

Cybersécurité – Mécanismes de gestion de la sécurité

Justification technique de la norme de
fiabilité CIP-003-9

Octobre 2022

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
Justification technique de la norme de fiabilité CIP-003-9	4
Introduction.....	4
Contexte	4
Remarques sur les sections 3 et 6.....	5
Justification de la section 6 de l'annexe 1 (exigence E2)	6
Section 6.1 de l'annexe 1 – Détermination des accès électroniques distants des fournisseurs	7
Section 6.2 de l'annexe 1 – Désactivation des accès électroniques distants des fournisseurs	7
Section 6.3 de l'annexe 1 – Détection de communications entrantes et sortantes malveillantes avérées ou présumées	8

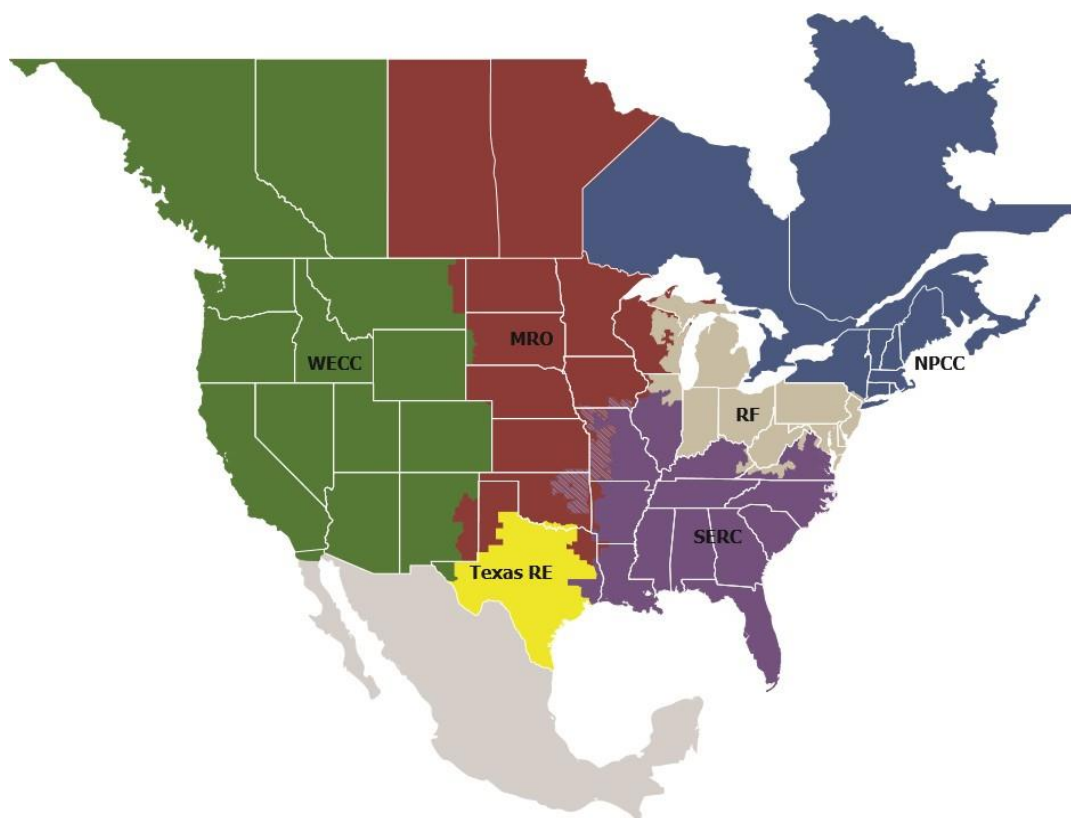
Préface

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

Fiabilité | Résilience | Sécurité

Parce que près de 400 millions de citoyens en Amérique du Nord comptent sur nous

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



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

Justification technique de la norme de fiabilité CIP-003-9

Introduction

Ce document expose la justification technique de la norme de fiabilité CIP-003-9 proposée. Il vise à guider les parties prenantes ainsi que l'ERO dans la compréhension des enjeux technologiques et des exigences techniques de cette *norme de fiabilité*. Le présent document de justification technique n'est pas une *norme de fiabilité* et son contenu ne doit donc pas être considéré comme obligatoire et exécutoire.

Les mises à jour du présent document reflètent désormais les intentions de l'équipe de rédaction des révisions relatives à la gestion des risques de cybersécurité dans la chaîne d'approvisionnement pour les systèmes électroniques BES à impact faible (projet 2020-03) quant aux changements apportés aux exigences.

Contexte

Dans son rapport final¹ accepté par le Conseil d'administration de la NERC en mai 2019, la NERC a documenté les résultats de l'évaluation des risques dans la chaîne d'approvisionnement associés à certaines catégories d'actifs non actuellement assujetties aux normes sur la chaîne d'approvisionnement et a recommandé des mesures concernant ces risques. Le personnel de la NERC a recommandé la réalisation d'autres études afin de déterminer si la nouvelle information justifie la révision des normes pour y inclure les *systèmes électroniques BES* à impact faible avec connectivité externe, en transmettant une demande de données ou d'information conformément à la section 1600 des règles de procédure de la NERC.

Le Conseil d'administration a approuvé la publication officielle de cette demande de données le 15 août 2019. La NERC a recueilli les données entre le 19 août et le 3 octobre 2019. Un rapport final sur l'évaluation des risques dans la chaîne d'approvisionnement, intitulé *Supply Chain Risk Assessment*, a été publié en décembre 2019. Il recommandait la modification des normes sur la chaîne d'approvisionnement afin d'y inclure les *systèmes électroniques BES* à faible impact avec connectivité pour accès électronique distant. De plus, les commentaires de l'industrie concernant cette recommandation, formulés au moyen du mécanisme d'aide à l'élaboration des politiques du comité des représentants des membres, ont été reçus lors de la réunion du Conseil d'administration de la NERC qui s'est tenue en février 2020.

Après l'examen de ces commentaires, le Conseil d'administration de la NERC a adopté une résolution² visant à mettre en route un projet de modification de la norme de fiabilité CIP-003-8 pour y inclure des politiques stipulant que les *systèmes électroniques BES* à faible impact doivent disposer de moyens pour : 1) détecter les communications entrantes et sortantes malveillantes avérées ou présumées ; 2) déterminer l'ouverture de sessions d'accès distant des fournisseurs ; et 3) désactiver les accès distants des fournisseurs.

1. Supply Chain Risk Assessment (nerc.com)

2. FINAL_Minutes_BOT_Open_Meeting_February_2020.pdf (nerc.com)

Remarques sur les sections 3 et 6

Lors de la formulation du texte visé par la présente demande d'autorisation de norme (SAR), l'équipe de rédaction a tenu compte d'un grand nombre de variables et de commentaires en vue de rédiger des exigences limpides, concises et pertinentes. L'équipe de rédaction a examiné la portée et la diversité des éléments suivants : la taille, les fonctions, les organisations, les systèmes et les configurations des entités, les processus opérationnels des entités, l'accès distant, l'accès électronique local, les architectures et les technologies employées pour l'accès distant, et les protocoles relatifs au chemin et à la communication des données. L'équipe de rédaction s'est penchée sur les systèmes utilisés pour l'accès électronique, sur l'accès électronique distant par rapport à l'accès électronique local, sur les comptes et les privilèges d'accès des fournisseurs, ainsi que sur les délais optimaux pour établir, identifier, déterminer et désactiver ou interrompre les accès électronique des fournisseurs.

L'équipe de rédaction a passé en revue les commentaires formulés par l'industrie et les formulations proposées pour le texte de la norme, a examiné les normes existantes, et a débattu et délibéré sur les options et sur leurs incidences et valeurs interprétatives potentielles pour l'industrie. L'équipe de rédaction reconnaît qu'une entité et son personnel pourraient employer le même processus ou système ou la même technologie (pour l'accès électronique des fournisseurs) ou encore que des entités pourraient utiliser des processus, des systèmes ou des technologies distincts pour gérer l'accès électronique des fournisseurs. L'équipe de rédaction a également examiné les systèmes et *actifs électroniques* détenus par des fournisseurs et dont l'usage est autorisé dans les réseaux des entités, par opposition aux systèmes et *actifs électroniques* détenus par des entités et qui sont utilisés par des fournisseurs aux fins d'accès électronique distant. En raison de la diversité mentionnée précédemment, l'équipe de rédaction s'est préoccupée avant tout de permettre aux entités de déterminer leurs propres risques liés à l'accès électronique distant des fournisseurs et d'élaborer des mécanismes et des plans pour définir et mettre en œuvre des mesures de sécurité visant à tenir compte de ces risques.

Lors de l'examen des commentaires formulés par l'industrie, l'équipe de rédaction a relevé d'éventuels termes à définir, en a discuté et a envisagé leur utilisation, pour en venir aux conclusions suivantes :

1. Accès électronique distant : L'équipe de rédaction a envisagé de définir le terme « accès distant » ou de préciser ce qui distingue l'« accès distant » de l'« accès électronique distant » et l'« accès local distant » de l'« accès hors site distant », ou les deux possibilités. Dans le terme « accès électronique distant », il est précisé que l'accès distant est obtenu par un moyen non physique, ce qui correspond à la définition figurant actuellement dans d'autres normes CIP pour ce même terme.
2. *Accès distant interactif* : L'équipe de rédaction a évité d'employer la définition figurant actuellement dans le glossaire de la NERC afin que les exigences relatives aux actifs et systèmes à impact élevé et moyen ne soient pas imposées aux actifs et systèmes à faible impact.
3. Actif : L'équipe de rédaction a évité d'utiliser le terme « actif » en raison de possibles conséquences imprévues. L'emploi de ce terme pourrait imposer aux entités d'autres exigences, c'est-à-dire leur demander de déterminer, de répertorier et de documenter les situations où un accès est « actif » ou non.

4. Lecture seule : L'équipe de rédaction a évité d'utiliser le terme « lecture seule » en raison de possibles conséquences imprévues. L'emploi de ce terme pourrait imposer aux entités d'autres exigences, c'est-à-dire leur demander de déterminer et de documenter les systèmes et les processus en lecture seule ou en lecture et écriture, ainsi que l'emplacement et le moment où ont lieu les accès en lecture seule.
5. Fournisseur : Les compléments de la norme CIP-013³ abordent l'emploi du terme « fournisseur » dans le contexte des *systèmes électroniques BES* à impact moyen et élevé applicables. L'équipe de rédaction a évité de définir le terme « fournisseur » dans les normes visant les systèmes à impact faible afin de prévenir tout conflit pour les entités comportant des systèmes à impact faible, moyen et élevé.

Le texte de la norme a été rédigé de manière à donner aux entités la possibilité d'établir des processus de définition et de gestion de l'accès électronique distant des fournisseurs adaptés à leurs propres politiques, processus, systèmes, configurations, organisations, activités d'exploitation et *installations* du *BES*. Il permet aussi aux entités de définir où et comment se produisent les accès électroniques distants des fournisseurs ainsi que les méthodes et les délais idéaux pour autoriser, établir et désactiver ces accès.

L'équipe de rédaction a convenu de conserver la section 3 de l'annexe 1 portant sur l'exigence E2 de la version précédente de la norme et a ajouté la section 6 afin de traiter plus précisément de l'accès électronique distant à faible impact des fournisseurs ainsi que des communications de données entrantes et sortantes avec des fournisseurs qui s'avèrent malveillantes. Conformément à la SAR, l'équipe de rédaction n'a pas ajouté la connectivité par lien commuté qui est mentionnée à la section 3.2.

La norme exige que l'entité élabore et mette en place un ou plusieurs processus pour constater l'accès électronique distant des fournisseurs et dispose d'une ou de plusieurs méthodes pour désactiver l'accès électronique distant des fournisseurs ainsi que de méthodes pour détecter les communications entrantes et sortantes malveillantes avérées ou présumées avec des fournisseurs.

Afin d'établir et de désactiver les communications distantes électroniques des fournisseurs, les entités peuvent choisir de définir des systèmes, des applications ou des configurations utilisés par ceux-ci, des comptes et des privilèges, des trajets de communication de données de réseau ou encore des processus physiques. La section 6 offre la souplesse voulue pour tenir compte des nombreux types de configurations d'accès électronique distant de fournisseurs et pour assurer la gestion des risques liés aux accès.

Justification de la section 6 de l'annexe 1 (exigence E2)

L'exigence E2 demande aux entités d'élaborer et de mettre en œuvre un ou plusieurs plans de cybersécurité afin de réaliser des objectifs de sécurité précis pour leurs actifs comportant un ou plusieurs *systèmes électroniques BES* à impact faible. En février 2020, le Conseil d'administration de la NERC a approuvé la mise en route d'un projet de modification de la norme de fiabilité CIP-003-8 pour y inclure des politiques stipulant que les *systèmes électroniques BES* à faible impact doivent disposer de moyens pour : 1) détecter des communications entrantes et sortantes malveillantes avérées ou présumées ; 2) déterminer l'ouverture de sessions d'accès électroniques distants des fournisseurs ; et 3) désactiver les accès électroniques distants des fournisseurs au besoin.

3. Justification technique de la norme CIP-013

Selon le rapport de la NERC intitulé [Supply Chain Risk Assessment – Analysis of Data Collected under the NERC Rules of Procedure Section 1600 Data Request](#), publié en décembre 2019, environ 66 % de la part des entités détenant des systèmes électroniques BES à faible impact qui ont répondu à la demande de données conformément à la section 1600 (cette part s'élevant à 87 %) ont une connectivité externe qui donne souvent lieu à une autorisation d'accès électronique distant des fournisseurs. Étant donné la complexité croissante de notre réseau, il est normal que l'on doive recourir de plus en plus à des parties externes pour soutenir et entretenir les équipements, les installations et les systèmes électroniques BES à faible impact. Or, la prédominance des systèmes électroniques BES à faible impact à connectivité externe pourrait avoir une incidence considérable sur la fiabilité du réseau en raison d'une possible vulnérabilité commune dans la chaîne d'approvisionnement. Afin de tenir compte de cette vulnérabilité, de l'ordonnance de la FERC⁴ à l'origine de la demande de modifications de la norme et de la résolution du Conseil d'administration de la NERC qui y a donné suite⁵, la section 6 de l'annexe 1 (laquelle porte sur l'exigence E2 existante) demande aux entités visées d'élaborer, de documenter et de mettre en œuvre un processus pour atténuer les risques liés aux communications malveillantes et aux accès électroniques distants des fournisseurs.

Section 6.1 de l'annexe 1 – Détermination des accès électroniques distants des fournisseurs

L'objectif de la section 6.1 de l'annexe 1 est d'obliger les entités à déterminer les accès électroniques distants des fournisseurs à leurs *systèmes électroniques BES* à faible impact ou *actifs électroniques BES* à faible impact. Une telle visibilité accroît la capacité de l'entité à détecter les problèmes pouvant provenir de l'accès électronique distant d'un fournisseur en particulier ou pouvant y être associés, à intervenir en cas de tels problèmes et à les résoudre. La section 6.1 oblige les entités à disposer d'une ou de plusieurs méthodes pour déterminer l'accès électronique distant des fournisseurs.

Section 6.2 de l'annexe 1 – Désactivation des accès électroniques distants des fournisseurs

L'objectif de la section 6.2 de l'annexe 1 est d'obliger les entités à disposer de moyens de désactiver l'accès électronique distant des fournisseurs, peu importe les raisons que pourrait invoquer l'entité, et de prévenir les événements de sécurité ainsi que la propagation de communications potentiellement malveillantes qui pourraient nuire aux actifs comprenant des *systèmes électroniques BES* à faible impact de l'entité ou avoir des effets adverses sur ces actifs. La section 6.2 oblige les entités à disposer d'une méthode pour désactiver l'accès électronique distant des fournisseurs. Cette obligation concourt également à la réalisation de l'objectif de sécurité visant à protéger les *systèmes électroniques BES* contre les compromissions pouvant entraîner un fonctionnement incorrect ou une instabilité du *système de production-transport d'électricité (BES)*.

4. Ordonnance n° 829, Revised Critical Infrastructure Protection Reliability Standards, 156 FERC ¶ 61,050 (2016).

5. Résolution - recommandations concernant la chaîne d'approvisionnement - approuvée par le Conseil d'administration – 6 février 2020 (LIEN)

Section 6.3 de l'annexe 1 – Détection de communications entrantes et sortantes malveillantes avérées ou présumées

L'objectif de la section 6.3 de l'annexe 1 est d'obliger les entités à disposer d'un moyen de détecter les communications malveillantes avérées ou présumées provenant de fournisseurs, de sorte que l'entité puisse intervenir en cas d'effet nuisible qui en résulterait, et d'y remédier.

Cette section vise seulement les communications avec les fournisseurs dont traitent la résolution du Conseil d'administration de la NERC et le rapport sur la chaîne d'approvisionnement. La section 6.3 oblige les entités à établir un ou plusieurs méthodes pour détecter les communications malveillantes avérées ou présumées provenant de fournisseurs et des systèmes utilisés par ceux-ci pour communiquer avec les actifs comprenant des *systèmes électroniques BES* à faible impact.

Les obligations figurant actuellement à l'exigence E2 de la norme CIP-003-8 qui régissent les communications électroniques directes avec les *systèmes électroniques BES* à faible impact ne sont pas aussi contraignantes que les obligations figurant dans la norme CIP-005-6 qui régissent les *systèmes électroniques BES* à impact moyen ou élevé. Des mesures de sécurité, telles que le recours à des *systèmes intermédiaires* et à l'authentification multifactorielle, procurent une protection supplémentaire contre les communications malveillantes et assurent un contrôle global des accès aux *systèmes électroniques BES* à impact moyen ou élevé. En plus des *systèmes intermédiaires* et de l'authentification multifactorielle, on exige que les *systèmes électroniques BES* à impact moyen ou élevé dans les *centres de contrôle* puissent détecter les communications malveillantes aux *points d'accès électronique* de ces systèmes. Ces mesures de sécurité ne sont pas imposées aux *systèmes électroniques BES* à faible impact.

Selon le modèle de la NERC, axé sur le degré de risque, il pourrait se produire une situation où un fournisseur communique directement avec un *système électronique BES*. Dans l'éventualité où cette connexion serait compromise, l'inclusion d'exigences de détection de communications malveillantes dans la section 6 de l'annexe 1 de la norme CIP-003-9 ferait en sorte que les entités disposent des moyens requis pour détecter de telles communications et pour atténuer les risques que posent les communications avec les fournisseurs.