

NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Cybersécurité – Protection de l'information

Justification technique de
la norme de fiabilité CIP-011-3

Mars 2021

FIABILITÉ | RÉSILIENCE | SÉCURITÉ



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

Table des matières

Préface.....	1
Introduction	2
Contexte	2
Exigence E1	3
Remarques générales sur l'exigence E1.....	3
Justification des modifications à l'exigence E1.....	3
Exigence E2.....	4
Remarques générales sur l'exigence E2.....	4
Justification de l'exigence E2.....	4
Annexe 1 : Justification technique de la norme de fiabilité CIP-011-2.....	5

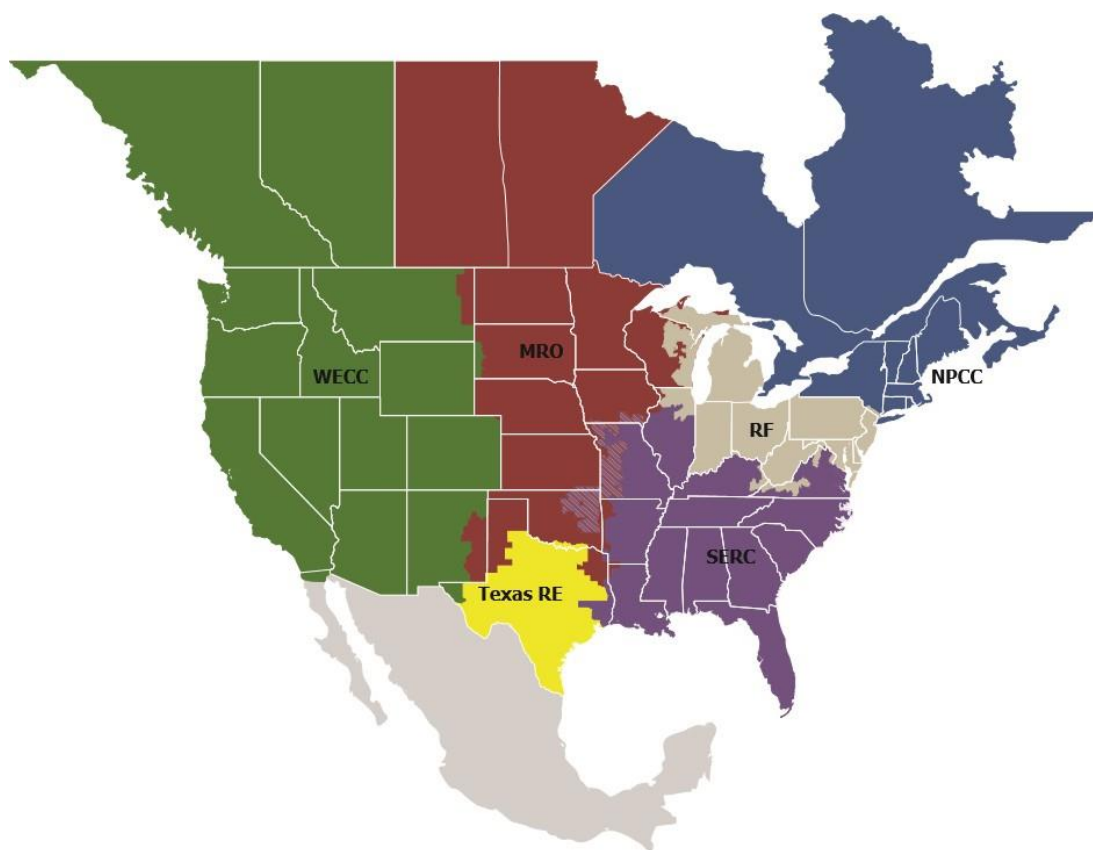
Préface

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

Fiabilité | Résilience | Sécurité

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

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



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

Introduction

Contexte

Ce document expose la justification technique de la *norme de fiabilité* CIP-011-3 proposée. Il vise à guider les parties prenantes ainsi que l'ERO dans la compréhension des enjeux technologiques et des exigences techniques de cette *norme de fiabilité*. Il présente aussi des précisions sur les intentions de l'équipe de rédaction (SDT) quant à ces exigences. Le présent document, *Justification technique de la norme de fiabilité CIP-011-3*, n'est pas une *norme de fiabilité* et son contenu ne doit donc pas être considéré comme obligatoire et exécutoire.

Le 24 juillet 2019, le Comité de normalisation de la North American Electric Reliability Corporation (NERC) a accepté une demande d'autorisation de norme (SAR) donnant suite à une initiative visant à renforcer la fiabilité du *BES* en offrant aux entités un meilleur éventail de choix, une flexibilité supérieure, une meilleure disponibilité et des options à meilleur coût pour la gestion de leurs *informations de système électronique BES* (BCSI), au moyen d'un encadrement sécuritaire du recours à des systèmes de stockage et d'analyse de données modernes offerts par des tiers. En outre, le projet visait à clarifier les protections à prévoir dans le cadre de l'utilisation de solutions de tiers (par exemple, des services infonuagiques).

En réponse à cette SAR, la SDT du projet 2019-02 a élaboré la *norme de fiabilité* CIP-011-3 afin d'exiger des entités responsables qu'elles mettent en œuvre les mesures particulières spécifiées à l'exigence E1. Il s'agit de mesures administratives, techniques et physiques portant sur les BCSI pendant leur stockage, leur manipulation et leur utilisation lorsqu'on a recours à des services infonuagiques de tiers fournisseurs, par exemple des logiciels-services (SaaS), des infrastructures-services (IaaS) ou des plateformes-services (PaaS).

Exigence E1

Remarques générales sur l'exigence E1

Aucune.

Justification des modifications à l'exigence E1

L'exigence E1 spécifie encore la nécessité de mettre en œuvre un ou plusieurs programmes documentés de protection des informations. La SDT souhaite préciser que cette exigence ne s'applique pas aux informations accessibles au public, comme les manuels de fournisseurs, non plus qu'à toute information considérée comme divulgable au grand public. La protection des informations englobe les versions électroniques et papier.

La SDT vient préciser qu'il s'agit de protéger les BCSI plutôt que les *systèmes électroniques BES* et les systèmes connexes pertinents qui pourraient contenir des BCSI. À cette fin, le libellé au début de l'exigence E1 de la norme CIP-011-3 a été modifié par l'ajout suivant : « des *informations de système électronique BES* (BCSI) relatives aux systèmes désignés ».

Justification des modifications à l'alinéa 1.1 de l'exigence E1

L'alinéa 1.1 de l'exigence E1 est une exigence axée sur l'objectif de désignation des *informations de système électronique BES* (BCSI). La modification de cette exigence vise à simplifier le libellé de l'alinéa 1.1 de la norme CIP-011-2.

Justification des modifications à l'alinéa 1.2 de l'exigence E1

L'alinéa 1.2 de l'exigence E1 énonce une exigence axée sur l'objectif de protection et de manipulation sécuritaire des *informations de système électronique BES* (BCSI) afin de réduire les risques de brèche de confidentialité. La référence à différents états des informations comme en « transport », en « stockage et en « utilisation » a été retirée. Le but recherché est de réduire la confusion pour les entités responsables qui tentent d'interpréter des mesures spécifiques à différents états des informations, de limiter les mesures à ces états et de gérer les chevauchements de mesures pour différents états ; il s'agit également de réduire la confusion sur le plan de la mise en application. Avec le retrait de cette formulation, les méthodes de protection des BCSI prennent explicitement un caractère englobant.

Les reformulations apportées à cette exigence visent l'harmonisation avec les exigences des autres normes CIP.

Exigence E2

Remarques générales sur l'exigence E2

Aucune.

Justification de l'exigence E2

Le processus de réutilisation et d'élimination des *actifs électroniques BES* vise à empêcher toute diffusion non autorisée des BCSI en cas de réutilisation ou d'élimination de ces actifs.

Cette exigence permet le retrait du service des *systèmes électroniques BES* et leur analyse avec leur support intact, car cela ne constitue pas une autorisation de réutilisation.

La justification de cette exigence est déjà présente dans les versions précédentes des normes CIP, ainsi que dans l'ordonnance 706 de la FERC et la proposition réglementaire (Notice of Proposed Rulemaking) connexe.

L'exigence E2 demeure inchangée. Elle concerne davantage la réutilisation et l'élimination des *systèmes électroniques BES* que les BCSI qui peuvent s'y trouver. Tout en reconnaissant que les *systèmes électroniques BES* et autres systèmes visés peuvent contenir des BCSI, l'intention originale de cette exigence est plus large que la question des BCSI. Il s'agit d'un enjeu concernant le cycle de vie des systèmes visés. La norme CIP-002 concerne spécifiquement le début du cycle de vie des *systèmes électroniques BES*, mais non leur fin de vie. La notion de fin de vie des systèmes visés est absente de la norme CIP-011, afin de réduire la confusion avec la réutilisation et l'élimination des BCSI. Le projet 2019 portant sur la gestion des accès aux BCSI ne prévoyait pas de modifier la norme CIP-002 dans le cadre de la demande SAR. Cette question a été communiquée en vue d'une évaluation future.

Annexe 1 : Justification technique de la norme de fiabilité

CIP-011-2

Cette section reproduit les éléments de justification technique de la section Principes directeurs et fondements techniques de la norme CIP-011-2, à titre de référence historique. Par ailleurs, le contenu de cette même section qui donne des indications sur la conformité est repris dans un Guide d'application distinct pour la présente norme.

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

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

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

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

Exigence E1

Les entités responsables sont libres d'utiliser les systèmes existants de gestion des changements et des actifs. Cependant, l'information que contiennent ces systèmes doit être évaluée, car les exigences de protection de l'information s'appliquent toujours.

La justification de cette exigence est déjà présente dans les versions précédentes des normes CIP, ainsi que dans l'ordonnance 706 de la FERC et la proposition réglementaire (*Notice of Proposed Rulemaking*) connexe.

Cette exigence stipule qu'il faut désigner l'*information de système électronique BES*. L'entité responsable dispose d'une certaine latitude quant à la mise en œuvre de cette exigence. L'entité responsable devrait expliquer par quels moyens l'*information de système électronique BES* est désignée dans son programme de protection de l'information. Par exemple, l'entité peut décider de marquer ou d'étiqueter les documents. Il n'est pas exigé d'établir des classes distinctes d'*information de système électronique BES*. Cependant, l'entité responsable est libre de le faire si elle le souhaite. Pour autant que le programme de protection de l'information englobe tous les éléments pertinents, l'entité peut aller plus loin et créer des niveaux de classification (public, confidentiel, usage interne, etc.). Si l'entité responsable choisit d'utiliser un système de classification, elle doit documenter les classes de ce système et tout étiquetage connexe dans son programme d'*information de système électronique BES*.

L'entité responsable peut stocker toute l'information concernant les *systèmes électroniques BES* dans une archive ou un emplacement séparé (physique ou électronique) protégé par un contrôle

d'accès. Par exemple, le programme de l'entité responsable pourrait spécifier que toute l'information stockée dans une archive particulière est une *information de système électronique BES*, ou que toute l'information stockée dans telle section d'une archive particulière est une *information de système électronique BES*, ou encore que toutes les copies papier de cette information sont stockées dans une partie sécurisée du bâtiment. D'autres méthodes pour la mise en œuvre de cette exigence sont suggérées à la section Mesures. Cependant, ces méthodes ne forment pas une liste exhaustive, et l'entité responsable peut recourir à d'autres moyens pour désigner l'*information de système électronique BES*.

La SDT souhaite préciser que cette exigence ne s'applique pas à l'information accessible au public, comme les manuels de fournisseurs consultables sur des sites Web publics, non plus qu'à toute information considérée comme divulgable au grand public.

La protection de l'information englobe les versions électroniques et papiers. L'exigence E1.2 prescrit une ou plusieurs procédures pour la protection et la manipulation sécuritaire de l'*information de système électronique BES*, notamment le stockage, le transport et l'utilisation. Ces procédures s'appliquent aussi à l'information qui peut se trouver sur des *actifs électroniques transitoires* ou des *supports amovibles*.

Le programme écrit de protection de l'information de l'entité doit expliquer comment celle-ci gère divers aspects de la protection de l'*information de système électronique BES*, notamment pendant le transport, afin de prévenir tout accès non autorisé, toute mauvaise utilisation ou toute corruption, et aussi pour protéger la confidentialité de l'information transmise. Par exemple, le recours à un fournisseur de service de télécommunications tiers plutôt qu'à une infrastructure détenue par l'organisation peut justifier le cryptage de l'information. L'entité peut choisir d'établir un trajet de communication de confiance pour le transport de l'*information de système électronique BES*; ce trajet de confiance utiliserait un mécanisme d'authentification ou d'autres mesures pour assurer la sécurité pendant le transport. L'entité peut adopter d'autres mesures de protection physique, comme le transport par messenger ou l'utilisation d'un contenant de transport verrouillé. La présente norme ne cherche pas à imposer un moyen particulier de sécuriser l'information pendant son transport.

Un bon programme de protection de l'information spécifie par écrit les circonstances dans lesquelles l'*information de système électronique BES* peut être partagée avec des tiers ou être utilisée par ceux-ci. L'entité ne doit diffuser ou partager l'information que selon le principe de l'accès sélectif. Par exemple, l'entité peut spécifier qu'un accord de confidentialité, une entente de non-divulgence, un contrat ou toute autre convention écrite concernant l'utilisation de l'information doit être en place entre l'entité et le tiers. Le programme de protection de l'information de l'entité doit spécifier les modalités de partage de l'*information de système électronique BES* avec des tiers ou de son utilisation par ceux-ci, par exemple une entente de non-divulgence. L'entité doit ensuite respecter son programme documenté. Ces exigences n'imposent pas un type particulier d'arrangement.

Exigence E2

Cette exigence permet le retrait du service des *systèmes électroniques BES* et leur analyse avec leur support intact, car cela ne constitue pas une autorisation de réutilisation. Cependant, si après analyse le support doit être réutilisé à l'extérieur d'un *système électronique BES* ou doit être éliminé, l'entité doit prendre des mesures pour empêcher la récupération non autorisée de l'*information de système électronique BES* présente sur le support.

La justification de cette exigence est déjà présente dans les versions précédentes des normes CIP, ainsi que dans l'ordonnance 706 de la FERC et la proposition réglementaire (*Notice of Proposed Rulemaking*) connexe.

Si un *actif électronique* visé est retiré du *périmètre de sécurité physique* avant que des mesures aient été prises pour empêcher la récupération non autorisée de l'*information de système électronique BES* ou avant que le support d'information ait été détruit, l'entité responsable doit tenir un dossier indiquant le détenteur du support d'information pendant que ce dernier se trouve hors du *périmètre de sécurité physique* avant l'application par l'entité des mesures prescrites à l'exigence E2.

On appelle « expurgation » le procédé qui consiste à éliminer l'information d'un support de données de manière à assurer raisonnablement que l'information ne pourra pas être récupérée ou reconstituée. Les moyens d'expurgation sont généralement divisés en quatre catégories : la mise au rebut, l'écrasement, la purge et la destruction. Aux fins de la présente exigence, la mise au rebut en elle-même – sauf dans certaines circonstances spéciales, comme le recours à un cryptage fort pour un disque utilisé dans un réseau de stockage (SAN) ou un autre support – ne doit jamais être jugée acceptable. Les techniques d'écrasement peuvent constituer un moyen d'expurgation adéquat pour les supports destinés à être réutilisés, tandis que les techniques de purge peuvent mieux convenir pour les supports destinés à l'élimination.

L'information suivante, tirée de la publication spéciale 800-88 du NIST, donne des précisions supplémentaires sur les types de mesures que l'entité pourrait prendre pour empêcher la récupération non autorisée de l'*information de système électronique BES* à partir de ses supports d'information :

Écrasement : Cette méthode d'expurgation consiste à écrire des données non sensibles à la place des données existantes du support, au moyen d'un logiciel ou d'un appareil spécial. Ce procédé peut écraser ainsi non seulement l'emplacement logique du ou des fichiers en cause (par exemple, la table d'allocation de fichiers), mais aussi tous les emplacements mémoire adressables. Cette opération a pour objet de remplacer les données existantes par des données quelconques. L'écrasement n'est pas possible dans le cas d'un support endommagé ou non réinscriptible. Le type et la taille du support peuvent aussi déterminer si l'écrasement est une méthode d'expurgation convenable [800-36].

Purge : La démagnétisation et l'exécution de la commande d'effacement sécurisé du microprogramme (pour les disques ATA seulement) sont des méthodes de purge acceptables. La démagnétisation consiste à exposer le support magnétique à un fort champ magnétique afin de perturber les domaines magnétiques d'enregistrement; ce champ magnétique est produit par un démagnétiseur. Il existe différents types de démagnétiseur (à faible puissance, à grande puissance, etc.) selon le type de support magnétique qu'ils peuvent traiter. Les démagnétiseurs comportent un aimant permanent puissant ou une bobine électromagnétique. La démagnétisation convient particulièrement pour purger un support endommagé, inopérant ou de très grande capacité, ou pour effacer rapidement des disquettes. [800-36] La commande d'effacement sécurisé (disques ATA) et la démagnétisation sont des exemples de méthodes de purge acceptables. La démagnétisation d'un disque dur détruit habituellement celui-ci, car elle efface aussi le microprogramme qui commande le disque.

Destruction : Il existe de nombreux moyens pour détruire un support d'information. La désintégration, la pulvérisation, la fusion et l'incinération sont des procédés d'expurgation conçus pour détruire complètement le support. On les confie généralement à une entreprise agréée de destruction de produits métalliques ou d'incinération disposant des moyens techniques appropriés pour effectuer cette opération de manière efficace, sécurisée et sécuritaire. Les supports optiques, notamment les cédéroms (réinscriptibles ou non), les disques optiques (DVD) et les disques magnéto-optiques, doivent être détruits par pulvérisation, par déchiquetage transversal ou par combustion.

Dans certains cas, notamment pour de l'équipement réseau, il peut être nécessaire de consulter le fabricant pour connaître la méthode d'expurgation appropriée.

Il est de la plus grande importance que l'organisation tienne un dossier de ses activités d'expurgation afin d'empêcher la récupération non autorisée d'*information de système électronique BES*. Les entités sont fortement invitées à consulter la publication spéciale 800-88 du NIST pour de plus amples renseignements sur l'élaboration de procédés d'expurgation des supports.

Justification

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

Justification de l'exigence E1 :

L'exigence d'un programme de protection de l'information vise à empêcher tout accès non autorisé à l'*information de système électronique BES*.

Justification de l'exigence E2 :

Le processus de réutilisation et d'élimination des *actifs électroniques BES* vise à empêcher toute diffusion non autorisée d'*information de système électronique BES* en cas de réutilisation ou d'élimination de ces actifs.