

NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Cybersécurité – Communications entre centres de contrôle

Justification technique de la norme de fiabilité
CIP-012-2

Novembre 2023

RELIABILITY | ACCOUNTABILITY



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

Table des matières

Préface..... iii

Introduction..... iv

 CIP-012-1 iv

 CIP-012-2 iv

 Exemption visant certains *centres de contrôle* dans la norme CIP-012 (section A.4.2.3) v

Exigence E1 1

 Remarques générales concernant l'exigence E1 1

 Concepts de confidentialité, d'intégrité et de disponibilité..... 2

 Coordination avec les normes IRO et TOP 3

 Indication des endroits où l'entité responsable applique les moyens de protection 4

 Propriété des centres de contrôle 4

Références 6

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, en travaillant à réduire de façon 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
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-012 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 contient aussi des éclaircissements sur l'intention de l'équipe de rédaction de la norme. Le présent document, *Justification technique de la norme de fiabilité CIP-012*, n'est pas une norme de fiabilité et son contenu ne doit donc pas être considéré comme obligatoire et exécutoire.

CIP-012-1

Le 21 janvier 2016, la Federal Energy Regulatory Commission (FERC) publiait l'Ordonnance 822, par laquelle elle approuvait sept normes de fiabilité sur la protection de l'infrastructure essentielle (normes CIP) ainsi que des termes nouveaux ou modifiés dans le *Glossaire des termes et des acronymes relatifs aux normes de fiabilité de la NERC*, et demandait des modifications aux normes de fiabilité CIP. Entre autres, la FERC demandait à la North American Electric Reliability Corporation (NERC) d'« apporter des modifications aux normes de fiabilité CIP afin d'exiger des entités responsables¹ qu'elles mettent en œuvre des mesures visant à protéger, à tout le moins, les liaisons de communication et les données sensibles du *système de production-transport d'électricité (BES)* transmises entre les *centres de contrôle* du *BES*, d'une manière adéquatement adaptée pour répondre aux risques que les actifs à protéger (à impact élevé, moyen et faible) présentent pour le *BES* » (paragraphe 53 de l'Ordonnance 822).

En réponse à la prescription formulée dans l'Ordonnance 822, l'équipe de rédaction du Projet 2016-02 a élaboré la norme de fiabilité CIP-012-1 afin d'exiger des entités responsables qu'elles mettent en œuvre des mesures visant à protéger les données sensibles du *BES* et les liaisons de communication entre les *centres de contrôle* du *BES*. Étant donné le caractère sensible des données échangées entre les *centres de contrôle*, selon la définition du *Glossaire des termes et des acronymes relatifs aux normes de fiabilité de la NERC*, la norme s'applique à tous les niveaux d'impact (élevé, moyen et faible).

Bien que la FERC ait demandé à la NERC d'apporter des modifications à la norme CIP-006, l'équipe de rédaction a déterminé que des modifications à cette norme ne seraient pas appropriées pour sécuriser les données. En effet, il y a des différences entre les plans dont la norme CIP-012-1 exige la création et la mise en œuvre, et la protection spécifiée à l'alinéa 1.10 de l'exigence E1 de la norme CIP-006. Les exigences E1 et E2 de la norme CIP-012-1 protègent les données visées pendant leur transmission entre deux *centres de contrôle* distincts. Quant à l'alinéa 1.10 de l'exigence E1 de la norme CIP-006, il vise à protéger les composants de communication non programmables situés à l'intérieur d'un *périmètre de sécurité électronique (ESP)*, mais à l'extérieur d'un *périmètre de sécurité physique (PSP)*. Étant donné que la transmission des données visées entre *centres de contrôle* se fait à l'extérieur d'un *ESP*, la protection exigée à l'alinéa 1.10 de l'exigence E1 de la norme CIP-006-6 n'est pas pertinente.

CIP-012-2

Le 23 janvier 2020, la Federal Energy Regulatory Commission (FERC) publiait l'Ordonnance 866, par laquelle elle approuvait la norme CIP-012-1 tout en demandant à la NERC de modifier cette norme pour exiger des entités responsables qu'elles élaborent un ou des plans visant à protéger la disponibilité des liaisons de communication et celle des données pendant leur transmission entre des *centres de contrôle* du *BES*. En réponse à cette prescription de l'Ordonnance 866, l'équipe de rédaction (SDT) du Projet 2020-04 a remanié les alinéas de l'exigence E1 en y ajoutant des exigences pour obliger les entités à décrire les

1. Dans le contexte des normes CIP, le terme « entité responsable » désigne les entités inscrites visées par les normes CIP.

moyens visant à atténuer les risques découlant d'une perte de la capacité de transmission des données entre *centres de contrôle*.

Dans l'Ordonnance 866, la FERC spécifiait par ailleurs que « l'impératif de maintenir la disponibilité des réseaux de communication et des données devrait se traduire par l'intégration de mesures de rétablissement après incident et de continuité des opérations dans le plan de conformité d'une entité responsable ». La FERC convenait qu'il est impossible de toujours garantir la redondance des liaisons de communication, d'où la nécessité de plans tant pour le rétablissement des liaisons de communication compromises que pour le recours à des moyens de communication de relève². L'équipe de rédaction reconnaît que les entités responsables peuvent déjà avoir prévu ces contingences dans leurs plans existants de rétablissement ou d'intervention en cas d'incident. Des pièces justificatives pertinentes liées à ces plans peuvent être mises en référence pour attester la conformité à la norme CIP-012, de manière à éviter la duplication des tâches administratives.

L'équipe de rédaction a formulé des exigences qui donnent aux entités responsables la latitude voulue pour protéger les liaisons de communication, les données, ou les deux, de manière à atténuer les risques associés en tenant compte des capacités de l'environnement opérationnel de l'entité responsable.

Exemption visant certains *centres de contrôle* dans la norme CIP-012 (section A.4.2.3)

Au cours de la rédaction de la norme CIP-012, l'équipe de rédaction a pris conscience de certaines situations où des actifs comme des centrales électriques ou des postes de transport pourraient aussi être classés comme *centres de contrôle* selon la définition actuelle de ce terme. Leurs communications avec les *centres de contrôle de responsable de l'équilibrage (BA)* ou d'*exploitant de réseau de transport (TOP)*, cependant, ne sont pas incluses dans le champ d'application de la norme CIP-012 : en effet, ces communications ne sont pas différentes de celles d'autres centrales ou postes. L'équipe de rédaction a donc prévu une exemption (section A.4.2.3 de la norme CIP-012) pour ce scénario particulier, qui est décrit plus en détail ci-dessous.

2. Voir l'Ordonnance 866 de la FERC, paragraphes 35 et 36.

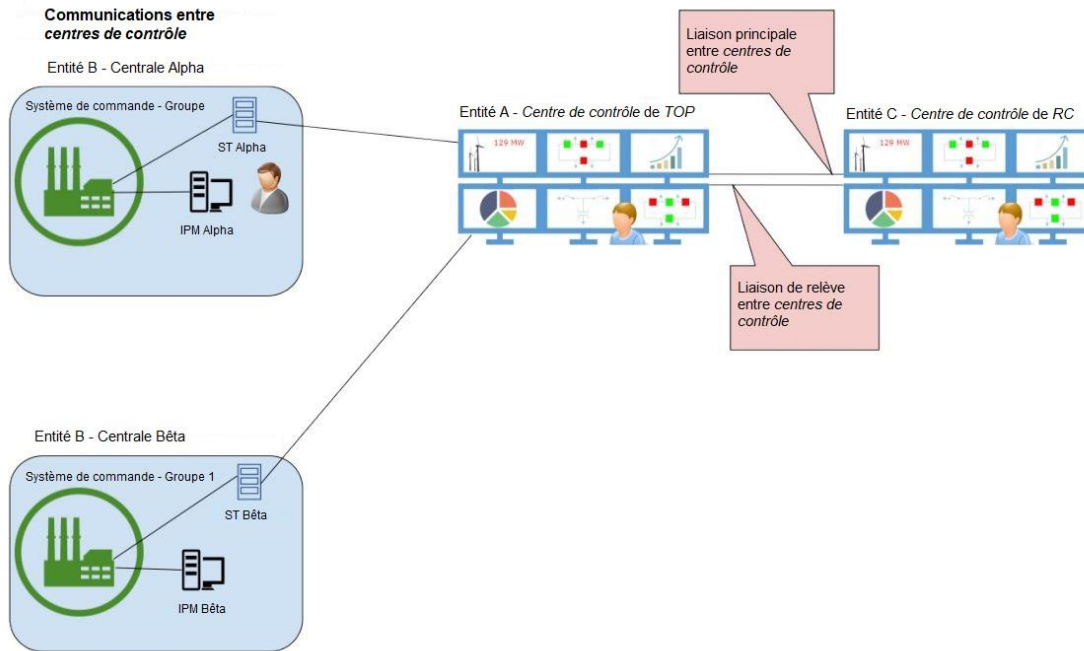


Figure 1

La figure 1 présente un scénario typique dans lequel deux *centres de contrôle* communiquent entre eux (ici, le *centre de contrôle* du RC de l'entité C et le *centre de contrôle* du TOP de l'entité A). La communication entre ceux-ci est visée par la norme CIP-012 si elle correspond aux inclusions et aux exclusions de la norme concernant les types de données. Le *centre de contrôle* du TOP communique avec une station terminale (ST) à deux des centrales électriques de l'entité B (centrales Alpha et Bêta). Ces stations terminales recueillent l'information de chacun des systèmes de commande de groupe de production. Chaque groupe de production de chaque centrale a une interface personne-machine (IPM) – soit un poste de travail d'exploitant – que le personnel local utilise pour piloter les différents groupes de production.

L'entité B décide que le groupe de production à la centrale Bêta – une petite installation de pointe – n'aura un exploitant sur place que pendant le jour. L'exploitant de la centrale Alpha devrait être capable de démarrer à distance le groupe de la centrale Bêta si nécessaire.

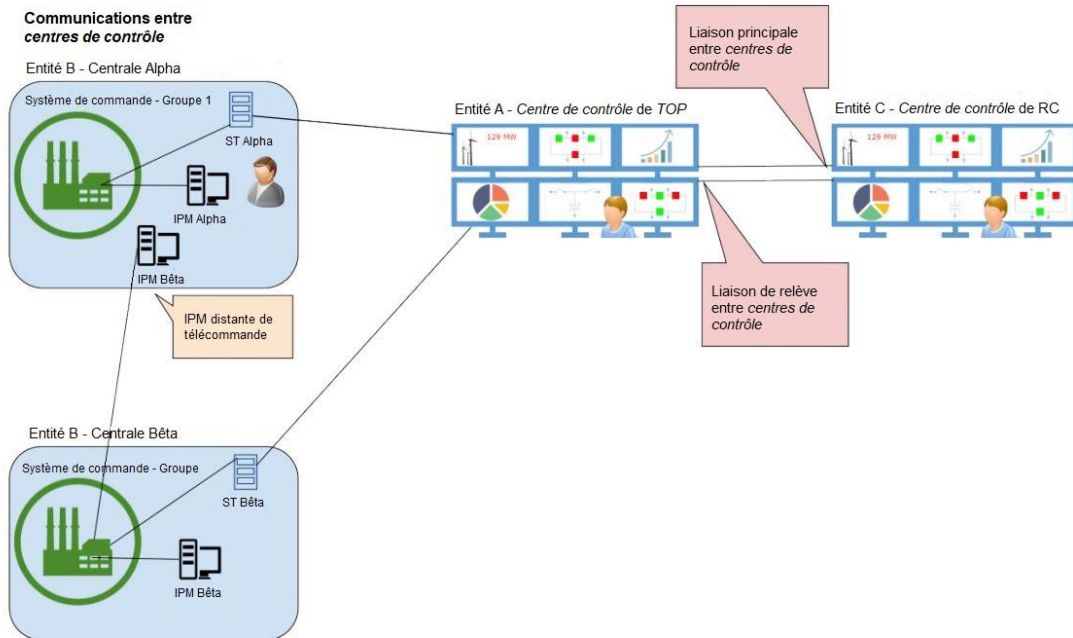


Figure 2

À la figure 2, l'entité B a installé un circuit de communication réservé entre le système de commande de la centrale Bêta et une IPM exclusive installée à l'intention de l'exploitant de la centrale Alpha. La centrale Alpha constitue maintenant « une ou plusieurs installations qui hébergent un personnel d'exploitation qui surveille et contrôle le *BES* en temps réel afin d'effectuer les tâches de fiabilité d'un... *exploitant d'installation de production* pour des *installations* de production à deux endroits ou plus » puisque les centrales Alpha et Bêta sont deux emplacements de centrale différents. La centrale Alpha peut maintenant être classée non seulement comme ressource de production, mais aussi comme *centre de contrôle*.

Les communications vers les *centres de contrôle* du *TOP* et du *RC* n'ont pas changé par rapport à la figure 1. Aucun nouveau système électronique susceptible d'avoir un impact sur plusieurs groupes de production n'a été mis en place. En outre, aucun système électronique n'a été ajouté pour remplir des fonctions de *centre de contrôle*. Le seul changement est le déplacement d'une IPM de la centrale Bêta vers la centrale Alpha à proximité physique immédiate d'une autre IPM.

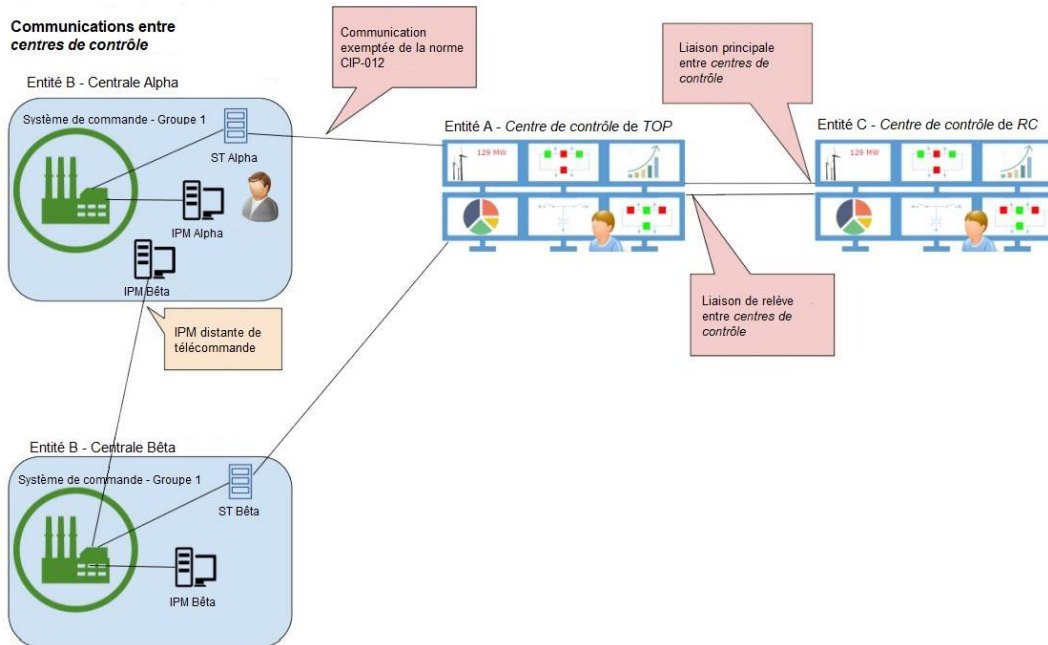


Figure 3

Bien que rien n'ait changé entre ces entités, cette proximité des IPM aurait pour conséquence (si l'on ne tient pas compte de l'exemption) que la communication indiquée à la figure 3 entre la centrale Alpha et le *centre de contrôle* du TOP de l'entité A serait visée par la norme CIP-012. Deux IPM ayant été mises en présence dans le même local, cette nouvelle norme CIP s'appliquerait aux deux entités. En raison de l'exemption 4.2.3, ce cas de figure n'est pas visé par la norme CIP-012.

Il s'agit là d'une anomalie liée à la définition actuelle de *centre de contrôle* applicable à une installation, à un local ou à un bâtiment à partir duquel certaines fonctions peuvent être exécutées sans égard à la façon de faire ou aux systèmes utilisés. L'exemple présenté est spécifique à des installations de production, mais la même possibilité existe dans le cas d'un poste électrique équipé d'une IPM ou d'un relais de protection que le « personnel d'exploitation » du poste pourrait utiliser pour agir sur un poste adjacent. Par ailleurs, il est clair que dans les critères applicables aux *propriétaires d'installation de transport (TO)* et aux *exploitants d'installation de production (GOP)*, la mention « deux endroits ou plus » n'est pas un filtre suffisamment précis pour définir ce qu'est vraiment un *centre de contrôle*. Les efforts de l'équipe de rédaction visant à corriger ce problème en clarifiant la définition de *centre de contrôle* ont révélé des problématiques plus étendues, qui débordent le mandat défini dans la demande d'autorisation de norme (SAR) de l'équipe de rédaction. C'est pourquoi l'équipe de rédaction a décidé de traiter ce cas au moyen de l'exemption de la section 4.2.3 de la norme CIP-012, qui se lit comme suit :

4.2.3. Tout *centre de contrôle* qui transmet à un autre *centre de contrôle* des données d'évaluation en temps réel ou de surveillance en temps réel concernant exclusivement la ressource de production ou le poste de *transport* situé au même endroit que le *centre de contrôle* transmetteur.

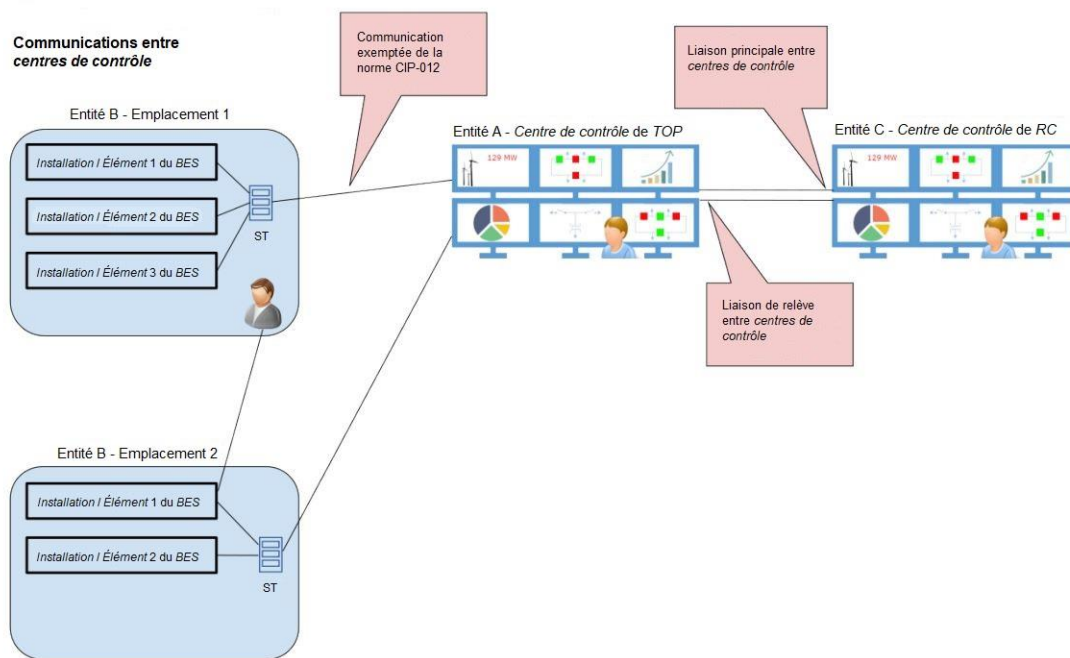
Cette exemption vise à exclure de l'application de la norme CIP-012 les communications normales d'un actif sur le terrain qui transmet des informations sur son état d'exploitation au moyen d'une station terminale ou d'un autre appareil de ce type. Dans ce scénario ou d'autres semblables, cette communication n'a pas changé et il s'agit toujours des mêmes données concernant un seul emplacement. L'équipe de rédaction considère qu'une telle communication ne doit pas être visée par une norme ayant pour objet de protéger les communications entre *centres de contrôle*, et que ce type d'équipement peut utiliser des technologies et des protocoles de communication existants plus anciens.

L'exemption de la section 4.2.3 couvre les emplacements de ressources de production ou de poste de *transport* où se trouve du personnel d'exploitation et où l'on peut commander des *installations* du *BES* à deux endroits ou plus, de sorte qu'on peut considérer qu'il s'agit de *centres de contrôle* situés au même endroit.

La communication est exemptée de la norme CIP-012 si chaque emplacement communique avec un autre *centre de contrôle* des données d'évaluation en temps réel ou de surveillance en temps réel concernant uniquement l'emplacement lui-même.

Les schémas qui précèdent sont spécifiques à des installations de production. Le schéma suivant est plus générique :

Figure 4



À la figure 4, chaque emplacement communique uniquement les données d'évaluation en temps réel ou de surveillance en temps réel qui le concernent spécifiquement, et aucune autre donnée d'évaluation en temps réel ou de surveillance en temps réel concernant un autre emplacement. La communication de l'emplacement 1 de l'entité B vers l'entité A est alors exemptée de la norme CIP-012.

Si l'emplacement 2 communiquait ses données par l'intermédiaire de l'emplacement 1, et que l'emplacement 1 avait pour fonction de contrôler et de regrouper des données de plusieurs emplacements

vers le *centre de contrôle* du *TOP* de l'entité A, alors la communication entre l'emplacement 1 et le *centre de contrôle* du *TOP* de l'entité A ne serait pas exemptée de la norme CIP-012.

Exigence E1

E1. L'entité responsable doit mettre en œuvre, sauf dans des *circonstances CIP exceptionnelles*, un ou des plans documentés visant à atténuer les risques découlant d'une divulgation non autorisée, d'une modification non autorisée ou d'une perte de disponibilité de données d'*évaluation en temps réel* ou de surveillance en *temps réel* pendant leur transmission entre des *centres de contrôle* visés. Le ou les plans de l'entité responsable peuvent ne pas englober les communications verbales. Le ou les plans doivent comprendre les éléments suivants :

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

- 1.1. une description des moyens visant à atténuer les risques découlant d'une divulgation non autorisée ou d'une modification non autorisée de données d'*évaluation en temps réel* ou de surveillance en *temps réel* pendant leur transmission entre des *centres de contrôle* ;
- 1.2. une description des moyens visant à atténuer les risques découlant d'une perte de la capacité de transmission des données d'*évaluation en temps réel* ou de surveillance en *temps réel* entre des *centres de contrôle* ;
- 1.3. une description des moyens prévus pour entreprendre le rétablissement des liaisons de communication servant à transmettre les données d'*évaluation en temps réel* et de surveillance en *temps réel* entre des *centres de contrôle* ;
- 1.4. les endroits où l'entité responsable applique les moyens prescrits aux alinéas 1.1 et 1.2 ; et
- 1.5. si les *centres de contrôle* sont détenus ou exploités par des entités responsables différentes, l'indication des responsabilités de chaque entité responsable dans l'application des moyens prescrits aux alinéas 1.1, 1.2 et 1.3.

Remarques générales concernant l'exigence E1

L'exigence E1 est axée sur la mise en œuvre d'un plan documenté visant à protéger l'information critique pour l'exploitation en *temps réel* du BES pendant sa transmission entre des *centres de contrôle* visés. Dans l'esprit de l'équipe de rédaction, la séquence des alinéas de l'exigence ne revêt aucune signification particulière. L'équipe de rédaction a décidé de remanier les alinéas de l'exigence E1 à partir des commentaires de l'industrie de manière à exiger la description des méthodes ou mesures prévues, afin d'aider les entités à bien évaluer ce qui est jugé nécessaire pour répondre aux exigences.

L'alinéa 1.1 demande à l'entité responsable d'inclure dans le plan exigé par la norme CIP-012 une description des moyens prévus pour protéger la sécurité des données, spécifiquement les données d'*évaluation en temps réel* et de surveillance en *temps réel* pendant leur transmission entre des *centres de contrôle* visés. Les moyens utilisables comprennent la protection physique de composants et d'équipements, ainsi que la protection logique des données pendant la transmission.

L'alinéa 1.2 demande d'inclure dans le plan exigé par la norme CIP-012 une description des moyens prévus pour atténuer les risques découlant d'une perte de la capacité de transmission des données d'*évaluation en temps réel* et de surveillance en *temps réel*. Une perte de la capacité de transmission de données entre *centres de contrôle* peut survenir dans divers scénarios – par exemple une mauvaise configuration d'équipement, un bris physique du support de transmission, ou encore une cyberattaque. Comme il s'agit

d'une norme CIP, la norme CIP-012 met l'accent sur les mesures de cybersécurité visant le maintien de la disponibilité. La redondance des circuits, le recours à des systèmes de relève et la cyberprotection des circuits sont quelques moyens potentiels de maintenir la capacité de transmission des données d'*évaluation en temps réel* et de surveillance en *temps réel*.

L'alinéa 1.3 concerne le besoin de décrire les moyens prévus pour entreprendre le rétablissement des liaisons de communication. Un facteur important pour une circulation fiable des données est la disponibilité des liaisons de communication elles-mêmes, c'est-à-dire le support par lequel les données sont transmises entre les *centres de contrôle* (fibre optique, conducteur de cuivre, satellite, etc.). Il importe d'être en mesure de rétablir la capacité de transmission en cas d'indisponibilité, quelle qu'en soit la cause. Cette description des moyens prévus peut être intégrée dans le plan exigé par la norme CIP-012, ou encore ce plan peut renvoyer à d'autres plans permettant de réaliser l'objectif de cet alinéa.

L'alinéa 1.4 demande d'indiquer les endroits où les moyens de protection prévus sont appliqués. Le fait que ces endroits soient indiqués explicitement aidera à assurer une couverture adéquate par les moyens de protection. À cette fin, on peut intégrer dans le plan un document qui décrit l'emplacement des divers composants, des schémas indiquant ces emplacements, ou une combinaison des deux. Pour d'autres détails, voir la section *Indication des endroits où l'entité responsable applique les moyens de protection*, ci-après.

L'alinéa 1.5 demande de préciser les exigences applicables à chacune des deux extrémités d'un transfert de données dans les cas où les *centres de contrôle* sont détenus ou exploités par des entités responsables différentes. Une compréhension claire de l'étendue exacte des responsabilités de chacune des deux entités facilitera le rétablissement de la liaison en cas de difficulté dans la transmission de données.

Rappelons enfin que dans l'esprit de l'équipe de rédaction, la séquence des alinéas de l'exigence ne revêt aucune signification particulière.

Concepts de confidentialité, d'intégrité et de disponibilité

Pour l'équipe de rédaction, la norme CIP-012 vise à assurer la confidentialité, l'intégrité et la disponibilité des données d'*évaluation en temps réel* et de surveillance en *temps réel*. Ainsi, l'exigence est rédigée de manière à atténuer les risques posés par une divulgation non autorisée (confidentialité), une modification non autorisée (intégrité) et des lacunes de transmission des données (disponibilité). Pour cette norme, l'équipe de rédaction se réfère aux définitions des termes « confidentialité », « intégrité » et « disponibilité » du National Institute of Standards and Technology (NIST) :

- La confidentialité est définie comme la « préservation des restrictions autorisées imposées à l'accès à l'information et à sa divulgation, notamment en employant des méthodes de protection des renseignements personnels et de l'information confidentielle »³.
- L'intégrité est définie comme la « protection de l'information contre toute destruction ou modification inappropriée en assurant notamment sa non-répudiation et son authenticité »⁴.

3. [Publication spéciale 800-53A \(révision 4\) du NIST](#), page B-3.

4. [Publication spéciale 800-53A \(révision 4\) du NIST](#), page B-6.

- À partir de la définition du NIST⁵, l'équipe de rédaction définit la disponibilité comme un « accès fiable et en temps voulu à l'information ».

L'exigence de la norme CIP-012 de préserver la disponibilité des données vise à atténuer les risques liés à un bris de transmission (notion de disponibilité) entre des *centres de contrôle* visés. L'équipe de rédaction reconnaît que la disponibilité et l'utilisation des données d'*évaluation en temps réel* et de surveillance en *temps réel* sont essentielles pour respecter les obligations de performance liées aux normes de fiabilité concernant l'exploitation et la planification. La norme CIP-012 a été rédigée de manière à couvrir les données pendant leur transmission entre des *centres de contrôle* visés. L'équipe de rédaction considère que ces données, sauf pendant leur transmission, résident à l'intérieur de *systèmes électroniques BES*, et qu'à ce titre elles sont protégées par d'autres normes CIP. L'utilisation de ces données est un enjeu d'exploitation et de planification et est explicitement couverte par d'autres normes de fiabilité de la NERC.

En cas de perte de données d'*évaluation en temps réel* ou de surveillance en *temps réel*, l'entité touchée se trouve privée de certaines données dont elle a besoin pour assurer le fonctionnement fiable du *BES*. L'atténuation des risques découlant d'une perte de données d'*évaluation en temps réel* ou de surveillance en *temps réel* peut être réalisée de différentes façons, lesquelles sont détaillées dans la section Mesures de la norme.

Coordination avec les normes IRO et TOP

L'équipe de rédaction a pris note de la mention par la FERC de normes de fiabilité supplémentaires et de la responsabilité de protéger les données visées conformément aux normes de fiabilité TOP-003 et IRO-010 de la NERC. L'équipe de rédaction a utilisé ces références dans sa démarche visant à déterminer les données *BES* sensibles, et a choisi de fonder les exigences de la norme CIP-012 sur les éléments de spécification des données en *temps réel* de ces normes. De cette façon, la cohérence dans l'applicabilité des données visées est assurée, et chaque entité n'est pas obligée de dresser sa propre liste de ces données. De nombreuses entités sont tenues de fournir ces données en vertu d'ententes conclues avec leur *RC*, leur *BA* ou leur *TOP*. Les données dont la protection est exigée par la norme CIP-012 correspondent à un sous-ensemble des données désignées par le *RC*, le *BA* et le *TOP* dans les normes de spécification des données TOP-003 et IRO-010, et se limitent aux données d'*évaluation en temps réel* et de surveillance en *temps réel*. La norme CIP-012 exclut les autres données généralement transférées entre *centres de contrôle*, comme les données d'*analyse de planification opérationnelle*, les données météorologiques, les données de marché, ainsi que d'autres données non utilisées par le *RC*, le *BA* et le *TOP* pour leurs évaluations et analyses de fiabilité en *temps réel* indiquées dans les normes TOP-003 et IRO-010. L'équipe de rédaction a déterminé que les données d'*analyse de planification opérationnelle*, si elles étaient dégradées, mal utilisées ou indisponibles, n'auraient pas d'impact négatif sur l'exploitation fiable du *BES* dans les 15 minutes suivant le début de la compromission, selon ce qu'indique la norme CIP-002-5.1a. L'équipe de rédaction note que dans certaines situations spéciales, des données d'*évaluation en temps réel* ou de surveillance en *temps réel* ne sont pas désignées par le *RC*, le *BA* ou le *TOP*. Il pourrait s'agir par exemple de données qui peuvent être échangées entre le *centre de contrôle* principal et le *centre de contrôle* de repli d'une entité responsable.

Si les moyens de protection adoptés par les entités responsables en conformité avec la norme CIP-012 ont pour effet d'ajouter des éléments d'infrastructure d'échange de données dans le *centre de contrôle* principal, les entités doivent veiller au maintien de la conformité avec les prescriptions des normes TOP-001 et

5. [Publication spéciale 800-59 du NIST](#), sous « *Availability* » (disponibilité), d'après 44 U.S.C., Sec. 3542 (b)(1)(C)

IRO-002 qui demandent la mise en œuvre et la mise à l'essai d'une infrastructure d'échange de données redondante et à acheminement diversifié.

Indication des endroits où l'entité responsable applique les moyens de protection

L'équipe de rédaction a noté le besoin que l'entité responsable indique à quels endroits elle applique les moyens de protection des données visées. L'équipe de rédaction ne spécifie pas à quels endroits les protections de sécurité et de disponibilité exigées par la norme CIP-012 doivent être appliquées ; les entités responsables ont ainsi toute latitude pour implanter les mécanismes de sécurité le mieux adaptés à leur situation particulière. Cette latitude permet aux entités de tirer parti de différentes mesures de sécurité, comme une inspection approfondie des paquets au *point d'accès électronique (EAP)* ou à proximité, en présence d'un *périmètre de sécurité électronique (ESP)*, tout en maintenant la capacité de protéger les données visées pendant leur transmission entre *centres de contrôle*.

L'équipe de rédaction reconnaît aussi que les moyens de protection de la norme CIP-012 peuvent être appliqués à un *actif électronique* qui n'est pas désigné comme *actif électronique BES (BCA)*, *actif électronique protégé (PCA)* ou *système de contrôle ou de surveillance des accès électroniques (EACMS)*. La désignation d'un *actif électronique* à l'endroit où une protection de sécurité est appliquée n'a pas pour effet d'étendre à cet *actif électronique* l'applicabilité de l'ensemble des normes de cybersécurité.

L'équipe de rédaction est consciente du fait que dans les échanges de données entre *centres de contrôle*, une seule et même entité peut ne pas être responsable des deux extrémités de la liaison de communication. Pour l'équipe de rédaction, une entité responsable doit indiquer seulement à quels endroits elle a appliqué ses propres moyens de protection de sécurité et de disponibilité. L'entité responsable doit agir en coordination avec une entité voisine, dans les cas où cette dernière a appliqué à son installation des moyens de protection qui ont un impact sur les flux de données de l'entité responsable, afin de veiller à ce que les protections appropriées soient en place. Si les protections de sécurité (chiffrement ou déchiffrement, etc.) sont appliquées sur une liaison de communication située à l'extérieur du *PSP* du *centre de contrôle* des entités responsables (zone sécurisée physiquement, local de télécommunications, etc.), les protections de sécurité doivent se prolonger jusqu'à l'entrée des données dans le *PSP* du *centre de contrôle*.

Une entité responsable peut décider d'assumer la responsabilité des deux extrémités d'une liaison de communication ; par exemple, elle peut placer un routeur dans le centre de données d'une entité voisine. Dans un scénario où une entité responsable assume la mise en place des moyens de protection aux deux extrémités de la liaison de communication, elle doit indiquer à quel endroit elle a appliqué les moyens de protection à chacune des extrémités de la liaison. L'équipe de rédaction souhaite que soient coordonnées la désignation de l'endroit d'application des moyens de protection selon l'alinéa 1.4 de l'exigence E1 de la norme CIP-012 et l'indication des responsabilités des entités responsables selon l'alinéa 1.5 de cette même exigence.

Propriété des centres de contrôle

Les exigences de la norme CIP-012 portent sur la protection des données d'*évaluation en temps réel* et de surveillance en *temps réel* pendant leur transmission entre des *centres de contrôle* appartenant à une même entité responsable ; elles concernent aussi les données visées transmises entre des *centres de contrôle* appartenant à différentes entités responsables. Par rapport au scénario où les *centres de contrôle* appartiennent à une même entité responsable, l'application de la protection entre des *centres de contrôle* appartenant à plusieurs entités responsables nécessite une coordination supplémentaire. La norme

n'impose pas explicitement des accords formels entre les entités responsables qui collaborent à la protection des données visées ; toutefois, il est fortement recommandé que ces entités établissent des ententes, ou utilisent des ententes existantes, pour définir leurs responsabilités en vue de réaliser l'objectif de sécurité. Pour reprendre un exemple donné au paragraphe 59 de l'Ordonnance 822 de la FERC : « si plusieurs entités inscrites ont une responsabilité commune dans l'utilisation d'un système de gestion de clés cryptographiques pour les transmissions entre leurs *centres de contrôle* respectifs, elles devraient avoir la prérogative de se concerter pour désigner quelle organisation administre ce système de gestion de clés ».

Pour récapituler, l'exemple de la figure 5 montre différentes transmissions de données entre *centres de contrôle* qu'une entité responsable devrait considérer comme visées par la norme. Le modèle de référence ne couvre pas tous les scénarios possibles. Les lignes vertes continues représentent les communications visées par la norme ; les lignes rouges pointillées, les communications non visées.

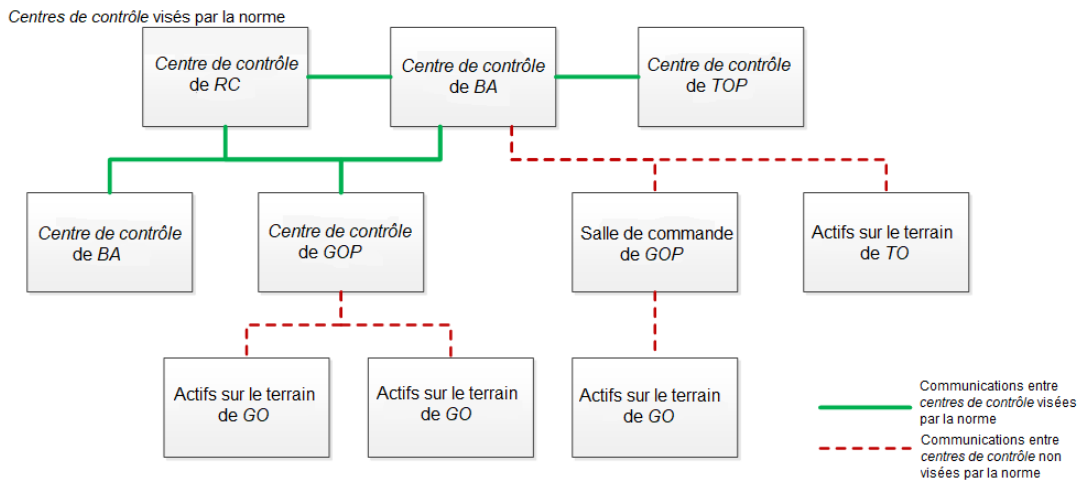


Figure 5 : Modèle de référence présenté à titre d'exemple (ne couvre pas tous les scénarios possibles)

L'équipe de rédaction a prévu l'alinéa 1.5 pour les situations où plusieurs entités inscrites sont concernées par la protection de données transmises entre *centres de contrôle*. L'alinéa 1.5 présente un mécanisme qui oblige à préciser les responsabilités des différentes entités dans l'application des protections de sécurité et de disponibilité. Cet alinéa vise à prévenir les problèmes de sécurité et de disponibilité et à simplifier le processus d'audit. Si les données sont transmises entre des entités différentes, l'équipe de rédaction souligne la nécessité que les deux entités comprennent les responsabilités d'application des moyens de protection des données sur l'intégralité du trajet de transmission, sans la moindre lacune dans les protections de sécurité et de disponibilité. L'équipe de rédaction souligne aussi que cet alinéa permettra de produire des pièces justificatives qui pourront éviter un audit simultané de plusieurs entités pour chaque liaison de communication entre des *centres de contrôle* exploités par des entités responsables différentes. Les moyens appliqués par chaque entité en vue de la conformité avec les alinéas 1.1 à 1.4 du plan devraient être en corrélation avec les responsabilités documentées à l'alinéa 1.5 du plan de l'entité.

Références

Les références suivantes pourront aider les entités à élaborer leurs plans de protection des liaisons de communication :

- [Publication spéciale 800-53A \(révision 4\) du NIST](#) : *Security and Privacy Controls for Federal Information Systems and Organizations*
- [Publication spéciale 800-82 du NIST](#) : *Guide to Industrial Control Systems (ICS) Security*
- [Publication spéciale 800-175B du NIST](#) : *Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms*
- [Publication 800-47 du NIST](#) : *Security Guide for Interconnecting Information Technology Systems*