Traduction française attestée de la norme de fiabilité

Je certifie que le présent texte est une traduction complète et exacte de l'original en langue anglaise

Éric Léonard, traducteur agréé – OTTIAQ, membre n° 3678

Le 25 mars 2021

A. Introduction

1. **Titre :** **Cybersécurité – Communications entre *centres de contrôle***

2. **Numéro :** **CIP-012-1**

3. **Objet :** Protéger la confidentialité et l'intégrité des données d'*évaluation en temps réel* et de surveillance en *temps réel* transmises entre différents *centres de contrôle*.

4. **Applicabilité :**

   4.1. Entités fonctionnelles : Les exigences de la présente norme s'appliquent aux entités fonctionnelles suivantes qui détiennent ou exploitent un *centre de contrôle*, ci-après appelées « entités responsables ».

   4.1.1. *Responsable de l'équilibrage*

   4.1.2. *Exploitant d'installation de production*

   4.1.3. *Propriétaire d'installation de production*

   4.1.4. *Coordonnateur de la fiabilité*

   4.1.5. *Exploitant de réseau de transport*

   4.1.6. *Propriétaire d'installation de transport*

   4.2. Exemptions : Sont exemptés de la norme de fiabilité CIP-012-1 :

   4.2.1. les *actifs électroniques* aux *installations* réglementées par la Commission canadienne de sûreté nucléaire.

   4.2.2. Les systèmes, structures et composants régis par la U.S. Nuclear Regulatory Commission en vertu d'un plan de cybersécurité conforme au règlement CFR 10, section 73.54.

   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.

5. **Date d'entrée en vigueur :** Voir le plan de mise en œuvre de la norme CIP-012-1.

B. Exigences et mesures

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*.

M1. Exemples non limitatifs de pièces justificatives acceptables : un ou des plans documentés qui répondent à l'objectif de sécurité de l'exigence E1, et documentation attestant la mise en œuvre de ce ou ces plans.

C. Conformité

1. Processus de surveillance de la conformité

1.1. Responsable des mesures pour assurer la conformité : Le terme « responsable des mesures pour assurer la conformité » (CEA) désigne la NERC ou l'*entité régionale*, ou toute entité désignée par un organisme gouvernemental pertinent, dans leurs rôles respectifs visant à surveiller et à assurer la conformité avec les normes de fiabilité obligatoires et exécutoires de la NERC.

1.2. Conservation des pièces justificatives : Les périodes de conservation des pièces justificatives indiquées ci-après établissent la durée pendant laquelle une entité est tenue de conserver certaines pièces afin de démontrer sa conformité. Dans les cas où la période de conservation indiquée est plus courte que le temps écoulé depuis l'audit le plus récent, le CEA peut demander à l'entité de fournir d'autres pièces justificatives attestant sa conformité pendant la période complète écoulée depuis l'audit le plus récent.

L'entité responsable doit conserver les données ou pièces justificatives attestant sa conformité de la façon indiquée ci-après, à moins que son CEA lui demande de conserver certains documents plus longtemps dans le cadre d'une enquête.

- Les entités responsables doivent conserver les données ou les pièces justificatives liées à chaque exigence de la présente norme de fiabilité pendant trois années civiles.
- Si une entité responsable est jugée non conforme, elle doit conserver l'information relative à cette non-conformité jusqu'à ce que les correctifs aient été appliqués et approuvés ou pendant la période indiquée ci-dessus, selon la durée la plus longue.
- Le CEA doit conserver les derniers dossiers d'audit ainsi que tous les dossiers d'audit demandés et soumis par la suite.

1.3. Programme de surveillance de la conformité et d'application des normes : Selon la définition des règles de procédure de la NERC, l'expression « programme de surveillance

de la conformité et d'application des normes » désigne la liste des processus qui serviront à évaluer les données ou l'information afin de déterminer les résultats de conformité avec la norme de fiabilité.

Niveau de gravité de la non-conformité

Ex.	Niveau de gravité de la non-conformité (VSL)			
	VSL faible	VSL modéré	VSL élevé	VSL critique
E1	S. O.	L'entité responsable a documenté son ou ses plans, mais en omettant un des alinéas de l'exigence E1.	L'entité responsable a documenté son ou ses plans, mais en omettant deux des alinéas de l'exigence E1.	L'entité responsable n'a pas documenté le ou les plans prescrits à l'exigence E1. OU L'entité responsable n'a pas mis en œuvre une partie de son ou ses plans prescrits à l'exigence E1, sauf en cas de *circonstances CIP exceptionnelles*.

D. Différences régionales

Aucune

E. Documents connexes

Plan de mise en œuvre
Justification technique de la norme de fiabilité CIP-012-1 (*Technical Rationale and Justification for Reliability Standard CIP-012-1*)
Guide d'application

Historique des versions

Version	Date	Intervention	Suivi des modifications
1		Mise en œuvre de l'Ordonnance 822 de la FERC	Nouvelle norme
1	16 août 2018	Adoption par le Conseil d'administration de la NERC	
1	23 janvier 2020	Ordonnance de la FERC approuvant la norme CIP-012-1 (dossier RM18-20-000).	