

NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

VERSION PROVISOIRE DU GUIDE
En attente de la présentation à l'ERO pour approbation

Cybersécurité – Communications entre *centres de contrôle*

Guide d'application de la norme CIP-012-2

Novembre 2023

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
Contexte	iv
Exigences.....	1
Généralités.....	2
Élaboration du plan	2
Détermination des données d'évaluation en temps réel et de surveillance en temps réel	2
Atténuation des risques découlant d'une divulgation non autorisée ou d'une modification non autorisée (alinéa 1.1)	3
Atténuation des risques découlant d'une perte de la capacité de transmission des données (alinéa 1.2).....	4
Moyens prévus pour entreprendre le rétablissement (alinéa 1.3)	4
Indication des endroits où les protections de sécurité et de disponibilité sont appliquées (alinéa 1.4).....	5
Indication des responsabilités si les <i>centres de contrôle</i> sont détenus ou exploités par des entités responsables différentes (alinéa 1.5)	6
Modèle de référence.....	7
Description du modèle de référence.....	7
Indication des protections de sécurité	8
Atténuation des risques découlant d'une perte de la capacité de transmission des données	9
Moyens prévus pour entreprendre le rétablissement des liaisons de communication.....	9
Indication des endroits où l'entité responsable applique les protections de sécurité et de disponibilité	10
Indication des responsabilités si les <i>centres de contrôle</i> sont détenus ou exploités par des entités responsables différentes.....	11
Références.....	14

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	Reliability First
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

Introduction

L'équipe de rédaction des normes du Projet 2020-04 a produit le présent Guide d'application afin de présenter des exemples de démarches de mise en conformité avec la norme CIP-012-2. 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 particulière¹.

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

Ce document sera revu et mis à jour lors de la mise en route d'un projet d'élaboration de norme visant à modifier la norme CIP-012-2.

Contexte

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 CIP ainsi que des définitions nouvelles ou modifiées, tout en réclamant 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 responsables 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 cette prescription de l'Ordonnance 822, l'équipe de rédaction du Projet 2016-02 a élaboré la norme de fiabilité CIP-012-1 afin d'exiger que les entités responsables mettent en œuvre un ou des plans documentés 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* visés. Étant donné le caractère sensible des données échangées entre les *centres de contrôle*, la norme s'applique à tous les niveaux d'impact (élevé, moyen et faible).

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 du Projet 2020-04 a incorporé à la norme CIP-012-2 de nouvelles exigences relatives à la disponibilité.

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

1. [Politique de la NERC relative aux lignes directrices sur la conformité.](#)

Introduction

recours à des moyens de communication de relève². L'équipe de rédaction est consciente que les entités responsables peuvent déjà avoir prévu de telles contingences dans les plans exigés par les normes CIP-008 et CIP-009, et que ces plans peuvent être mis en référence pour réaliser la conformité à la norme CIP-012, de manière à éviter une duplication des tâches.

L'équipe de rédaction a remanié les exigences de la norme de manière à accorder aux entités responsables la latitude souhaitable pour protéger les données d'*évaluation en temps réel* et de surveillance en *temps réel*, dans le but d'atténuer les risques liés à toute divulgation non autorisée, modification non autorisée ou perte de disponibilité, afin de réaliser les objectifs de sécurité et de disponibilité.

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

Exigences

- 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.

Généralités

Élaboration du plan

Comme l'explique le document *Justification technique de la norme de fiabilité CIP-012-2*, l'exigence E1 vise essentiellement à mettre en œuvre un plan documenté afin de protéger l'information critique pour l'exploitation en temps réel du *BES* pendant son transit entre les *centres de contrôle* visés. Tout en approuvant la norme CIP-012-1 dans son Ordonnance 866, la FERC a aussi invité la NERC à exiger des protections quant à la disponibilité des liaisons de communication et des données transmises entre des *centres de contrôle* du *BES*. La norme CIP-012-2 a été élaborée afin de répondre à ces besoins supplémentaires de protection de la disponibilité des données pendant leur transmission.

Pour la norme CIP-012-2, l'équipe de rédaction a modifié la définition du terme « disponibilité » donnée par le National Institute of Standards and Technology (NIST)³ :

- La disponibilité est définie comme étant « un accès fiable et en temps voulu à l'information ».

Le nombre de plans et leur contenu peuvent varier selon la structure de gestion et le contexte d'exploitation de l'entité responsable. Celle-ci peut documenter autant de plans que nécessaire en fonction de ses besoins. Si les plans de l'entité responsable en matière de protection de l'infrastructure essentielle ou d'exploitation et planification couvrent tous les éléments exigés par la norme CIP-012-2, les pièces justificatives pertinentes liées à ces plans peuvent être mises en référence dans le plan exigé par la norme CIP-012, de manière à attester la conformité à cette norme tout en évitant la duplication des tâches administratives. Par exemple, l'entité responsable peut, dans le plan exigé par la norme CIP-012, faire référence à la portion de son plan exigé par la norme CIP-009 qui se trouve à répondre à l'alinéa 1.3 de la norme CIP-012.

Par ailleurs, l'entité responsable peut choisir d'avoir un plan pour chaque *centre de contrôle*, ou opter au contraire pour un seul plan global couvrant l'ensemble de l'environnement de communication de ses *centres de contrôle*. Elle peut aussi choisir d'avoir un plan pour les communications entre les *centres de contrôle* dont elle est propriétaire, et un autre plan pour les communications entre ses *centres de contrôle* et ceux d'une entité voisine. Le nombre et la structure des plans sont laissés à la discrétion de l'entité responsable, pourvu que le ou les plans couvrent les éléments spécifiés aux alinéas 1.1 à 1.5 de l'exigence E1.

Les entités responsables doivent prendre note que la définition de *centre de contrôle* inclut les « centres informatiques connexes ». Rappelons aussi que la norme CIP-012 ne vise pas les données au repos, non plus que les communications verbales⁴.

Détermination des données d'évaluation en temps réel et de surveillance en temps réel

Les entités responsables peuvent s'attendre à recevoir ou ont déjà reçu des demandes de données d'*analyse de planification opérationnelle*, d'*évaluation en temps réel* ou de surveillance en temps réel de la part de leur *coordonnateur de la fiabilité (RC)*, de leur *responsable de l'équilibrage (BA)* ou de leur *exploitant de réseau de transport (TOP)*. Ces demandes de données, assujetties aux exigences de spécification des données des normes TOP-003 et IRO-010, peuvent aussi englober d'autres types de données. Or, la protection exigée par la norme CIP-012 porte uniquement sur les données d'*évaluation en temps réel* et de surveillance en temps réel. Si la spécification des données fournie ne précise pas quelles sont les données

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

4. Voir l'Ordonnance 866 de la FERC, paragraphe 11.

d'*évaluation en temps réel* et de surveillance en *temps réel*, l'entité responsable pourrait choisir de procéder à une analyse afin de distinguer ces types de données parmi les autres données demandées ou communiquées. Une fois cette analyse terminée, l'entité responsable devra confirmer ses conclusions auprès de l'autre entité avec laquelle elle communique avant d'appliquer les moyens de protection. Si les données d'*évaluation en temps réel* et de surveillance en *temps réel* ne sont pas clairement indiquées dans la spécification des données fournie, l'entité responsable doit documenter la méthode et les moyens qu'elle a utilisés pour déterminer les données d'*évaluation en temps réel* et de surveillance en *temps réel*.

Atténuation des risques découlant d'une divulgation non autorisée ou d'une modification non autorisée (alinéa 1.1)

Les entités ont toute latitude pour déterminer et choisir les protections de sécurité à utiliser pour 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*.

Ces protections de sécurité pourraient être de type logique ou physique, ou encore combiner ces deux types. Pour déterminer les moyens de protection de sécurité, il faut s'assurer que, conformément à l'exigence, ces moyens atténuent les risques découlant d'une divulgation non autorisée ou d'une modification non autorisée des données visées. Une protection physique convient habituellement si deux *centres de contrôle* sont très proches l'un de l'autre, cette protection étant appliquée intégralement au trajet de transmission (câblage et connexions) entre les deux. Une protection physique peut aussi être de mise si l'équipement de chiffrement est situé à proximité d'un *centre de contrôle*, mais quand même hors de celui-ci : la protection physique sert alors à protéger le câblage et les connexions entre le point terminal de chiffrement et le *centre de contrôle* lui-même.

Il existe différentes manières d'attester la mise en œuvre des protections de sécurité. Dans le cas d'une protection physique, l'entité responsable peut soumettre un plan d'étage du *centre de contrôle* visé, les détails étant par la suite confirmés par une inspection visuelle des mesures de sécurité physique en place pour protéger la liaison de communication. Dans le cas d'une protection logique, l'entité responsable peut attester la mise en œuvre en présentant l'exportation de la configuration du dispositif qui applique les protections de sécurité, par exemple :

- une exportation de la configuration d'un pare-feu montrant les paramètres d'un tunnel VPN et du routage des données visées dans le VPN ;
- une exportation de la configuration d'un dispositif de la couche transport qui démontre que le chiffrement est actif pour les données visées (ou pour toutes les données) ;
- la configuration d'une application qui atteste que les données visées sont chiffrées à partir de l'application d'origine jusqu'au client ou à l'application de destination.

Si les obligations opérationnelles relatives à l'ensemble de la liaison de communication – y compris ses deux points terminaux – incombent au *centre de contrôle* d'une seule des deux entités responsables, l'entité responsable exempte d'obligations opérationnelles pour la liaison de communication peut établir sa conformité en veillant à ce que le point terminal de la liaison de communication se trouve à l'intérieur de son *centre de contrôle*, ce qui pourrait consister simplement à situer le point terminal à l'intérieur d'un *périmètre de sécurité physique (PSP)* ou à tout autre endroit bénéficiant d'une protection physique.

Quant à la mise en œuvre du critère de disponibilité de la norme CIP-012, les entités responsables disposent d'une certaine latitude. L'information qui correspond à des données d'évaluation en temps réel et de surveillance en temps réel est soumise à un critère qualitatif défini par les exigences des normes IRO-010 et TOP-003. Ainsi, les alinéas 1.3 et 1.4 de l'exigence E1 de la norme TOP-003 spécifient les contraintes temporelles imposées à une entité responsable pour la fourniture des données d'évaluation en temps réel et de surveillance en temps réel. Une non-disponibilité de ces données en temps voulu peut nuire à la capacité d'une entité responsable de fournir ou d'utiliser ces données lorsqu'elle en a besoin. Une entité responsable doit indiquer comment le critère de disponibilité de la norme CIP-012 est respecté lors de la transmission des données. La disponibilité peut être réalisée au moyen de mesures de diversité ou de redondance, ou par une combinaison des deux. La diversité consiste à miser sur l'hétérogénéité afin de réduire les risques de défaillance de mode commun⁵ : par exemple, utiliser au moins deux protocoles ou voies de communication ayant des caractéristiques différentes. La redondance consiste à avoir plusieurs exemplaires protégés de ressources critiques⁶ : par exemple, prévoir au moins deux trajets ou modes de transmission pour acheminer les données. Une solution combinant diversité et redondance aux fins de la norme CIP-012 peut consister à utiliser plusieurs types de circuit (par exemple, fibre optique et liaison radio) et différents réseaux (par exemple, réseaux primaire et secondaire) pour éloigner les scénarios de défaillances multiples pouvant menacer la disponibilité des données.

Comme il a été dit précédemment, la disponibilité est généralement définie comme étant un accès fiable et en temps voulu à l'information. La disponibilité des données en transit peut être assurée de diverses manières. Un exemple serait d'utiliser des circuits redondants empruntant des trajets différents, de telle sorte que si un des circuits se dégrade ou tombe en panne, les données continueront de parvenir à destination. Une autre manière d'utiliser des trajets différents consisterait à acheminer les mêmes données à partir de plusieurs centres de contrôle : par exemple, un coordonnateur de la fiabilité peut vouloir faire transiter les données par le centre de contrôle d'un tiers, créant ainsi une source secondaire liée à un chemin séparé. Cette méthode peut être attestée au moyen de schémas de réseau indiquant la diversité des opérateurs ou l'utilisation de trajets distincts.

Une autre stratégie pour assurer la disponibilité consisterait à utiliser plusieurs systèmes différents, de telle sorte qu'une solution logicielle de transmission pourrait tomber en panne indépendamment d'un autre logiciel ou pile protocolaire, qui continuerait d'acheminer les données. On peut également attester cette solution au moyen de schémas de réseau ou de système montrant la diversité des ressources de transmission utilisées.

Atténuation des risques découlant d'une perte de la capacité de transmission des données (alinéa 1.2)

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, des mesures sont nécessaires pour préserver la continuité du transit des données. Les moyens utilisables sont variés : liaisons redondantes, diversité des systèmes ou services utilisés, etc. Les données d'évaluation en temps réel et de surveillance en temps réel sont nécessaires pour permettre à l'entité responsable de maintenir l'intégrité fonctionnelle et la stabilité du BES. Si la responsabilité de la liaison est partagée entre deux entités, les méthodes utilisées pour atténuer la perte de capacité de transmission de ces données doivent faire l'objet d'une entente entre les deux entités.

Moyens prévus pour entreprendre le rétablissement (alinéa 1.3)

En ce qui a trait au maintien de la disponibilité, le plan exigé par la norme CIP-012 doit décrire les moyens prévus pour entreprendre le rétablissement des liaisons de transmission de données en cas d'interruption.

5. [Publication spéciale du NIST 800-160v2](#), page 11

6. [Publication spéciale du NIST 800-160v2](#), page 11

Cet objectif est en concordance avec les normes TOP et IRO. Les modalités de rétablissement des liaisons de communication peuvent être décrites spécifiquement dans le plan exigé par la norme CIP-012, ou encore dans d'autres plans pertinents mis en référence dans ce plan. Dans le cadre du partage de données avec d'autres entités responsables, les responsabilités en matière de soutien et la coordination du rétablissement peuvent être documentées par différents moyens comme une procédure commune, un protocole d'entente, une convention, un procès-verbal ou d'autres documents précisant le partage des responsabilités entre les deux parties.

L'équipe de rédaction reconnaît aussi que les éléments du plan relatifs à la disponibilité peuvent ou non s'appliquer à des *actifs électroniques* déclarés comme *actifs électroniques BES*. Lorsqu'un plan exigé par la norme CIP-012 décrit les moyens de rétablissement de liaisons ou de circuits en faisant référence à un autre plan (par exemple, un plan de rétablissement exigé par la norme CIP-009), l'*entité responsable* doit préciser si certains éléments de la solution de disponibilité ne sont pas couverts par le plan mis en référence ; tout élément non couvert par le plan mis en référence peut soit être ajouté à ce plan, soit être incorporé directement dans le plan exigé par la norme CIP-012.

Indication des endroits où les protections de sécurité et de disponibilité sont appliquées (alinéa 1.4)

Pour déterminer à quels endroits appliquer les protections de sécurité et de disponibilité, l'entité responsable doit prendre en compte son environnement. Une approche consiste à mettre en œuvre les moyens de protection à l'intérieur du *centre de contrôle* lui-même de manière que la confidentialité et l'intégrité des données soient protégées tout au long du transit. L'entité responsable a le choix d'indiquer les endroits où sont appliquées les protections de sécurité selon un type d'emplacement logique ou physique. La mise en œuvre des mesures de sécurité de la norme CIP-012 n'a pas pour effet d'élargir le champ d'application des normes de fiabilité CIP à des actifs supplémentaires. L'emplacement des protections de sécurité appliquées peut varier selon de multiples facteurs, comme les niveaux d'impact du *centre de contrôle* ainsi que les différentes technologies ou infrastructures présentes. Si les obligations opérationnelles relatives à l'ensemble de la liaison de communication – y compris ses deux points terminaux – incombent au *centre de contrôle* d'une seule des deux entités responsables, l'entité responsable exempte d'obligations opérationnelles pour la liaison de communication peut établir sa conformité en veillant à ce que le point terminal de la liaison de communication se trouve à l'intérieur de son *centre de contrôle*, ce qui pourrait consister simplement à situer le point terminal à l'intérieur d'un *périmètre de sécurité physique (PSP)* ou à tout autre endroit bénéficiant d'une protection physique.

L'indication des endroits où l'entité responsable applique les protections de sécurité et de disponibilité pourrait prendre la forme d'une liste ou d'un schéma de *centre de contrôle* précisant les mesures de sécurité physiques ou logiques ainsi que les composants qui assurent la protection de disponibilité. Un schéma physique peut nécessiter une confirmation visuelle de ces mesures. Le schéma ou la liste pourrait être intégré au plan établi conformément à l'exigence E1. L'entité responsable pourrait aussi utiliser des étiquettes pour désigner les dispositifs en place aux endroits où les protections de sécurité et de disponibilité selon la norme CIP-012 sont appliquées.

Dans le cas d'échanges de données entre deux entités différentes, si une entité responsable gère seulement une extrémité de la liaison de communication, elle n'a pas à indiquer à quel endroit l'entité voisine avec laquelle elle échange des données applique ses protections de sécurité. Par contre, si une des entités assume la responsabilité des deux extrémités de la liaison de communication (par exemple en installant un routeur dans le centre de données de l'entité voisine), il lui incombe alors d'indiquer à quels endroits sont appliquées les protections de sécurité aux deux extrémités de la liaison. Les entités responsables aux deux

extrémités de la liaison doivent chacune indiquer où leurs protections de disponibilité sont appliquées, respectivement.

De même, si une entité responsable détient et exploite les deux *centres de contrôle* qui s'échangent des données (comme dans le cas d'un *centre de contrôle* principal et d'un *centre de contrôle* de repli), cette entité doit alors indiquer à quels endroits sont appliquées les protections de sécurité et de disponibilité aux deux extrémités de la liaison.

Indication des responsabilités si les *centres de contrôle* sont détenus ou exploités par des entités responsables différentes (alinéa 1.5)

La section *Propriété des centres de contrôle* du document de justification technique de la norme de fiabilité CIP-012 apporte des indications importantes sur les communications entre *centres de contrôle* de propriétaires ou d'exploitants différents. Dans bien des cas, les relations opérationnelles entre les différentes entités responsables ont leurs particularités. Il n'existe donc pas de formule universelle pour établir les responsabilités quant à l'application des protections de sécurité et de disponibilité pour la transmission des données d'évaluation en temps réel et de surveillance en temps réel entre *centres de contrôle*. Des discussions entre entités responsables pourraient permettre de cerner les besoins de soutien technique en dehors des heures ouvrables dans des situations où la disponibilité des données dépend d'actions indépendantes, comme la réinitialisation d'une liaison ICCP (Inter-Control Center Communications Protocol).

L'établissement des responsabilités doit être documenté de manière à désigner clairement les parties responsables et le point de démarcation où la responsabilité de la liaison de communication passe d'une entité à l'autre. Cette documentation peut comprendre des schémas de réseau, une procédure commune, un protocole d'entente ou encore un procès-verbal indiquant les responsabilités respectives de chaque partie.

Si les obligations opérationnelles relatives à l'ensemble de la liaison de communication – y compris ses deux points terminaux – incombent au *centre de contrôle* d'une seule des deux entités responsables, l'entité responsable exempte d'obligations opérationnelles pour la liaison de communication peut établir sa conformité en veillant à ce que le point terminal de la liaison de communication se trouve à l'intérieur de son *centre de contrôle*, ce qui pourrait consister simplement à situer le point terminal à l'intérieur d'un *périmètre de sécurité physique (PSP)* ou à tout autre endroit bénéficiant d'une protection physique.

Modèle de référence

Dans le présent Guide d'application, l'équipe de rédaction utilise un modèle de référence de base comportant un *centre de contrôle* principal et un *centre de contrôle* de repli (appartenant à l'entité Alpha) pour illustrer différentes manières de démontrer la conformité. Ces *centres de contrôle* communiquent entre eux ainsi qu'avec le *centre de contrôle* d'une entité voisine (entité Bêta) selon les configurations représentées aux schémas ci-après. L'équipe de rédaction reconnaît que le modèle de référence fait abstraction d'un bon nombre des complexités d'un véritable *centre de contrôle*. Dans ce Guide d'application, l'inscription des entités et les fonctions assurées dans les *centres de contrôle* du modèle de référence ne sont pas non plus prises en compte. La figure 1 présente un schéma fonctionnel de haut niveau du modèle de référence de base. L'exposé qui suit est rédigé dans la perspective de l'entité Alpha.

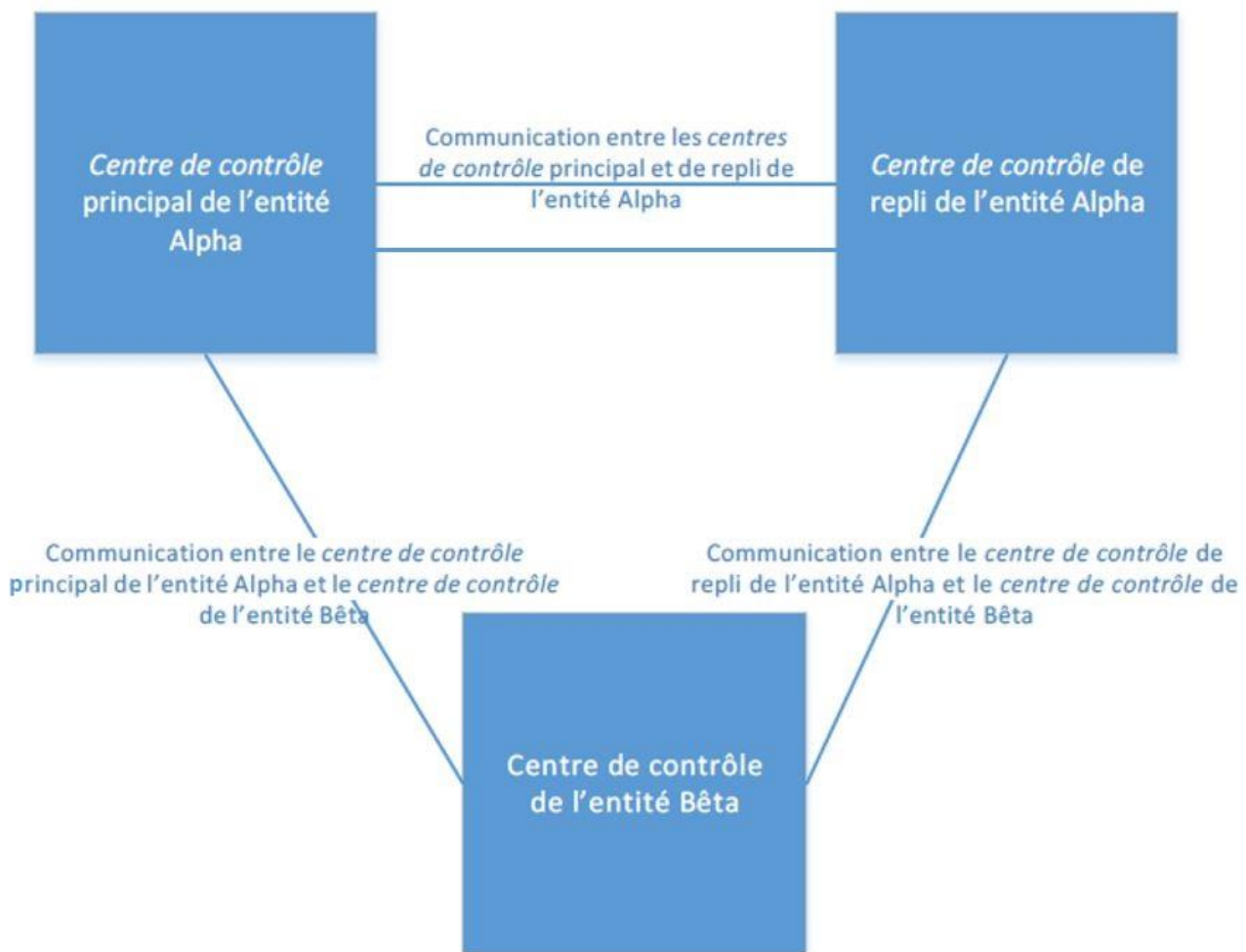


Figure 1 : Schéma fonctionnel de haut niveau des *centres de contrôle* du modèle de référence

Description du modèle de référence

L'exigence E1 demande la mise en œuvre d'un plan documenté. Pour satisfaire à cette exigence, une démarche appropriée consiste à déterminer d'abord quelles communications sont visées par la norme CIP-012. Il existe diverses manières d'établir la portée de l'exigence E1 pour une entité donnée. Par

exemple, l'entité Alpha du modèle de référence peut commencer par déterminer les *centres de contrôle* avec lesquels elle communique. Ceux-ci sont au nombre de trois : le *centre de contrôle* principal de l'entité Alpha, le *centre de contrôle* de repli de l'entité Alpha et un *centre de contrôle* de l'entité Bêta. L'entité Alpha n'a pas besoin de savoir si l'entité Bêta communique à son tour ses données à une autre entité ; cela concerne l'entité Bêta, et n'est plus dans le champ de responsabilité de l'entité Alpha. Par ailleurs, l'entité Alpha n'a pas besoin de considérer les communications avec des installations autres que des *centres de contrôle* (comme des centrales ou des postes électriques), car ces communications ne sont pas visées par la norme CIP-012.

Après avoir recensé les *centres de contrôle* avec lesquels elle communique, l'entité Alpha détermine ensuite, au choix : 1) les données d'*évaluation en temps réel* et de surveillance en *temps réel* ; ou 2) les liaisons de communication qui servent à transmettre des données d'*évaluation en temps réel* et de surveillance en *temps réel* entre les *centres de contrôle*. Dans un cas comme dans l'autre, l'entité Alpha peut se référer à la spécification de données des normes TOP-003 et IRO-010 pour les données d'*évaluation en temps réel* et de surveillance en *temps réel*. Ces normes spécifient aussi des exigences de fréquence pour la transmission des données, afin d'établir le critère de disponibilité. Dans le scénario du modèle de référence, le plus simple est probablement de déterminer les liaisons de communication qui servent à transmettre les données d'*évaluation en temps réel* et de surveillance en *temps réel*. Ainsi, après avoir évalué les liaisons de communication entre les *centres de contrôle* et examiné comment se font l'émission et la réception des données d'*évaluation en temps réel* et de surveillance en *temps réel*, l'entité Alpha détermine qu'elle communique les données visées entre ses *centres de contrôle* principal et de repli au moyen de liaisons de communication redondantes. L'entité Alpha détermine aussi qu'elle échange les données visées, dans les deux sens, avec le *centre de contrôle* de l'entité Bêta au moyen de l'une ou l'autre de deux liaisons rattachées au *centre de contrôle* principal ou de repli de l'entité Alpha, selon le protocole ICCP (Inter-Control Center Communications Protocol).

Après avoir inventorié les liaisons de communication empruntées par les données visées, l'entité Alpha considère les cinq éléments exigés pour son plan relatif aux communications entre les *centres de contrôle*.

Indication des protections de sécurité

L'entité Alpha doit s'assurer que les moyens de protection sont appliqués conformément au plan exigé par la norme CIP-012. La protection doit aussi réaliser l'objectif de sécurité d'atténuer les risques découlant d'une divulgation non autorisée ou d'une modification non autorisée des données visées pendant leur transmission entre des *centres de contrôle*.

Dans un cas simple où les protections de sécurité sont situées à l'intérieur du *centre de contrôle*, par exemple à l'intérieur du *PSP* du *centre de contrôle*, l'entité Alpha peut utiliser un seul moyen de protection de sécurité pour réaliser l'objectif de sécurité. Dans ce cas, représenté à la figure 2, l'entité Alpha met en place une connexion par réseau privé virtuel (VPN) sur un circuit de communication pour chacune de ses trois liaisons de communication visées par la norme, ainsi qu'une capacité de basculement vers une autre source de données. Afin de satisfaire à l'objectif de sécurité, l'entité Alpha documente le fait que son VPN utilise le protocole IPsec (Internet Protocol Security) avec chiffrement, et que lors d'un basculement vers le *centre de contrôle* de repli, les données empruntent un chemin différent.

Dans des scénarios plus complexes, l'entité Alpha peut devoir combiner plusieurs mesures de sécurité. Par exemple, à la figure 3, l'entité Alpha utilise une combinaison de mesures de sécurité physiques (contrôle des accès physiques) et logiques (chiffrement de la communication comme dans le scénario précédent) pour réaliser l'objectif de sécurité. À la figure 3, le point terminal de chiffrement est situé sur un dispositif de la couche transport (routeur WAN) situé hors du *PSP* du *centre de contrôle* ; l'entité Alpha protège alors

physiquement le câblage et les connexions de transit des données jusqu'à l'intérieur du *PSP* du *centre de contrôle* (alinéa 1.10 de l'exigence E1 de la norme CIP-006). L'équipe de rédaction fait remarquer que la même architecture technique pourrait s'appliquer dans des cas où les responsabilités des entités inscrites sont différentes. Ainsi, si on applique aux figures 2 et 3 un scénario dans lequel l'entité Alpha détient et exploite la liaison de communication et l'équipement des deux points terminaux, il incombe à l'entité Bêta de veiller à ce que le point terminal de la liaison de communication soit protégé. L'entité Bêta fait en sorte que l'équipement du point terminal de la liaison de communication de l'entité Alpha soit protégé en situant le point terminal à l'intérieur d'un *PSP* du *centre de contrôle* ou dans un autre endroit bénéficiant d'une protection physique. Les mesures physiques applicables au *PSP* sont décrites dans la documentation de la norme CIP-006, et il n'y a donc pas lieu de les répéter ici. Les obligations de l'entité Bêta énoncées à l'alinéa 1.1 se trouvent ainsi remplies.

Tous les scénarios qui précèdent ciblent les liaisons de communication. Toutefois, les entités Alpha et Bêta peuvent aussi réaliser l'objectif de sécurité en protégeant les données elles-mêmes plutôt que les liaisons de communication. Dans ce scénario, l'application qui gère l'échange de données entre les *centres de contrôle* peut être capable de protéger directement les données. Une telle protection atténue les risques découlant d'une divulgation non autorisée ou d'une modification non autorisée des données visées, ce qui évite d'avoir à s'en remettre à des services réseau d'un niveau inférieur pour sécuriser les données. Par exemple, les entités Alpha et Bêta peuvent appliquer une protection de sécurité au niveau de la couche application au moyen du protocole SSL/TLS ou d'une autre méthode de chiffrement de la couche application pour l'échange des données visées.

Atténuation des risques découlant d'une perte de la capacité de transmission des données

La figure 2 montre comment l'entité Alpha répond au besoin d'assurer une disponibilité adéquate des données. Le *centre de contrôle* principal de l'entité Alpha compte deux circuits qui communiquent, par l'intermédiaire du « nuage » de l'opérateur de télécommunications, avec le *centre de contrôle* de repli de l'entité Alpha et avec l'entité Bêta. De son côté, l'entité Bêta comporte deux liaisons de communication qui utilisent le même « nuage » pour communiquer avec les *centres de contrôle* primaire et secondaire de l'entité Alpha. Ainsi, chaque entité dispose d'au moins deux chemins vers chacun des *centres de contrôle* avec lesquels elle doit communiquer. Une telle configuration pourrait être confirmée par un schéma de réseau semblable à celui des figures 2 ou 3, qui indique un ou plusieurs segments de communication entre les *centres de contrôle* et qui précise pour chaque segment les moyens de protection mis en œuvre.

Moyens prévus pour entreprendre le rétablissement des liaisons de communication

En conformité avec la norme CIP-009, l'entité Alpha dispose d'un plan complet de rétablissement en cas de sinistre. L'information contenue dans ce plan permet à l'entité Alpha de remettre en fonction non seulement les *systèmes électroniques BES* visés par la norme CIP-009, mais aussi l'infrastructure réseau essentielle pour les communications entre *centres de contrôle*. Afin de répondre à l'objectif de sécurité du rétablissement des liaisons de communication entre *centres de contrôle*, le plan de l'entité Alpha exigé par la norme CIP-012 fait référence au plan de rétablissement exigé par la norme CIP-009, en précisant la partie pertinente de ce plan qui décrit le rétablissement des liaisons de communication nécessaires.

Indication des endroits où l'entité responsable applique les protections de sécurité et de disponibilité

De façon analogue aux explications précédentes portant sur la nature des protections de sécurité, l'endroit où ces protections sont appliquées peut aussi être attesté par un schéma de réseau semblable à ceux des figures 2 et 3.

- La figure 2 montre une situation où la protection de sécurité selon la norme CIP-012 est appliquée dans le modèle de référence de l'entité Alpha lorsqu'un seul tunnel chiffré est utilisé pour mettre en œuvre la protection requise. L'entité Alpha indique qu'une protection de sécurité est appliquée dans chacun de ses *centres de contrôle* à l'interface Ethernet externe du routeur WAN. Dans cet exemple, l'entité Bêta dispose de liaisons redondantes, par l'entremise de l'opérateur de télécommunications, vers les *centres de contrôle* primaire et secondaire de l'entité Alpha. À titre purement indicatif, la figure 2 montre aussi à quel endroit l'entité Bêta applique sa protection de sécurité ; rappelons toutefois qu'il n'incombe pas à l'entité Alpha d'indiquer à quel endroit l'entité Bêta a appliqué ses protections de sécurité.
- Afin de comprendre l'application de la protection de sécurité dans un contexte où se pose la question de savoir qui contrôle la liaison de communication, il peut être utile d'indiquer non seulement l'endroit où est appliquée la protection de sécurité exigée par la norme CIP-012, mais aussi l'emplacement du point de démarcation de l'opérateur de télécommunications (point de démarcation télécoms). La figure 3 en montre un exemple, où ce point de démarcation peut ne pas être situé dans le *PSP* du *centre de contrôle* et où l'entité Alpha, compte tenu de l'environnement lié à ce scénario, a mis en œuvre une combinaison de mesures de sécurité pour satisfaire à la norme CIP-012. Dans ce scénario, l'entité Alpha indique qu'elle a utilisé une protection physique pour son routeur WAN, et appliqué une protection logique (chiffrement) au routeur WAN. L'entité Alpha indique aussi que le point de démarcation télécoms est situé à un endroit précis dans le câblage de télécommunications relié au routeur WAN de l'entité Alpha, par exemple à un bloc de raccordement. À la figure 3, le point de démarcation télécoms est situé dans le même local que le routeur WAN. Les points de démarcation télécoms sont indiqués sur le schéma pour plus de clarté.
- Les figures 2 et 3 présentent un exemple dans lequel les obligations opérationnelles de la totalité de la liaison de communication, y compris les deux points terminaux, incombent à l'entité Alpha. Dans ce cas, l'entité Bêta peut être responsable de veiller à ce que le point terminal de la liaison de communication soit bien situé dans son *centre de contrôle*. L'entité Bêta fait en sorte que l'équipement du point terminal de la liaison de communication de l'entité Alpha se trouve à l'intérieur du *centre de contrôle* en situant le point terminal à l'intérieur d'un *PSP* ou dans un autre endroit bénéficiant d'une protection physique. La documentation fournie pour l'alinéa 1.1 par l'entité Bêta répond à cette obligation.
- Le scénario décrit ci-dessus, axé sur les données, est moins intuitif pour ce qui est d'indiquer à quel endroit la protection de sécurité est appliquée par l'entité Alpha. Si la protection est mise en œuvre au niveau de la couche application, l'entité Alpha pourrait raisonnablement désigner l'application ou le service qui met en œuvre la protection comme étant l'endroit où la protection de sécurité est appliquée.
- L'atténuation du risque d'une perte de la capacité de transmission de données peut être attestée au moyen de schémas de réseau montrant divers circuits, systèmes

redondants ou détails d'application, ou au moyen de toute autre documentation décrivant les protections utilisées.

Indication des responsabilités si les *centres de contrôle* sont détenus ou exploités par des entités responsables différentes

Les entités Alpha et Bêta peuvent déterminer qu'elles sont chacune responsables d'une des extrémités de la configuration VPN à leurs routeurs WAN respectifs. Les deux entités peuvent convenir d'une clé prépartagée (PSK) de 30 caractères pour l'authentification IPSec.

Plutôt qu'une clé prépartagée, les entités Alpha et Bêta peuvent décider d'utiliser des certificats numériques pour l'authentification IPSec fournis par une autorité de certification de confiance. Dans ce scénario, les entités Alpha et Bêta s'entendraient pour désigner la partie responsable des arrangements avec l'autorité de certification.

Dans l'exemple où la liaison de communication et les équipements de point terminal appartiennent à l'entité Alpha, les entités doivent préciser la propriété ou les responsabilités dans leurs plans respectifs pour satisfaire à l'alinéa 1.5. Exemples non limitatifs : lettre précisant la propriété ou la responsabilité, copie d'un contrat précisant la propriété ou les responsabilités, extrait d'une entente opérationnelle ou d'un manuel précisant la propriété ou la responsabilité. Cette documentation doit aussi préciser les rôles ou responsabilités quant au maintien de la disponibilité des circuits, des systèmes ou des flux de données.

Modèle de référence

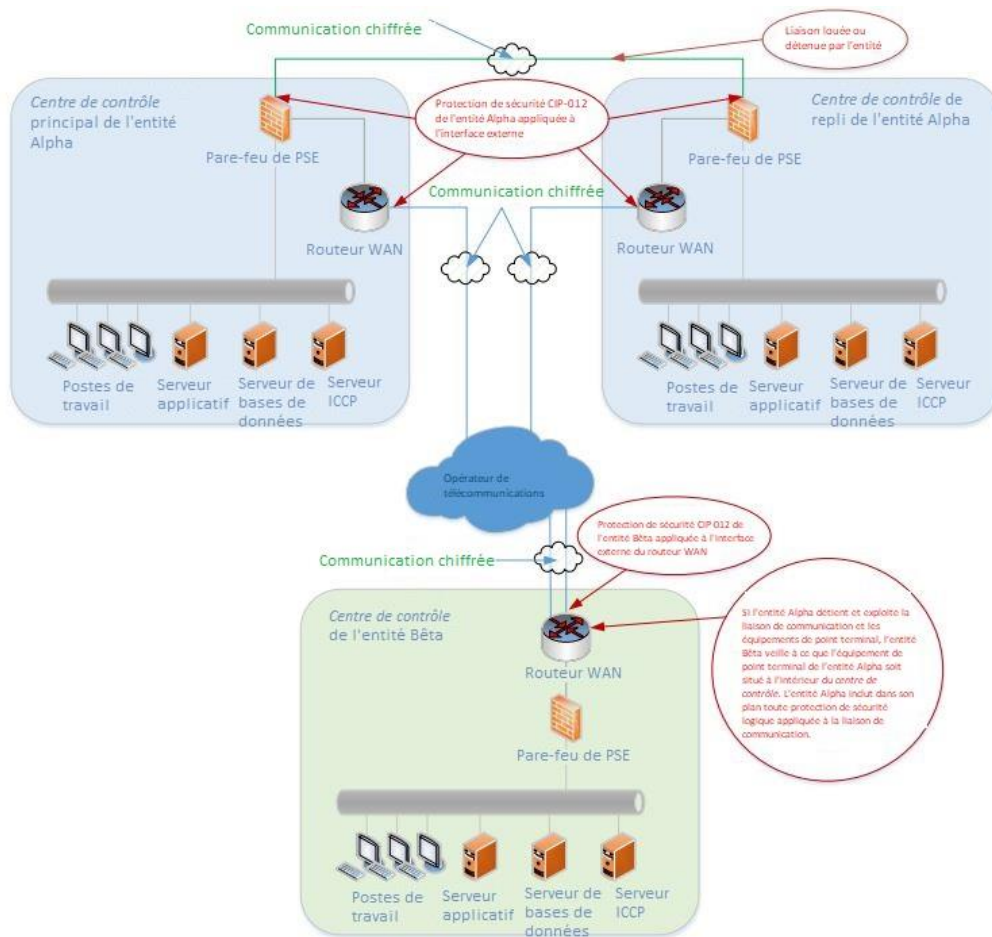


Figure 2 : Schéma du réseau et indication des endroits où la protection logique est appliquée

Modèle de référence

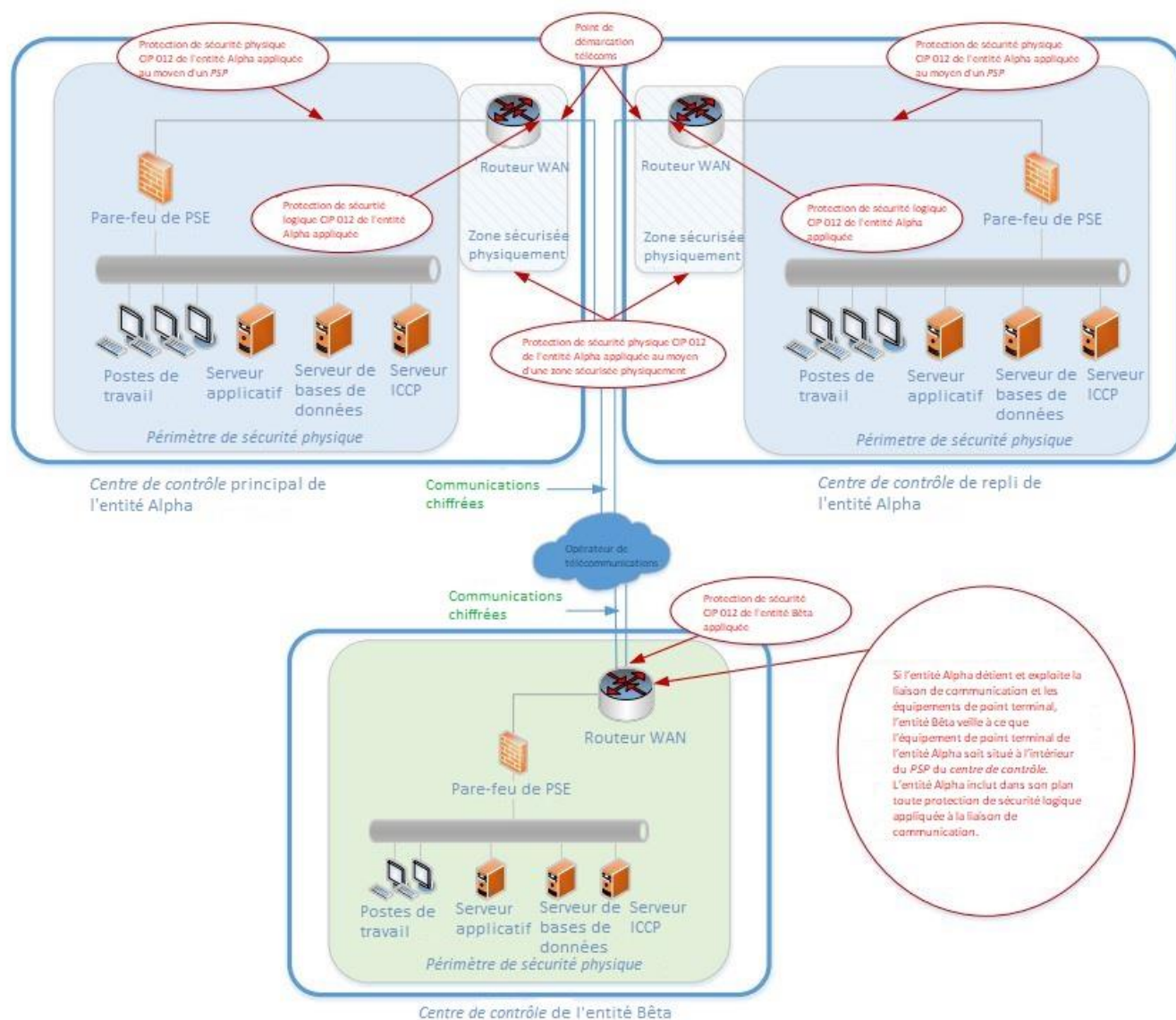


Figure 3 : Schéma de réseau illustrant une combinaison de moyens de protection CIP 012

Références

Énumération des types de faiblesse courants (CWE™) de MITRE Corporation

<https://cwe.mitre.org/data/definitions/327.html>

Normes et directives cryptographiques

<https://csrc.nist.gov/Projects/Cryptographic-Standards-and-Guidelines>

Publication spéciale 800-175B du NIST :

Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms

<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-175B.pdf>

Guide de cryptographie

https://www.owasp.org/index.php/Guide_to_Cryptography#Symmetric_Cryptography