Justification technique et Guide d'application de la norme CIP-012-1 (version française)

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Cybersécurité – Communications entre centres de contrôle

Justification technique de la norme de fiabilité CIP-012-1

Août 2018

RELIABILITY | ACCOUNTABILITY



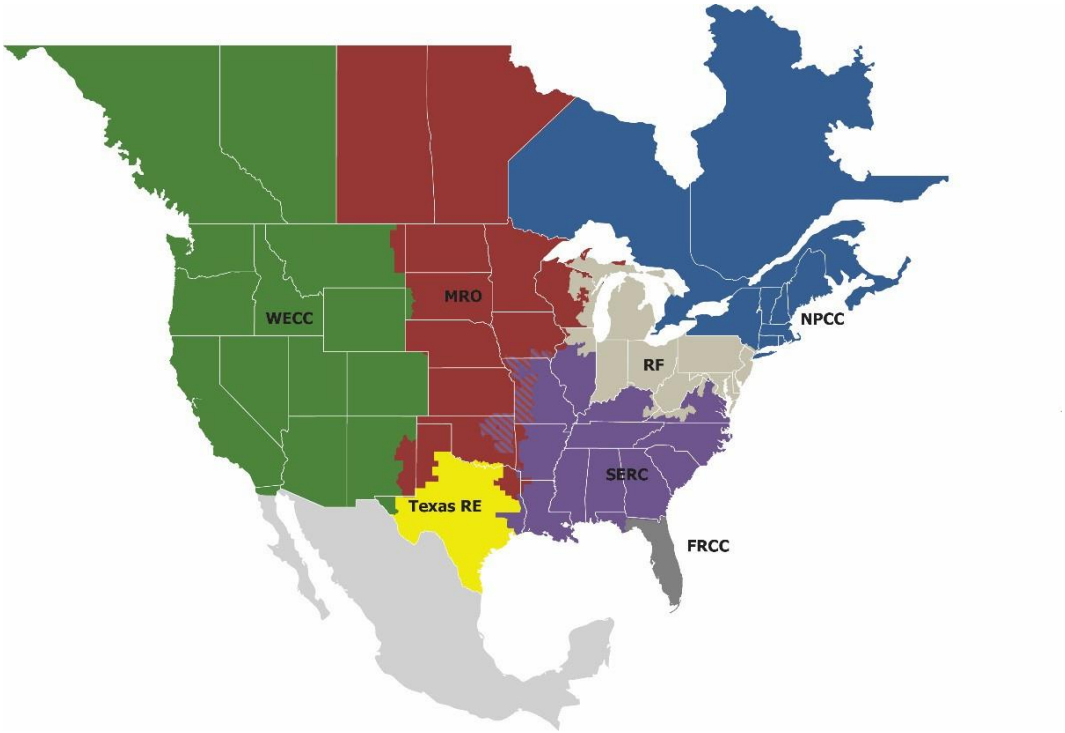

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table des matières

Préface

L'organisme de fiabilité électrique (ERO), qui regroupe la North American Electric Reliability Corporation (NERC) et les sept entités régionales (RE), a pour mission d'assurer la fiabilité et la sécurité du *système électrique interconnecté* (*BPS*) nord-américain, en travaillant à réduire de façon efficace et efficiente les risques pour la fiabilité et la sécurité du réseau électrique.

Le BPS nord-américain est divisé en sept territoires gérés par les RE, comme l'indiquent 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.



FRCC	Florida Reliability Coordinating Council
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

Ce document expose la justification technique de la norme de fiabilité CIP-012-1 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-012-1*, n'est pas une norme de fiabilité et son contenu ne doit donc pas être considéré comme obligatoire et exécutoire.

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 (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 responsables[1] 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 demande 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 la norme CIP-006 ne seraient pas appropriées. 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 exigée à l'alinéa 1.10 de l'exigence E1 de la norme CIP-006-6. 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-006-6, il protège les composants de communication non programmables situés à l'intérieur d'un même *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.

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 réaliser l'objectif de sécurité 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 *BA* ou de *TOP*, cependant, n'ont pas à être 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-après.

1. Dans le contexte des normes CIP, le terme « entité responsable » désigne les entités inscrites selon les modalités de normes CIP.

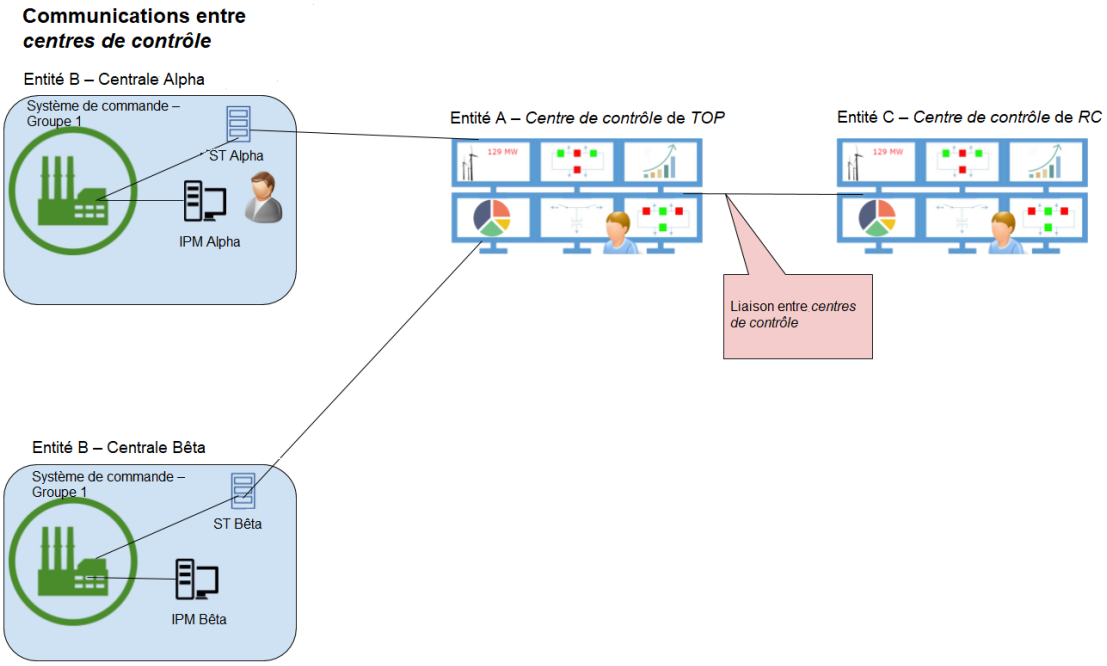


Figure 1

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.

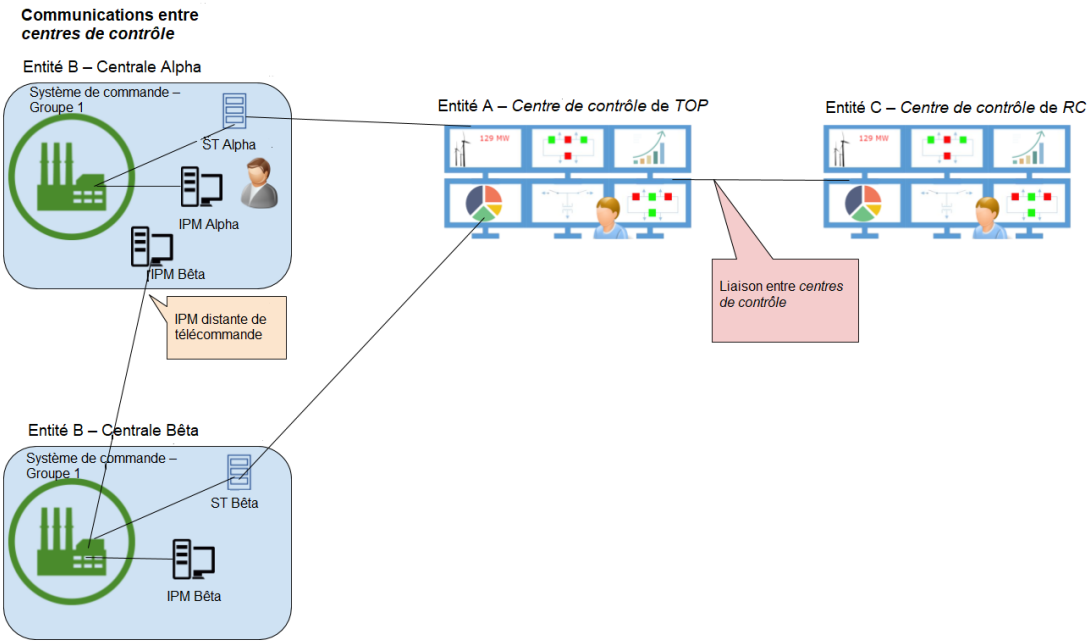


Figure 2

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.

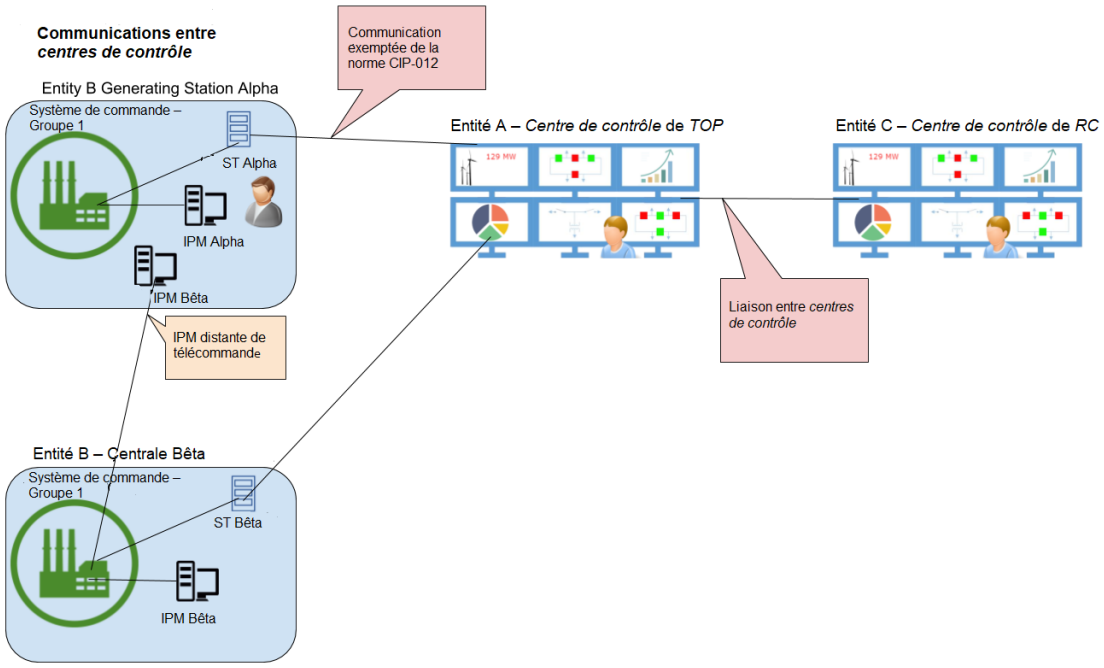


Figure 3

Bien que rien n'ait changé entre ces entités, cette proximité des IPM a pour conséquence 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, à moins d'une exemption. Deux IPM ayant été mises en présence dans le même local, cette nouvelle norme CIP s'appliquerait aux deux entités.

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 *TO* et aux *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 A.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 de communication peut se faire avec des technologies et des protocoles de communication existants plus anciens.

L'exemption de la section A.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 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 cet emplacement.

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

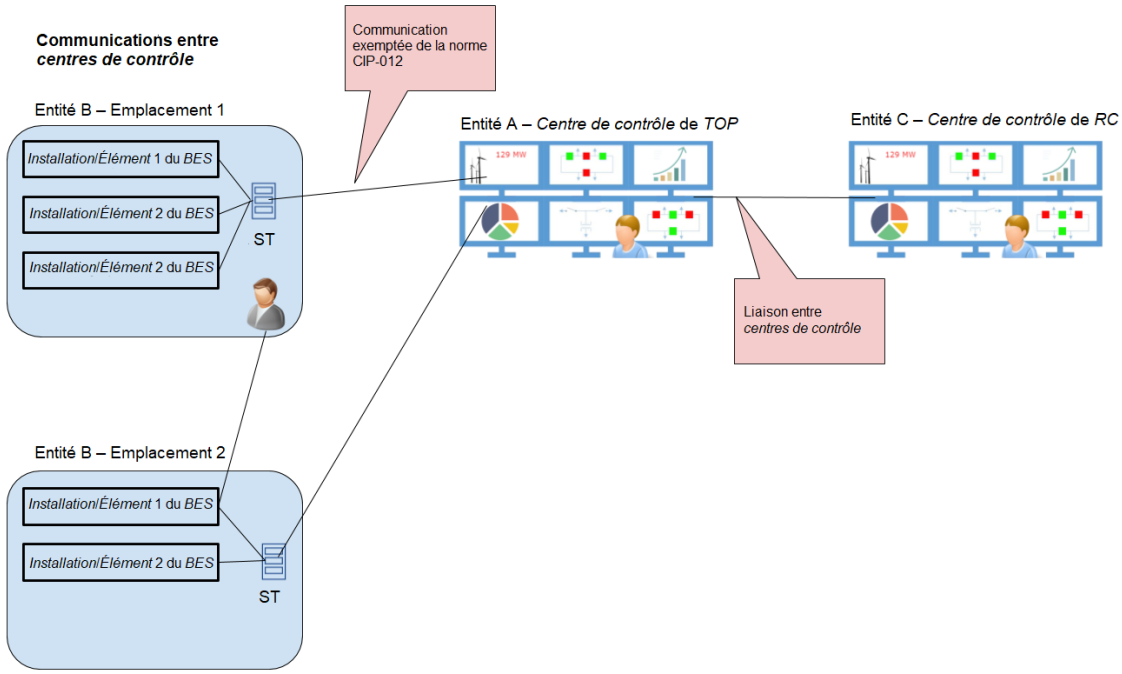


Figure 4

À la figure 4, chaque emplacement communique uniquement les données d'*évaluation en temps réel* ou de surveillance en *temps réel* relatives à ce seul emplacement. La communication provenant de l'emplacement 1 de l'entité B est alors exemptée de la norme CIP-012-1.

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 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. 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 de protection 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 les endroits où l'entité responsable applique les moyens de protection des données d'*évaluation en temps réel* et de surveillance en *temps réel* pendant leur transmission entre des *centres de contrôle* ; et

1.3 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 de protection des données d'*évaluation en temps réel* et de surveillance en *temps réel* pendant leur transmission entre ces *centres de contrôle.*

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, l'ordre d'énumération des trois alinéas de l'exigence ne revêt aucune signification particulière.

Concepts de confidentialité et d'intégrité

Pour l'équipe de rédaction, la norme CIP-012-1 vise à assurer la confidentialité et l'intégrité 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 la divulgation non autorisée (confidentialité) et la modification non autorisée (intégrité). Pour cette norme, l'équipe de rédaction se réfère aux définitions des termes « confidentialité » et « intégrité » 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[2] ».
- 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[3] ».

L'équipe de rédaction rappelle que la disponibilité de ces données est déjà exigée par les obligations de performance des normes de fiabilité concernant l'exploitation et la planification. La norme CIP-012-1 a été rédigée de manière à protéger les données pendant leur transmission. L'équipe de rédaction rappelle aussi que ces données résident à

2. Publication spéciale 800-53A (révision 4) du NIST, page B-3.
3. Publication spéciale 800-53A (révision 4) du NIST, page B-6.

l'intérieur de *systèmes électroniques BES*, et qu'à ce titre, elles sont protégées par les normes CIP-003-6 à CIP-011-2, sauf pendant leur transmission.

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-012-1 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-012-1 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-012-1 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 rendues 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.

Détermination 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 n'a pas spécifié à quels endroits les moyens de protection exigés par la norme CIP-012-1 doivent être appliqués ; les entités responsables ont ainsi toute latitude pour implanter les mécanismes de sécurité de la manière la mieux adaptée 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* ou à proximité, en présence d'un *périmètre de sécurité électronique*, 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*, *actif électronique protégé* ou *système de contrôle ou de surveillance des accès électroniques* (*EACMS*). La désignation d'un *actif électronique* comme étant l'endroit où un moyen de protection est appliqué n'a pas pour effet d'étendre à ce type d'actif l'applicabilité des normes de cybersécurité CIP-002 à CIP-011.

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 ; elle ne devrait pas être tenue d'indiquer à quels endroits une entité voisine a appliqué ses moyens de protection dans les installations qui lui sont propres. Cependant, 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 à l'alinéa 1.2 de l'exigence E1 de la norme CIP-012-1 et l'indication des responsabilités des entités responsables à l'alinéa 1.3 de cette même exigence.

Propriété des *centres de contrôle*

Les exigences de la norme 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. Les exigences n'imposent 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. Cet exemple 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.

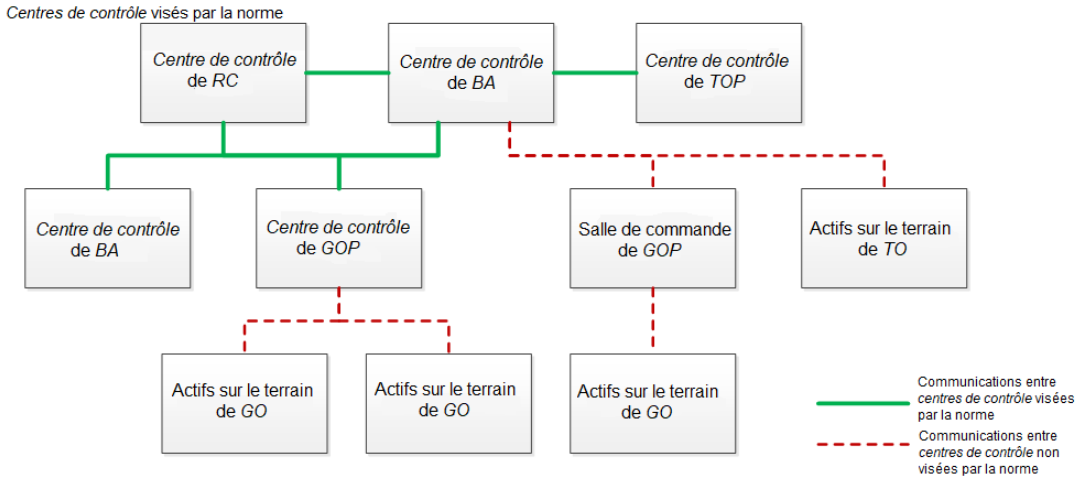


Figure 5 : Modèle de référence présenté à titre d'exemple (ne couvre pas tous les scénarios possibles)

L'équipe de rédaction a prévu l'alinéa 1.3 pour les situations où plusieurs entités inscrites sont concernées par la protection de données transmises entre *centres de contrôle*. L'alinéa 1.3 présente un mécanisme qui oblige à préciser les responsabilités des différentes entités dans l'application des moyens de protection. Cet alinéa vise à prévenir les problèmes de sécurité 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 de sécurité. 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 *centres de contrôle* exploités par des entités responsables différentes. Les moyens de protection appliqués par chaque entité en vue de la conformité avec les alinéas 1.1 et 1.2 du plan devraient être en corrélation avec les responsabilités documentées à l'alinéa 1.3 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*

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Document entériné par l'ERO

Cybersécurité – Communications entre *centres de contrôle*

Guide d'application de la norme CIP-012-1

FIABILITÉ | RÉSILIENCE | SÉCURITÉ




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

Table des matières

Introduction

L'équipe de rédaction des normes du projet 2016-02 a produit le présent Guide d'application afin de présenter des exemples de démarches de mise en conformité avec la norme CIP-012-1. 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]

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-012-1*.

Contexte

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 des normes 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).

L'équipe de rédaction a formulé les exigences de la norme de manière à accorder aux entités responsables la latitude voulue pour protéger les données d'*évaluation en temps réel* et de surveillance en *temps réel* elles-mêmes, les liaisons de communication par lesquelles ces données transitent, ou une combinaison des deux, de manière à réaliser l'objectif de sécurité en tenant compte des capacités de l'environnement opérationnel des entités responsables.

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

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 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. 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 de protection 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. les endroits où l'entité responsable applique les moyens de protection des données d'*évaluation en temps réel* et de surveillance en *temps réel* pendant leur transmission entre des *centres de contrôle* ; et

1.3. 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 de protection des données d'*évaluation en temps réel* et de surveillance en *temps réel* pendant leur transmission entre ces *centres de contrôle*.

Généralités

Élaboration du plan

Comme l'explique le document *Justification technique de la norme de fiabilité CIP-012-1,* 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. 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. Par exemple, elle 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*. Une entité responsable 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 comprennent les éléments spécifiés aux alinéas 1.1, 1.2 et 1.3 de l'exigence E1.

Les entités responsables doivent prendre note que la définition de *centre de contrôle* inclut les « centres informatiques connexes ».

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* et de surveillance en *temps réel* de la part de leurs *RC*, *BA* et *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 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*.

Indication des moyens de protection (E1.1)

Les entités ont toute latitude pour déterminer et choisir les moyens de protection 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 moyens de protection pourraient être de type logique ou physique, ou encore combiner ces deux types. Pour déterminer les moyens de protection, 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. 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 moyens de protection. 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 moyens de protection, 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.

Indication des endroits où l'entité responsable applique les moyens de protection (E1.2)

Pour déterminer à quels endroits appliquer les moyens de protection, l'entité responsable doit prendre en compte son environnement. Une approche consiste à mettre en œuvre la sécurité 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'appliquer les moyens de protection 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 moyens de protection appliqués 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 *PSP* ou à tout autre endroit bénéficiant d'une protection physique.

L'indication des endroits où l'entité responsable applique les moyens de protection pourrait prendre la forme d'une liste ou d'un schéma de *centre de contrôle* précisant les mesures de sécurité physiques ou logiques. 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 moyens de protection de la norme CIP-012 sont appliqués.

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 moyens de protection. 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 appliqués les moyens de protection aux deux extrémités de la liaison.

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 appliqués les moyens de protection aux deux extrémités de la liaison.

Indication des responsabilités si les *centres de contrôle* sont détenus ou exploités par des entités responsables différentes (E1.3)

La section *Propriété des centres de contrôle* du document *Justification technique de la norme de fiabilité CIP-012-1* 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 différentes entités responsables ont leurs particularités. Il n'existe donc pas de formule universelle pour établir les responsabilités quant à l'application des moyens de protection pour la transmission des données d'*évaluation en temps réel* et de surveillance en *temps réel* entre *centres de contrôle*.

De même, la mise en œuvre des responsabilités pourrait être attestée de diverses manières : par exemple une procédure commune, un protocole d'entente ou un procès-verbal de réunion qui documente le partage des responsabilités entre les deux parties.

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 *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.

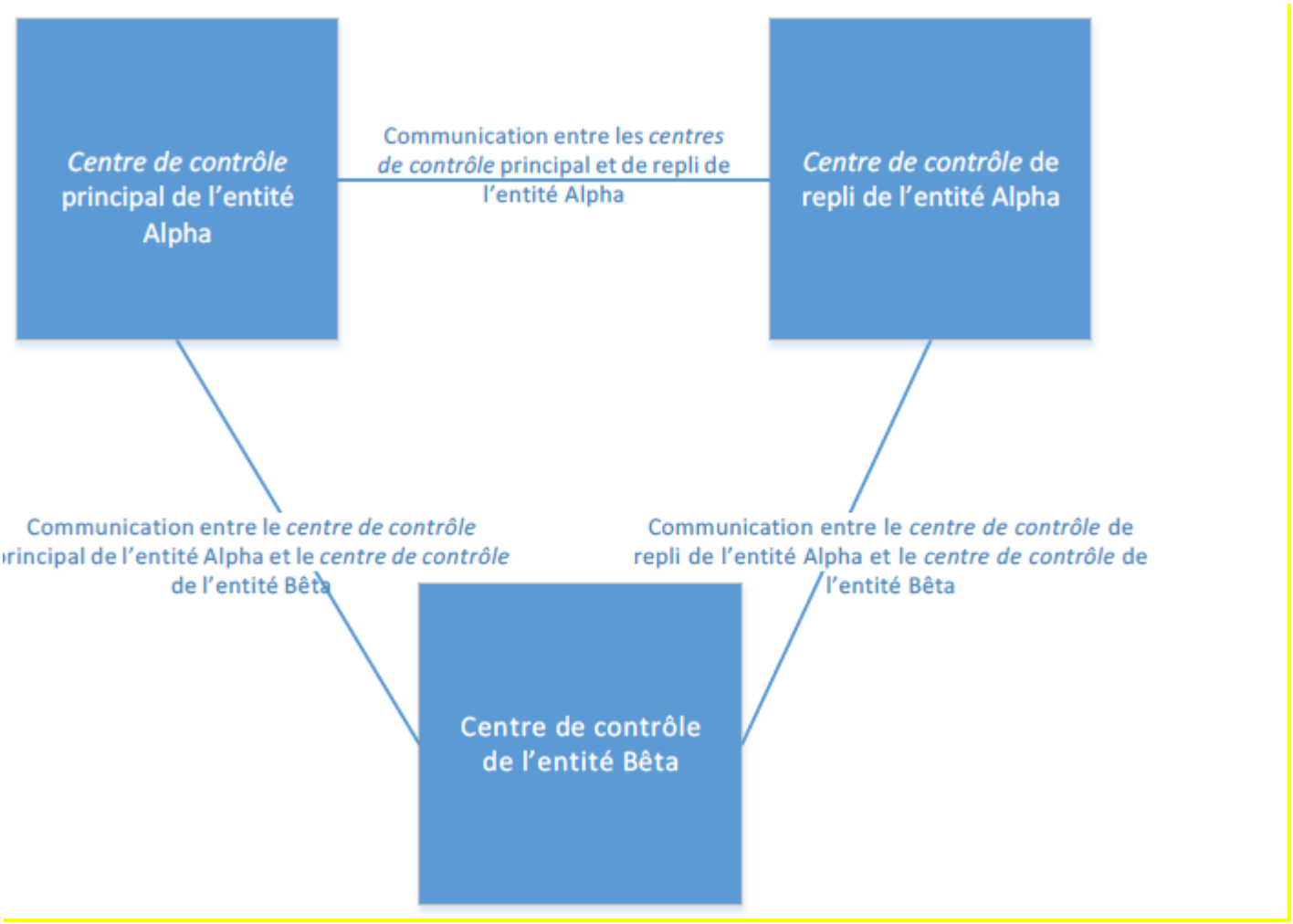


Figure 1 : Schéma fonctionnel de haut niveau des centres de contrôle du modèle de référence

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-012-1. 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-012-1.

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-003-3 et IRO-010-2 pour les données d'*évaluation en temps réel* et de surveillance en *temps réel*. 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 d'une seule liaison de communication. 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 maintenant les trois éléments exigés pour son plan relatif aux communications entre les *centres de contrôle*.

Indication des moyens de protection

L'entité Alpha doit s'assurer que la protection est appliquée conformément au plan exigé par la norme CIP-012-1. 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*. L'application des moyens de protection 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 précise pour chaque segment les moyens de protection mis en œuvre.

Dans un cas simple où les moyens de protection sont situés 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 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. 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.

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 à l'extérieur du *centre de contrôle* ; l'entité Alpha protège alors physiquement le câblage et les connexions de transit des données jusqu'à l'intérieur du *centre de contrôle*. 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 se trouve à l'intérieur de 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* du *centre de contrôle*. Les mesures physiques applicables au *PSP* sont décrites dans la documentation de la norme CIP-006, et il n'est donc pas pertinent de les répéter ici. Les obligations de l'entité Bêta liées aux alinéas 1.1 et 1.2 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 de niveau inférieur pour sécuriser les données. Par exemple, les entités Alpha et Bêta peuvent appliquer une protection 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.

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

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

- La figure 2 montre une situation où les moyens de protection de la norme CIP-012-1 sont appliqués 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 est appliquée dans chacun de ses *centres de contrôle* à l'interface Ethernet externe du routeur WAN. À des fins d'illustration, la figure 2 montre aussi à quel endroit l'entité Bêta applique sa protection ; rappelons toutefois qu'il n'incombe pas à l'entité Alpha d'indiquer à quel endroit l'entité Bêta a appliqué ses moyens de protection.
- Afin de comprendre l'application des moyens de protection 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 la norme CIP-012-1, 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 le point de démarcation télécoms peut ne pas être situé dans le *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-012-1. Dans ce scénario, l'entité Alpha indique qu'elle a utilisé des moyens de protection physiques pour son *PSP*, qui englobe son routeur WAN, et appliqué une protection logique (chiffrement) au routeur WAN. L'entité Alpha détermine aussi que le point de démarcation télécoms est situé à un endroit précis sur 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, mais ne font pas partie du plan.
- 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* du *centre de contrôle*. 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 les moyens de protection sont appliqués 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 les moyens de protection sont appliqués.

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

L'entité Alpha et l'entité 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 1.3. 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.

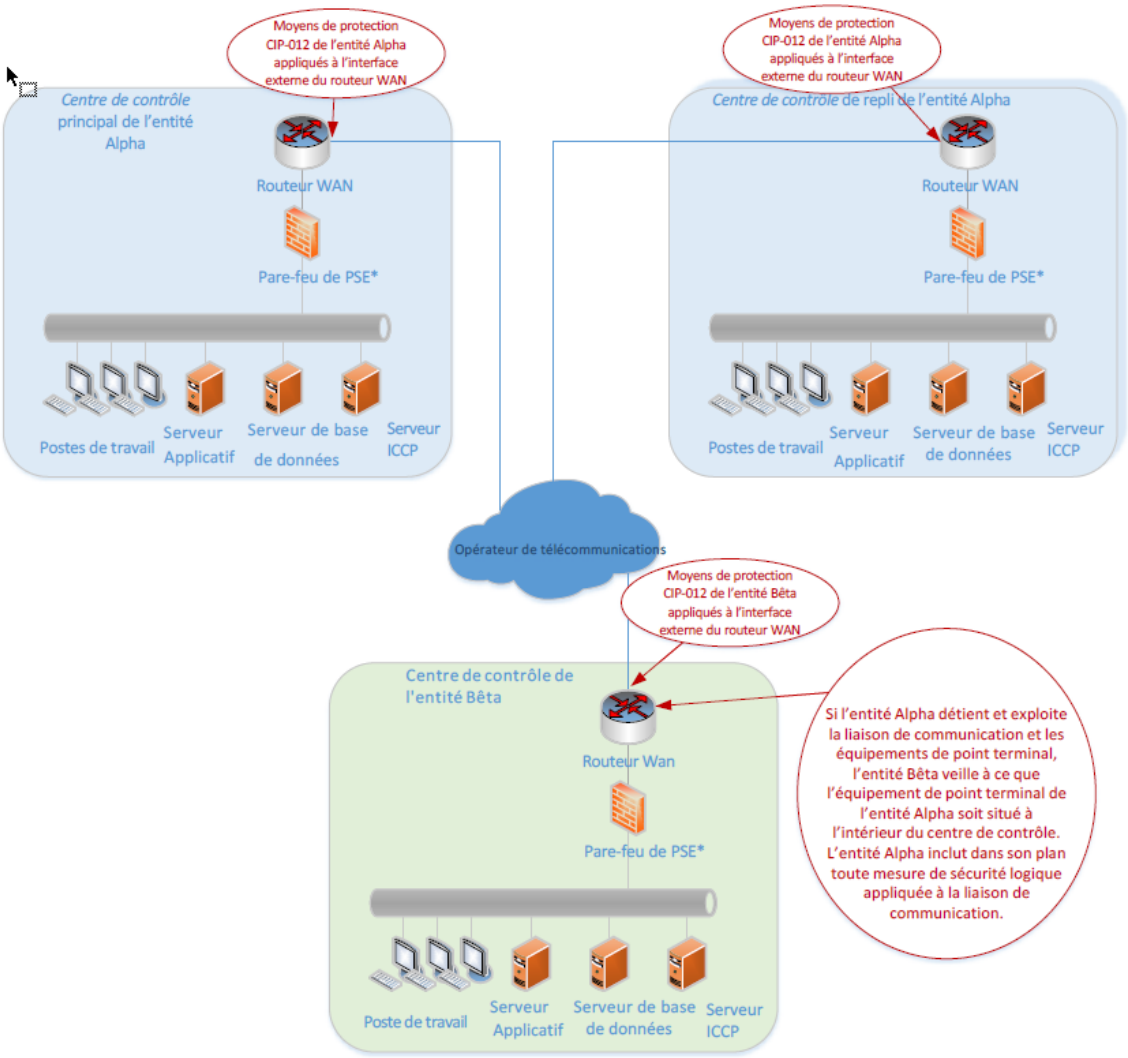


Figure 2 : Schéma du réseau et indication de l'endroit où les moyens de protection sont appliqués

*PSE : périmètre de sécurité électronique

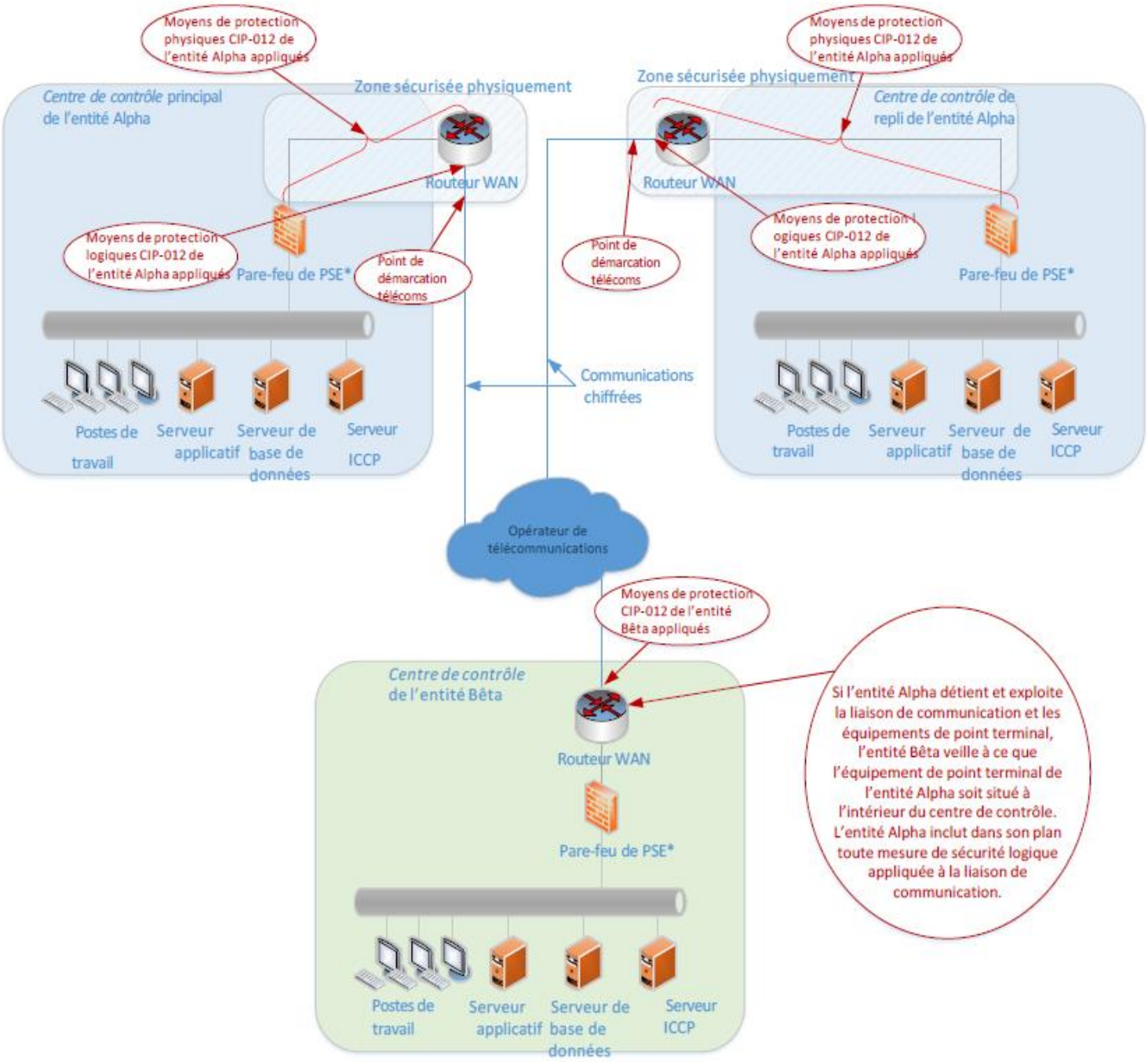


Figure 3 : Schéma de réseau illustrant une combinaison de moyens de protection CIP-012-1

*PSE : périmètre de sécurité électronique

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