique temporaire* reçoit les correctifs de sécurité appropriés.
- L'utilisation de systèmes d'exploitation et de logiciels exécutables uniquement à partir de supports non inscriptibles permet d'avoir un système d'exploitation protégé qui ne peut être modifié de manière à transmettre des programmes malveillants. Lorsqu'une entité crée un système d'exploitation personnalisé sur support externe, elle doit vérifier l'image pendant sa création afin de s'assurer que l'image ne contient aucun programme malveillant.
- Le renforcement du système d'exploitation consiste à éliminer tous les logiciels et utilitaires non essentiels et à n'installer que le minimum indispensable au fonctionnement de l'ordinateur, ce qui aide à réduire les vulnérabilités. Les programmes supplémentaires peuvent offrir des fonctionnalités utiles, mais ils peuvent aussi receler des « portes dérobées » d'accès au système ; leur élimination a pour effet de renforcer le système.
- Si elle opte pour des moyens autres que ceux qui sont suggérés pour atténuer le risque lié aux vulnérabilités logicielles, l'entité doit établir une documentation qui indique comment ces moyens réalisent l'objectif d'atténuer le risque en question.

Section 1.4 L'entité doit aussi déterminer si la détection du programme malveillant constitue un *incident de cybersécurité.*

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

Section 1.5 La liste d'exemples ci-après présente différentes possibilités suggérées.

- Les restrictions d'accès physique consistent à maintenir l'*actif électronique temporaire* à l'intérieur d'un *périmètre de sécurité physique* ou d'un autre lieu ou enceinte physique dont les accès physiques sont contrôlés afin de protéger l'*actif électronique temporaire*.
- Le cryptage de disque intégral avec authentification est une option qui permet de protéger un *actif électronique temporaire* contre toute utilisation non autorisée ; il est toutefois important qu'une authentification soit exigée avant le décryptage. Par exemple, l'authentification avant le démarrage ou à la mise sous tension sécurise le système d'exploitation en constituant autour de lui une couche d'authentification externe. Les données du disque dur ne peuvent pas être lues tant que l'utilisateur n'a pas confirmé son identité au moyen d'un mot de passe ou d'autres éléments d'authentification. En imposant une authentification avant le décryptage du système et le démarrage, on réduit le risque qu'une personne non autorisée puisse manipuler l'*actif électronique temporaire*.
- L'authentification multifactorielle sert à confirmer l'identité de la personne qui accède au dispositif. L'authentification multifactorielle atténue aussi le risque qu'une personne non autorisée puisse manipuler l'*actif électronique temporaire.*

- Outre les mécanismes d'authentification et de sécurité physique pure, d'autres possibilités existent. Certaines solutions de sécurisation en cas de vol permettent de géolocaliser l'*actif électronique temporaire*, de détecter tout accès, d'effacer le contenu à distance et de verrouiller le système, limitant ainsi la menace potentielle liée à une utilisation non autorisée si l'*actif électronique temporaire* était par la suite connecté à un *actif électronique BES*. D'autres solutions plus rudimentaires peuvent aussi être efficaces pour atténuer le risque lié à l'utilisation d'un *actif électronique temporaire* falsifié, par exemple des étiquettes ou des sceaux d'inviolabilité dont l'intégrité est vérifiée au moyen d'une procédure spéciale avant l'utilisation du dispositif.
- Si elle opte pour des moyens autres que ceux qui sont suggérés pour atténuer le risque lié aux utilisations non autorisées, l'entité doit établir une documentation qui indique comment ces moyens réalisent l'objectif d'atténuer le risque en question.

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

Afin d'assurer un contrôle adéquat, les entités responsables peuvent choisir de conclure des ententes avec des tierces parties pour la prestation de services de soutien des *systèmes électroniques BES* et des *actifs électroniques BES* qui peuvent nécessiter l'utilisation d'*actifs électroniques temporaires*. Les entités pourront juger avantageux d'adopter les clauses normalisées du département de l'Énergie des États-Unis pour les contrats de cybersécurité dans le domaine de la fourniture d'énergie (*Cybersecurity Procurement Language for Energy Delivery Systems*[4], avril 2014). Ces clauses d'approvisionnement peuvent aider à harmoniser les actions de l'entité responsable et des tierces parties chargées du soutien des *systèmes électroniques BES* et des *actifs électroniques BES*. Les attributs du programme de protection des infrastructures essentielles (CIP), y compris les rôles et responsabilités, les contrôles d'accès, la surveillance, la journalisation, la gestion des vulnérabilités et celle des correctifs ainsi que les interventions en cas d'incident et la récupération des sauvegardes, peuvent faire partie des prestations confiées à une tierce partie. Les entités pourront s'inspirer des chapitres General Cybersecurity Procurement Language et The Supplier's Life Cycle Security Program du document précité pour la rédaction des ententes-cadres de services, des contrats et des processus et contrôles du programme CIP.

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

- Procéder à un examen de l'*actif électronique temporaire* géré par une tierce partie autre que l'entité responsable afin de déterminer si la version des correctifs de sécurité du dispositif atténue adéquatement le risque de vulnérabilités logicielles avant la connexion de l'actif *électronique temporaire* à un système visé.
- Procéder à un examen de la procédure d'application de correctifs de la tierce partie. Cet examen peut être fait lors de l'entente contractuelle, ou au plus tard avant de connecter l'*actif électronique temporaire* à un système visé. Tout comme pour l'examen de la version des correctifs de sécurité du dispositif, le choix de ce moyen vise à confirmer que l'entité responsable a atténué le risque lié aux vulnérabilités logicielles pour les systèmes visés.

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

- Procéder à un examen d'autres processus adoptés par la tierce partie pour atténuer le risque lié aux vulnérabilités logicielles, par exemple le renforcement du système d'exploitation, les listes blanches d'applications, les machines virtuelles, etc.
- Si elle opte pour des moyens autres que ceux qui sont suggérés pour atténuer le risque lié aux vulnérabilités logicielles, l'entité doit établir une documentation qui indique comment ces moyens réalisent l'objectif d'atténuer le risque en question.

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

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

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

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

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

L'entité doit aussi déterminer si la détection du programme malveillant constitue un *incident de cybersécurité.*

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

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

VERSION PRÉLIMINAIRE

Plans de gestion des risques de cybersécurité dans la chaîne d'approvisionnement

Guide d'application de la norme de fiabilité CIP-013-2

Octobre 2020

FIABILITÉ | RÉSILIENCE | SÉCURITÉ

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table des matières

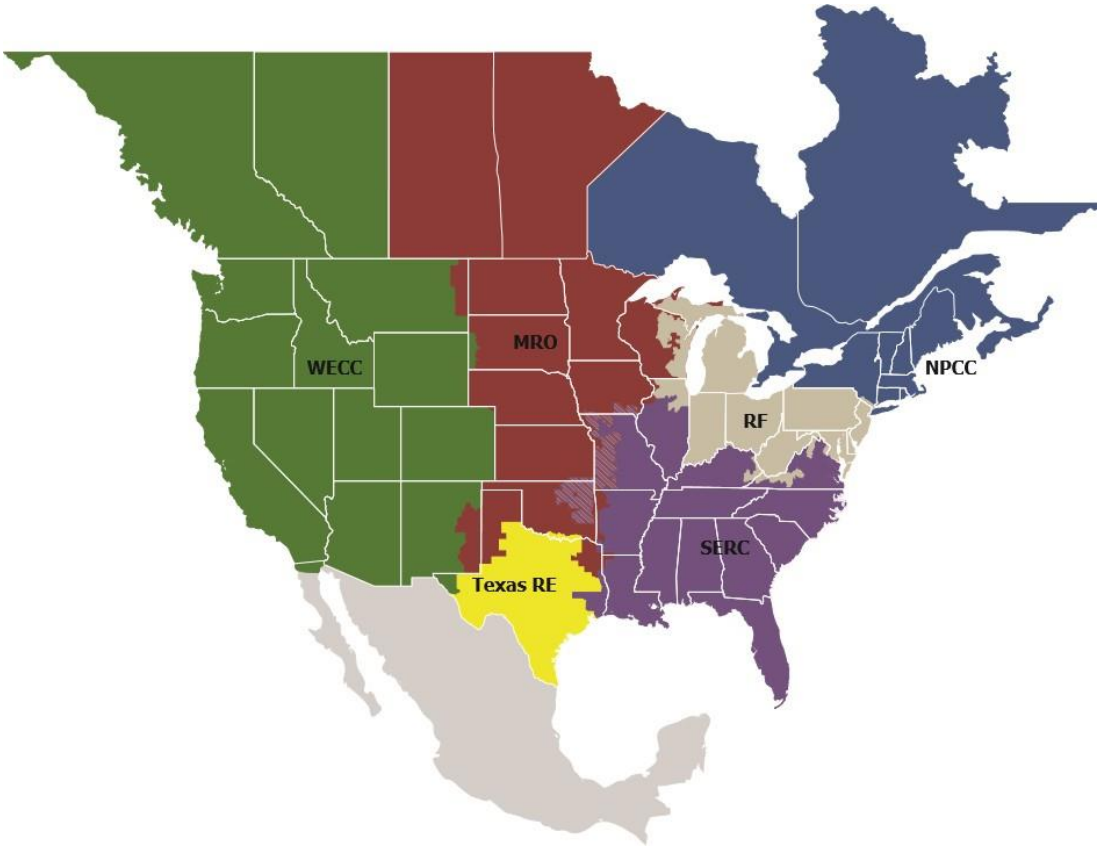
Préface.....
Introduction i
Exigence E1 1
Remarques générales sur l'exigence E1 1
Guide d'application pour l'exigence E1 2
Exigence E2 10
Remarques générales sur l'exigence E2 10
Exigence E3 11
Remarques générales sur l'exigence E3 11
Guide d'application pour l'exigence E3 11
Références.....12

Préface

L'électricité est un élément essentiel du tissu de nos sociétés modernes, et l'organisme de fiabilité électrique (ERO) a pour mission de renforcer ce tissu. L'ERO, qui regroupe la North American Electric Reliability Corporation (NERC) et les six entités régionales, veille à maximiser la fiabilité et la sécurité du *système électrique interconnecté* (*BPS*) de l'Amérique du Nord. Nous travaillons en permanence à réduire de manière efficace et efficiente les risques pour la fiabilité et la sécurité du réseau électrique.

Fiabilité | Résilience | Sécurité
Parce que près de 400 millions de citoyens en Amérique du Nord comptent sur nous

Le *système électrique interconnecté* de l'Amérique du Nord est divisé en six territoires d'entités régionales, comme le montrent la carte et le tableau ci-dessous. Les zones combinant deux couleurs indiquent des chevauchements, car certains *responsables de l'approvisionnement* sont actifs dans une région alors que les *propriétaires d'installation de transport* et les *exploitants de réseau de transport* associés sont actifs dans une autre région.



MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst Corporation
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

Introduction

Le 21 juillet 2016, la Federal Energy Regulatory Commission (FERC) publiait l'Ordonnance 829 dans laquelle elle demandait à la North American Electric Reliability Corporation (NERC) de créer ou de modifier une norme de fiabilité portant sur la gestion des risques de cybersécurité dans la chaîne d'approvisionnement pour les équipements, les logiciels et les services informatiques et de réseau des systèmes de commande industrielle associés à l'exploitation du *système de production-transport d'électricité* (*BES*), en stipulant ce qui suit :

> [La Commission demande à] la NERC d'élaborer une norme de fiabilité prospective et axée sur des objectifs, qui exige que chaque entité visée établisse et mette en œuvre un plan pour l'intégration de mécanismes de sécurité dans la chaîne d'approvisionnement pour les équipements, les logiciels et les services informatiques et de réseau des systèmes de commande industrielle associés à l'exploitation du système de production-transport d'électricité. La norme de fiabilité ainsi créée ou modifiée doit répondre aux objectifs de sécurité suivants [décrits en détail dans l'Ordonnance] : 1) l'intégrité et l'authenticité des logiciels ; 2) l'accès distant par les fournisseurs ; 3) la planification des systèmes d'information ; et 4) la gestion des risques liés aux fournisseurs et les contrôles d'approvisionnement.

Le 18 octobre 2018, la Federal Energy Regulatory Commission (FERC) publiait l'Ordonnance 850 dans laquelle elle approuvait les normes de fiabilité CIP-013-1 (*Cybersécurité – Gestion des risques dans la chaîne d'approvisionnement*), CIP-005-6 (*Cybersécurité – Périmètres de sécurité électronique*) et CIP-010-3 (*Cybersécurité — Gestion des changements de configuration et analyses de vulnérabilité*), portant sur la gestion des risques dans la chaîne d'approvisionnement et soumises par la North American Electric Reliability Corporation (NERC). Dans cette même ordonnance, la FERC demandait à la NERC d'étendre la portée de ces normes aux *systèmes de contrôle ou de surveillance des accès électroniques* (*EACMS*).

Le 17 mai 2019, la NERC publiait un rapport sur les risques de cybersécurité dans la chaîne d'approvisionnement dans lequel elle recommandait d'étendre la portée des normes précitées aux *systèmes de contrôle des accès physiques* (*PACS*).

La norme de fiabilité **CIP-013-2, *Cybersécurité – Gestion des risques dans la chaîne d'approvisionnement*,** porte sur les risques de cybersécurité pertinents dans la chaîne d'approvisionnement, pendant les phases de planification, d'acquisition et de déploiement, pour les *systèmes électroniques BES* à impact moyen ou élevé[1] ainsi que pour les *EACMS* et les *PACS* associés.

Le présent Guide d'application donne des indications sur la mise en œuvre des exigences de la norme CIP-013-2 et présente des exemples de démarches que les entités responsables pourraient adopter pour répondre à ces exigences. Ces exemples de mise en conformité avec la norme CIP-013-2 ne sont nullement limitatifs ; les entités responsables sont libres de choisir toute autre démarche plus adaptée à leur situation particulière.

1. Les entités responsables dressent la liste des *systèmes électroniques BES* à impact moyen ou élevé, ainsi que des *EACMS* et des *PACS* associés, conformément au processus de désignation et de catégorisation prescrit à la norme CIP-002-5, ou toute version ultérieure de celle-ci.

Exigence E1

E1. Chaque entité responsable doit établir un ou des plans documentés de gestion des risques de cybersécurité dans la chaîne d'approvisionnement pour les *systèmes électroniques BES* à impact moyen ou élevé ainsi que les *systèmes de contrôle ou de surveillance des accès électroniques* (*EACMS*) et les *systèmes de contrôle des accès physiques* (*PACS*) associés. Ce ou ces plans doivent comprendre les éléments suivants :

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

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

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

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

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

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

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

1.2.6. la coordination des contrôles visant les accès distants commandés par un fournisseur.

Remarques générales sur l'exigence E1

Voici quelques remarques générales à l'intention des entités responsables qui doivent mettre en œuvre l'exigence E1.

D'abord, lorsqu'elles élaborent leurs plans de gestion des risques de cybersécurité dans la chaîne d'approvisionnement, les entités responsables doivent chercher à s'appuyer sur les divers éléments et phases du processus d'acquisition (exigences préétablies, appel d'offres, évaluation des soumissions, outils et données externes d'évaluation de fournisseurs, certifications et rapports d'audit de tiers, etc.) afin de se donner les moyens de réaliser l'objectif de l'exigence E1, notamment une flexibilité adéquate pour négocier les contrats avec les fournisseurs de manière à atténuer efficacement les risques. Le fait de miser uniquement sur des modalités contractuelles rigides pourrait avoir des conséquences imprévues, notamment une forte augmentation des coûts pour le produit ou le service, ou encore le refus de fournisseurs de signer le contrat.

En outre, l'entité responsable n'a pas nécessairement la capacité de faire inscrire chacun des mécanismes de cybersécurité souhaités dans son contrat avec chacun de ses fournisseurs. Des facteurs comme la concurrence, des sources d'approvisionnement limitées, les coûts, la criticité du produit ou du service et le degré de maturité du fournisseur ou de la gamme de produits pourraient influer sur les modalités finalement négociées par les parties et incluses dans le contrat. Cette variabilité des modalités contractuelles est anticipée, et c'est pourquoi la remarque de l'exigence E2 précise que les modalités exactes du contrat ne sont pas visées par la norme de fiabilité CIP-013-2.

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

L'exigence E1 met l'accent sur les mesures prises par l'entité responsable pour gérer les risques de cybersécurité associés aux produits ou services des fournisseurs pendant la planification et l'acquisition des *systèmes électroniques BES*. Dans le cas où un fournisseur se montrerait réticent à négocier des mécanismes de cybersécurité, l'entité responsable pourrait explorer d'autres sources d'approvisionnement ou divers mécanismes d'atténuation afin de réduire le risque pour les *systèmes électroniques BES*, selon ce que permet la situation de l'entité responsable.

Dans l'établissement et la mise en œuvre de son plan de gestion des risques de cybersécurité dans la chaîne d'approvisionnement, l'entité responsable peut juger bon de définir et de prioriser certains mécanismes de sécurité en fonction des risques de cybersécurité présentés par le fournisseur et selon la criticité du produit ou service pour la fiabilité de l'exploitation. Par exemple, l'entité responsable pourrait établir, pour certains produits ou services, une liste de base de mécanismes essentiels qu'un fournisseur doit avoir pour être admissible (critère éliminatoire). Comme les risques varient entre différents produits et services, cette liste de base peut varier pour les différents produits et services achetés par l'entité responsable pour ses *systèmes électroniques BES*. Cette démarche axée sur les risques pourrait favoriser l'efficience dans le processus d'acquisition de l'entité responsable, tout en réalisant les objectifs de sécurité de l'exigence E1.

L'exigence concernant la vérification de l'intégrité et de l'authenticité des logiciels, applicable à la phase d'acquisition des *systèmes électroniques BES* (sous-alinéa 1.2.5), a pour objectif de confirmer la capacité du fournisseur de faire en sorte que les logiciels installés dans les *systèmes électroniques BES* soient dignes de confiance. Le sous-alinéa 1.2.5 n'est pas une exigence opérationnelle qui demande à l'entité responsable d'assurer elle-même la vérification ; il s'agit plutôt de déterminer, pendant la phase d'acquisition, la capacité du fournisseur de donner une assurance quant à l'intégrité et à l'authenticité des logiciels, et d'établir la performance du fournisseur selon cette capacité, afin de mettre en œuvre l'alinéa 1.6 de l'exigence E1 de la norme CIP-010-4.

Guide d'application pour l'exigence E1

Les entités responsables utilisent divers processus dans leurs activités d'acquisition des *systèmes électroniques BES*. Quelques exemples de démarches visant à répondre à cette exigence sont présentés ci-après.

E1. Chaque entité responsable doit établir un ou des plans documentés de gestion des risques de cybersécurité dans la chaîne d'approvisionnement pour les *systèmes électroniques BES*

à impact moyen ou élevé ainsi que les *systèmes de contrôle ou de surveillance des accès électroniques* (*EACMS*) et les *systèmes de contrôle des accès physiques* (*PACS*) associés. Ce ou ces plans doivent comprendre les éléments suivants :

- L'entité responsable pourrait créer un ou plusieurs documents expliquant le processus qu'elle a adopté pour la gestion des risques de cybersécurité dans la chaîne d'approvisionnement pour les *systèmes électroniques BES* à impact moyen ou élevé ainsi que pour les *EACMS* et *PACS* associés. Afin de se donner la flexibilité voulue pour la gestion des risques de cybersécurité dans la chaîne d'approvisionnement, l'entité responsable peut adopter une démarche « axée sur les risques ». Cette démarche peut être « orientée système », c'est-à-dire centrée sur des mesures spécifiques aux *systèmes électroniques BES* à impact moyen ou élevé ainsi qu'aux *EACMS* et aux *PACS* associés afin de gérer les risques inhérents à l'acquisition de ces systèmes ou des services afférents. Cette démarche peut aussi être « orientée fournisseur », c'est-à-dire centrée sur les risques posés par divers fournisseurs de *systèmes électroniques BES*. Il est également possible pour l'entité de combiner ces deux orientations dans ses plans. Cette flexibilité est importante pour tenir compte « des différences dans les besoins et les caractéristiques des entités responsables ainsi que de la diversité des environnements, des technologies et des risques des *systèmes électroniques BES* » (Ordonnance 829 de la FERC, paragraphe 44).

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

Une entité responsable pourrait documenter dans son plan de gestion des risques de cybersécurité dans la chaîne d'approvisionnement un ou plusieurs processus qu'elle utilisera dans sa planification de l'acquisition de *systèmes électroniques BES* afin de déceler et d'évaluer les risques de cybersécurité pour le *système de production-transport d'électricité* posés par les produits ou services des fournisseurs conformément à l'exigence. Des exemples de processus, ou de résultats de ces processus, permettant de réaliser la conformité à l'alinéa 1.1 sont présentés ci-après. Une entité responsable pourrait satisfaire à l'alinéa 1.1 en adoptant la première démarche (examen par une équipe), la seconde démarche (processus d'évaluation des risques), une combinaison des deux, ou encore une autre démarche établie par l'entité responsable pour satisfaire à l'alinéa 1.1.

- L'entité responsable peut établir un processus consistant à former une équipe d'experts techniques choisis dans l'ensemble de l'organisation pour participer aux processus de planification et d'acquisition des *systèmes électroniques BES*. L'entité responsable devrait tenir compte des expertises pertinentes nécessaires pour réaliser l'objectif de l'alinéa 1.1 et faire en sorte que l'équipe représente les secteurs appropriés (activités commerciales, architecture de sécurité, technologies de l'information et des communications, chaîne d'approvisionnement, conformité réglementaire et affaires juridiques). Voici quelques exemples de facteurs que cette équipe pourrait intégrer dans la planification de l'acquisition de *systèmes électroniques BES* pour satisfaire à l'alinéa 1.1 :
  - risques de cybersécurité pour le *BES* qui pourraient être introduits par un fournisseur dans un nouveau *système électronique BES* ou lors de modifications planifiées à un *système électronique BES* ;
  - processus de sécurité des fournisseurs et procédures connexes, notamment l'architecture de système, les processus de contrôle des changements, les exigences en matière d'accès distant et les processus de notifications de sécurité ;

- processus d'examen périodiques applicables à des fournisseurs critiques pour évaluer tout changement dans les mécanismes de sécurité du fournisseur, sa gestion du cycle de vie des produits et sa chaîne d'approvisionnement, ainsi qu'une méthode de recherche des occasions d'amélioration continue ;
- recours chez les fournisseurs à des évaluations par des tiers (par exemple, des certifications de produits ou de travailleurs) ou indépendantes pour vérifier les pratiques de sécurité entourant les produits et services ;
- évaluations de sécurité ou essais d'intrusion par des tiers offerts par les fournisseurs ;
- canaux de chaîne d'approvisionnement du fournisseur et plans visant à atténuer les risques potentiels ou les perturbations ;
- vulnérabilités connues des systèmes d'information, composants ou services de système d'information du fournisseur ainsi que les techniques, tactiques et procédures de menace connues qui pourraient être introduites, et les mesures d'atténuation connexes ;
- processus de gouvernance d'entreprise et d'approbation ;
- méthodes permettant de réduire au minimum l'exposition du réseau, par exemple le blocage de l'accès à Internet, l'utilisation de pare-feu et l'application de techniques d'accès distant sécurisé ;
- méthodes permettant de limiter ou de contrôler les accès distants par les fournisseurs aux *systèmes électroniques BES* de l'entité responsable ;
- évaluations des risques de cybersécurité par le fournisseur pendant le processus de planification et d'approvisionnement, et les mesures d'atténuation associées ;
- mécanismes d'atténuation qui peuvent être mis en œuvre par l'entité responsable ou le fournisseur (renforcer le système d'information, réduire au minimum la surface d'attaque, assurer un soutien permanent pour les composants de système, prévoir des sources de substitution pour des composants critiques, etc.).

- L'entité responsable peut élaborer un processus d'évaluation des risques afin de déceler et d'évaluer les risques de cybersécurité potentiels résultant i) de l'acquisition et de l'installation d'équipements et de logiciels de fournisseurs, et ii) d'une transition entre fournisseurs. Ce processus pourrait tenir compte des points suivants :
  - risques potentiels liés aux systèmes d'information, aux composants de système ou aux services ou intégrateurs de systèmes d'information du fournisseur. Exemples :
    - systèmes, composants ou services critiques qui influent sur l'exploitation ou sur la fiabilité des *systèmes électroniques BES* ;
    - composants de produits qui ne sont pas détenus et contrôlés par le fournisseur et qui peuvent introduire des risques supplémentaires, comme du code source libre ou des composants de développeurs ou de fabricants tiers ;
  - risques potentiels liés aux contrôles de gestion des risques du fournisseur. Exemples de contrôles de gestion des risques du fournisseur à considérer[2] :
    - pratiques de vérification des antécédents et de criblage du personnel par les fournisseurs ;

2. Des outils comme le questionnaire normalisé de collecte de renseignements SIG (Standardized Information Gathering) de Shared Assessments peut aider à évaluer les risques du fournisseur.

- programmes de formation et évaluations du personnel du fournisseur en matière de cybersécurité ;
- programmes formels de sécurité du fournisseur, y compris les pratiques techniques, organisationnelles et de gestion de la sécurité ;
- contrôles des accès physiques et de cybersécurité du fournisseur visant à protéger les installations et le cycle de vie des produits ;
- principes d'ingénierie de sécurité mis en œuvre par le fournisseur pour i) créer des protections par couches ; ii) établir des politiques, architectures et contrôles de sécurité solides comme fondement du travail de conception ; iii) intégrer les exigences de sécurité au cycle de développement de systèmes ; iv) définir des périmètres de sécurité physique et logique ; v) veiller à ce que les développeurs de système soient formés à la conception des logiciels de sécurité ; vi) adapter les mécanismes de sécurité aux besoins organisationnels et opérationnels ; vii) procéder à la modélisation des menaces afin de définir des cas d'utilisation, des agents de menace, des vecteurs d'attaque et des schémas d'attaque ainsi que des mesures compensatoires et des schémas de conception permettant d'atténuer les risques ; et viii) réduire les risques à des niveaux acceptables, de manière à favoriser une prise de décision éclairée en gestion des risques (source : NIST SP-800-53, SA-8 – *Security Engineering Principles*) ;
- méthodologie SDLC de cycle de développement de système, à partir de la conception jusqu'à la gestion des correctifs, permettant de comprendre comment la cybersécurité est intégrée dans tous les processus du fournisseur ;
- certifications des fournisseurs et leur concordance avec les normes de l'industrie et réglementaires reconnues ;
- résumé de tout essai de cybersécurité interne ou indépendant portant sur les produits du fournisseur afin d'assurer un fonctionnement sûr et fiable[3] ;
- stratégie produit du fournisseur décrivant le soutien après-vente du fournisseur (correctifs logiciels, mises à jour de micrologiciel, pièces de rechange et soutien continu de la maintenance) ;
- déterminer les processus et les mesures de contrôle assurant la gestion continue de la propriété intellectuelle et des responsabilités de l'entité responsable et du fournisseur, s'il y a lieu (par exemple, l'utilisation d'algorithmes de chiffrement pour sécuriser le code source, les données et l'information des logiciels, les conceptions et les processus exclusifs, sur place ou en transit).

▪ À partir de l'évaluation des risques, déterminer les mécanismes d'atténuation qui peuvent être mis en œuvre par l'entité responsable ou le fournisseur. Exemples : renforcer le système d'information, réduire au minimum la surface d'attaque, assurer un soutien permanent pour les composants de système, prévoir des sources de substitution pour des composants critiques, etc.

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

L'entité responsable pourrait documenter dans son plan de gestion des risques de cybersécurité dans la chaîne d'approvisionnement un ou plusieurs processus qu'il compte utiliser dans son processus

3. Par exemple, l'entité responsable peut demander au fournisseur de présenter un rapport d'audit SSAE (Statement on Standards for Attestation Engagements) 18 SOC 2.

d'acquisition de *systèmes électroniques BES* afin de satisfaire aux sous-alinéas 1.2.1 à 1.2.6. Ci-après quelques exemples de processus, ou de résultats de ces processus, qui permettent de satisfaire à l'alinéa 1.2.

- Demander l'inclusion dans le processus d'acquisition de *systèmes électroniques BES* (à l'étape de l'appel d'offres ou de la négociation contractuelle) de modalités concernant la cybersécurité en rapport avec les sous-alinéas 1.2.1 à 1.2.6, de sorte que les fournisseurs comprennent les attentes en matière de cybersécurité quant à la mise en œuvre de mécanismes de sécurité appropriés tout au long du cycle de vie du produit : conception, développement, essais, fabrication, livraison, installation, soutien technique et mise au rebut finale[4].
- Pendant la négociation de contrats ou de processus d'acquisition avec les fournisseurs, l'entité responsable peut documenter la justification, les mécanismes d'atténuation ou l'acceptation des dérogations aux clauses d'approvisionnement normalisées sur la cybersécurité de l'entité responsable qui s'appliquent aux composants de système, aux intégrateurs de systèmes ou aux fournisseurs de services externes du fournisseur.

Des exemples de manières dont l'entité responsable pourrait, dans le cadre des processus d'acquisition de *systèmes électroniques BES* mentionnés à l'alinéa 1.2, satisfaire aux sous-alinéas 1.2.1 à 1.2.6, sont présentés ci-après.

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

- À l'étape de l'appel d'offres ou de la négociation contractuelle, demander que soit incorporée dans les modalités contractuelles une obligation pour le fournisseur de transmettre des notifications de toute brèche constatée, menace de brèche ou tentative de brèche touchant des composants, des logiciels ou des systèmes du fournisseur (« événement de sécurité ») quant aux conséquences possibles sur la disponibilité ou la fiabilité de *systèmes électroniques BES*. Les notifications d'événement de sécurité destinées à l'entité responsable devront être envoyées à un point de contact désigné par l'entité responsable et le fournisseur. Exemples d'information à demander au fournisseur d'inclure dans les notifications à l'entité responsable : i) les mécanismes d'atténuation que l'entité responsable peut mettre en place, s'il y a lieu, et ii) la disponibilité de correctifs ou de composants corrigés, s'il y a lieu.

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

- L'entité responsable et le fournisseur peuvent convenir d'ententes de niveau de service portant sur la réponse à des incidents de cybersécurité et sur un engagement du fournisseur à collaborer avec l'entité responsable pour mettre en place des mécanismes d'atténuation et les correctifs de produit.
- À l'étape de l'appel d'offres ou de la négociation contractuelle, demander que soit incorporé dans les modalités contractuelles un engagement du fournisseur selon lequel,

4. À titre d'exemple, le document *Cybersecurity Procurement Language for Energy Delivery Systems* publié par l'Energy Sector Control Systems Working Group (ESCSWG) présente des clauses types en matière de cybersécurité dans la chaîne d'approvisionnement, utilisables par les propriétaires, les exploitants et les fournisseurs du *BES* dans le cadre de leur processus d'acquisition.

dans le cas où celui-ci constaterait une vulnérabilité ayant entraîné un incident de cybersécurité touchant des produits ou services fournis à l'entité responsable, le fournisseur devra transmettre une notification à l'entité responsable. Le contrat pourrait stipuler que le fournisseur doit fournir une information prédéfinie sur les produits ou services à risque et sur les précautions appropriées pour réduire au minimum les risques. Tant que l'incident de cybersécurité n'aura pas été corrigé, il pourrait être demandé au fournisseur de faire une analyse de l'information disponible ou qu'il est possible d'obtenir, de présenter un plan d'action, de transmettre des rapports d'étape réguliers, d'indiquer des mécanismes d'atténuation et d'aboutir à une résolution finale dans des délais raisonnables convenus par le fournisseur et l'entité responsable.

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

- À l'étape de l'appel d'offres ou de la négociation contractuelle, demander que soit incorporée dans les modalités contractuelles une obligation pour le fournisseur de transmettre une notification à l'entité responsable lorsqu'il n'y a plus lieu d'autoriser un accès distant ou local à un employé du fournisseur. Une telle notification ne doit pas obliger le fournisseur à divulguer des informations sensibles sur l'employé. Les circonstances dans lesquelles il n'y a plus lieu d'autoriser un accès distant ou local à un employé du fournisseur sont notamment les suivantes : i) le fournisseur détermine que l'employé en question n'a plus besoin de cet accès, ii) l'employé en question n'a plus les qualifications justifiant le maintien de cet accès, ou iii) l'employé en question cesse d'être à l'emploi du fournisseur pour une raison quelconque. Demander au fournisseur de s'engager à transmettre la notification dans un délai prénégocié suivant le constat du changement. Le fournisseur et l'entité responsable devraient définir des méthodes de substitution à mettre en œuvre afin de maintenir la continuité des opérations ou des services selon les besoins.
- Si un fournisseur utilise un tiers (ou un sous-traitant) pour fournir des services à l'entité responsable, exiger que le fournisseur obtienne l'approbation préalable de l'entité responsable et exiger que le tiers respecte les exigences de notification de fin d'accès imposées directement au fournisseur.

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

- À l'étape de l'appel d'offres ou de la négociation contractuelle, demander que soit incorporé dans les modalités contractuelles un engagement du fournisseur à collaborer pour donner accès à une documentation sommaire, dans un délai prénégocié, en cas de découverte d'une brèche de sécurité concernant le produit livré ou sa chaîne d'approvisionnement et pouvant avoir un impact sur la disponibilité ou la fiabilité du *système électronique BES* de l'entité responsable. Cette documentation devrait comprendre une description sommaire de la brèche et indiquer son impact potentiel sur la sécurité, sa cause première et les actions correctives recommandées relativement au produit livré.
- À l'étape de l'appel d'offres ou de la négociation contractuelle, demander que soit incorporé dans les modalités contractuelles un engagement du fournisseur à collaborer pour donner accès dans un délai prénégocié, après signature d'une entente de confidentialité appropriée, à une documentation sommaire sur les vulnérabilités de sécurité non corrigées dans le produit livré et qui n'ont pas été divulguées publiquement. Cette documentation devrait comprendre une description sommaire de chaque vulnérabilité et indiquer son impact potentiel, sa cause première ainsi que des

mécanismes de sécurité compensatoires, des mesures d'atténuation ou des contournements procéduraux recommandés.

- Au cours du processus d'acquisition, passer en revue avec le fournisseur la documentation sommaire sur les vulnérabilités du produit livré divulguées publiquement ainsi que l'état du traitement par le fournisseur de ces vulnérabilités.

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

- Au cours du processus d'acquisition, demander de consulter la documentation du fournisseur décrivant le programme de gestion des correctifs du fournisseur et le processus de mise à jour de tous les composants de système livrés (y compris le matériel, les logiciels et les micrologiciels de tiers fournisseurs). Cette documentation devrait décrire la méthode ou la recommandation du fournisseur quant à la vérification de l'intégrité des correctifs par l'entité responsable. Demander au fournisseur de décrire les processus qu'il utilise pour livrer les logiciels et les méthodes utilisables pour vérifier l'intégrité et l'authenticité des logiciels après réception, y compris pour les systèmes avec logiciels préinstallés.
- À l'étape de l'appel d'offres ou de la négociation contractuelle, demander que soit incorporé dans les modalités contractuelles un engagement du fournisseur à donner accès à la documentation du fournisseur sur les produits livrés (y compris le matériel, les logiciels, les micrologiciels et les services de tiers fournisseurs) concernant le calendrier des versions et la disponibilité des mises à jour et des correctifs à considérer ou à appliquer. Cette documentation devrait comprendre des instructions décrivant comment appliquer, valider et tester de façon sécuritaire les mises à jour et les correctifs.
- À l'étape de l'appel d'offres ou de la négociation contractuelle, demander que soit incorporé dans les modalités contractuelles un engagement du fournisseur à livrer, dans un délai raisonnable, des mises à jour appropriées de logiciels et de micrologiciels pour remédier à des vulnérabilités ou à des faiblesses nouvellement découvertes, pendant toute la durée du cycle de vie du produit. Les ententes de niveau de service pour les mises à jour et les correctifs visant à remédier à des vulnérabilités critiques devraient spécifier des délais plus courts que pour les autres mises à jour. Si le fournisseur ne peut pas livrer des mises à jour dans un délai raisonnable, il doit être tenu de proposer des mesures d'atténuation ou de contournement.
- À l'étape de l'appel d'offres ou de la négociation contractuelle, demander que soit incorporé dans les modalités contractuelles un engagement du fournisseur à produire des empreintes électroniques ou des codes de hachage pour tous les logiciels, de telle sorte que l'entité responsable puisse vérifier ces valeurs avant l'installation dans le *système électronique BES* afin de confirmer l'intégrité des logiciels.
- À l'étape de l'appel d'offres ou de la négociation contractuelle, demander que soit incorporé dans les modalités contractuelles un engagement du fournisseur à ce que, s'il livre des composants logiciels de tiers, il soit en mesure de fournir des mises à jour et des correctifs appropriés pour remédier à des vulnérabilités ou à des faiblesses nouvellement découvertes dans les composants logiciels de tiers.

1.2.6. la coordination des contrôles visant les accès distants commandés par un fournisseur.

- Pendant le processus d'acquisition, demander aux fournisseurs de spécifier les adresses IP, les ports et les privilèges minimaux requis pour utiliser les services d'accès distant.

- Demander aux fournisseurs d'utiliser des comptes d'utilisateur individuels qu'il est possible de configurer de manière à limiter l'accès et les permissions.
- À l'étape de l'appel d'offres ou de la négociation contractuelle, demander que soit incorporé dans les modalités contractuelles un engagement du fournisseur à assurer la bonne maintenance de ses actifs informatiques (matériel, logiciels et micrologiciels) qui doivent se connecter au réseau de l'entité responsable, en y appliquant les plus récentes mises à jour afin de remédier à des vulnérabilités de sécurité ou à des faiblesses signalées par le fournisseur d'origine ou par l'entité responsable.
- Au cours du processus d'acquisition, demander aux fournisseurs de documenter leurs processus visant à empêcher les connexions par des personnes non autorisées. Il doit être interdit au personnel du fournisseur de divulguer des éléments d'authentification, des mots de passe ou des connexions établies.
- À l'étape de l'appel d'offres ou de la négociation contractuelle, demander que soit incorporé dans les modalités contractuelles un engagement du fournisseur à ce que, pour les connexions de système à système du fournisseur pouvant limiter la capacité de l'entité responsable de valider les accès du personnel à partir des systèmes du fournisseur, le fournisseur tienne un registre complet et exact des accès par les utilisateurs, des données d'authentification et d'autres informations pertinentes aux activités d'accès par connexion, pendant une période prénégociée.

Exigence E2

E2. Chaque entité responsable doit mettre en œuvre le ou les plans de gestion des risques de cybersécurité dans la chaîne d'approvisionnement prescrits à l'exigence E1.

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

Remarques générales sur l'exigence E2

La mise en œuvre d'un plan de gestion des risques de cybersécurité n'oblige pas l'entité responsable à renégocier ou à résilier des contrats existants (y compris les modifications aux ententes-cadres ou les bons de commande), comme le précise le paragraphe 36 de l'Ordonnance 829. La norme CIP-013-2 s'applique aux contrats qui entrent dans le processus d'acquisition de l'entité responsable (par exemple, par appel d'offres) à compter de la date d'entrée en vigueur de la norme. La date d'entrée en vigueur du contrat ou toute autre date d'effet stipulée dans le contrat ne détermine pas si le contrat est visé par la norme CIP-013-2.

Exigence E3

E3. Chaque entité responsable doit réexaminer et faire approuver par le *cadre supérieur CIP* ou son délégataire, au moins une fois tous les 15 mois civils, le ou les plans de gestion des risques de cybersécurité dans la chaîne d'approvisionnement prescrits à l'exigence E1.

Remarques générales sur l'exigence E3

Dans l'examen prescrit à l'exigence E3, les entités responsables doivent tenir compte des nouveaux risques ainsi que des mesures d'atténuation disponibles, selon diverses sources comme la NERC et le département de la Sécurité intérieure (DHS) des États-Unis, entre autres.

Guide d'application pour l'exigence E3

Les entités responsables utilisent divers processus pour satisfaire à cette exigence. Ci-après quelques exemples de telles démarches.

- Une équipe d'experts techniques de tous les secteurs de l'organisation (activités commerciales, architecture de sécurité, technologies de l'information et des communications, chaîne d'approvisionnement, conformité réglementaire, affaires juridiques, etc.) analyse le plan de gestion des risques de cybersécurité dans la chaîne d'approvisionnement au moins une fois tous les 15 mois civils afin de déterminer s'il y a lieu d'y apporter des changements. Les sources d'information utilisables à cette fin comprennent, sans limitation :
  - les exigences ou directives des organismes de réglementation ;
  - les pratiques exemplaires et lignes directrices de l'industrie visant à améliorer les mesures de gestion des risques de cybersécurité dans la chaîne d'approvisionnement, telles que formulées par des organisations comme la NERC, le département de l'Énergie (DOE), le département de la Sécurité intérieure (DHS), l'ICS-CERT, le Centre canadien pour la cybersécurité (CCC, anciennement Centre canadien de réponse aux incidents cybernétiques) et le National Institute of Standards and Technology (NIST) ;
  - les mécanismes d'atténuation créés en réponse aux préoccupations et aux vulnérabilités nouvelles et émergentes concernant la cybersécurité dans la chaîne d'approvisionnement ;
  - les retours d'expérience internes visant l'amélioration continue au sein des organisations – déficiences décelées, occasions d'amélioration et leçons à retenir.
- Le *cadre supérieur CIP* ou son délégataire dûment désigné examine, au moins une fois tous les 15 mois civils, tout changement apporté aux plans de gestion des risques de cybersécurité dans la chaîne d'approvisionnement. Ces examens peuvent être plus fréquents selon le moment et l'ampleur des changements aux plans de gestion des risques de cybersécurité dans la chaîne d'approvisionnement. Après avoir approuvé ces changements, le *cadre supérieur CIP* ou son délégataire dûment désigné doit en informer adéquatement les organisations ou personnes concernées. En outre, il peut être souhaitable de créer des outils de communication ou du matériel de formation afin d'informer les secteurs organisationnels touchés par les révisions.

Références

- Utilities Technology Council (UTC) – *Cyber Supply Chain Risk Management for Utilities – Roadmap for Implementation*
- ISO/CEI 27036 – *Sécurité d'information pour la relation avec le fournisseur*
- NIST PE 800-53 – *Security and Privacy Controls for Federal Information Systems and Organizations System and Services Acquisition* (SA-3, SA-8 et SA-22)
- NIST PE 800-161 – *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*
- Energy Sector Control Systems Working Group (ESCSWG) – *Cybersecurity Procurement Language for Energy Delivery Systems*