

A. Introduction

1. **Titre :** Plans de défense
2. **Numéro :** PRC-012-2
3. **Objet :** Faire en sorte que les *plans de défense* n'entraînent pas de risques imprévus ou inacceptables pour la fiabilité du *système de production-transport d'électricité (BES)*.
4. **Applicabilité :**
 - 4.1. **Entités fonctionnelles :**
 - 4.1.1 *Coordonnateur de la fiabilité*
 - 4.1.2 *Coordonnateur de la planification*
 - 4.1.3 Entité propriétaire de *plan de défense* : *propriétaire d'installation de transport, propriétaire d'installation de production* ou *distributeur* qui possède la totalité ou une partie d'un *plan de défense*
 - 4.2. **Installations :**
 - 4.2.1 *Plans de défense*
5. **Date d'entrée en vigueur :** Voir le plan de mise en œuvre de la norme PRC-012-2.

B. Exigences et mesures

- E1. Avant de mettre en service un *plan de défense* nouveau ou dont le fonctionnement a été modifié ou avant de retirer un *plan de défense* existant, chaque entité propriétaire de *plan de défense* doit fournir pour examen l'information spécifiée à l'annexe 1 à tout *coordonnateur de la fiabilité* dans la zone duquel est situé le *plan de défense*.
[Facteur de risque de non-conformité : moyen] [Horizon : planification de l'exploitation]
- M1. Exemples non limitatifs de pièces justificatives : copie de la documentation spécifiée à l'annexe 1 et communications datées avec le ou les *coordonnateurs de la fiabilité* chargés de l'examen dans le cadre de l'exigence E1.
- E2. Chaque *coordonnateur de la fiabilité* qui reçoit l'information spécifiée à l'annexe 1 en vertu de l'exigence E1 doit, dans un délai de quatre mois civils complets suivant la réception ou selon un calendrier établi d'un commun accord, procéder à l'examen du *plan de défense* conformément à l'annexe 2, et fournir une réponse écrite à chaque entité propriétaire de *plan de défense*.
[Facteur de risque de non-conformité : moyen] [Horizon : planification de l'exploitation]
- M2. Exemples non limitatifs de pièces justificatives : rapports datés, listes de contrôle ou autres documents décrivant l'examen du *plan de défense*, et communications datées avec l'entité propriétaire de *plan de défense*, dans le cadre de l'exigence E2.
- E3. Avant de mettre en service un *plan de défense* nouveau ou dont le fonctionnement a été modifié ou avant de retirer un *plan de défense* existant, chaque entité propriétaire de *plan de défense* qui reçoit d'un *coordonnateur de la fiabilité* chargé de l'examen un constat de problèmes de fiabilité doit corriger chacun de ces problèmes à la satisfaction de chaque *coordonnateur de la fiabilité* chargé de l'examen.
[Facteur de risque de non-conformité : moyen] [Horizon : planification de l'exploitation]

- M3.** Exemples non limitatifs de pièces justificatives : documents datés et communications avec le *coordonnateur de la fiabilité* chargé de l'examen confirmant qu'aucun problème de fiabilité n'a été constaté lors de l'examen ou que tous les problèmes de fiabilité signalés ont été corrigés conformément à l'exigence E3.
- E4.** Chaque *coordonnateur de la planification*, au moins une fois toutes les cinq années civiles complètes, doit :
[Facteur de risque de non-conformité : moyen] [Horizon : planification à long terme]
- 4.1.** évaluer chaque *plan de défense* situé dans sa zone de planification afin de déterminer si les conditions suivantes sont remplies :
- 4.1.1.** le *plan de défense* doit atténuer la ou les conditions ou *contingences de réseau* pour lesquelles il a été conçu ;
 - 4.1.2.** le *plan de défense* doit éviter toute interaction nuisible avec d'autres plans de défense ou systèmes de protection et de contrôle ;
 - 4.1.3.** dans le cas d'un *plan de défense* à impact limité¹, le fonctionnement intempestif du *plan de défense* ou son non-fonctionnement ne doit pas donner lieu ou contribuer à des *déclenchements en cascade*, à une séparation fortuite, à une instabilité angulaire, à l'instabilité de la tension, à l'effondrement de la tension ou à des oscillations incorrectement amorties dans le *BES* ;
 - 4.1.4.** sauf dans le cas d'un *plan de défense* à impact limité, le fonctionnement intempestif possible du *plan de défense* par suite d'une défectuosité d'un de ses éléments doit répondre à toutes les exigences suivantes :
 - 4.1.4.1.** le *BES* doit demeurer stable ;
 - 4.1.4.2.** il ne doit pas y avoir de *déclenchements en cascade* ;
 - 4.1.4.3.** les *caractéristiques assignées d'installation* pertinentes ne doivent pas être dépassées ;
 - 4.1.4.4.** les tensions du *BES* doivent demeurer en deçà des limites de tension *postcontingences* ainsi que des limites d'écart de tension *postcontingences* établies par le *planificateur de réseau de transport* et le *coordonnateur de la planification* ;
 - 4.1.4.5.** les réponses aux tensions transitoires doivent demeurer en deçà des limites acceptables établies par le *planificateur de réseau de transport* et le *coordonnateur de la planification* ;
 - 4.1.5.** sauf dans le cas d'un *plan de défense* à impact limité, une défaillance d'un élément du *plan de défense*, dans une situation où il est prévu que le *plan de défense* fonctionne, ne doit pas empêcher le *BES* de respecter les mêmes exigences de performance (définis dans la norme de fiabilité TPL-001-4 [où elles sont appelées « *critères de comportement* »] ou toute norme qui la remplace) que celles prescrites pour les événements et les conditions en vue desquels le *plan de défense* est conçu ;

1. Un *plan de défense* désigné comme étant à impact limité ne peut pas, en cas de fonctionnement intempestif ou de non-fonctionnement, donner lieu ou contribuer à des *déclenchements en cascade*, à une séparation fortuite, à une instabilité angulaire, à l'instabilité de la tension, à l'effondrement de la tension ou à des oscillations incorrectement amorties dans le *BES*.

- 4.2. fournir les résultats d'évaluation du *plan de défense*, y compris toute lacune constatée, à chaque *coordonnateur de la fiabilité* chargé de l'examen et entité propriétaire de *plan de défense*, ainsi qu'à chaque *planificateur de réseau de transport* et *coordonnateur de la planification* touché.
- M4. Exemples non limitatifs de pièces justificatives : rapports datés ou autres documents d'analyse concernant l'évaluation de chaque *plan de défense*, et communications datées avec les entités propriétaires de *plan de défense*, les *planificateurs de réseau de transport*, les autres *coordonnateurs de la planification* et les *coordonnateurs de la fiabilité* chargés de l'examen, dans le cadre de l'exigence E4.
- E5. Chaque entité propriétaire de *plan de défense*, dans un délai de 120 jours civils complets suivant le fonctionnement d'un *plan de défense* ou son non-fonctionnement dans une situation où il aurait dû fonctionner, ou selon un calendrier établi d'un commun accord avec le ou les *coordonnateurs de la fiabilité* chargés de l'examen, doit :
[Facteur de risque de non-conformité : moyen] [Horizon : planification de l'exploitation]
- 5.1. participer à l'analyse de la performance opérationnelle du *plan de défense* afin de déterminer :
- 5.1.1. si les événements ou les conditions du *réseau* ont déclenché adéquatement le *plan de défense* ;
- 5.1.2. si le *plan de défense* a fonctionné comme prévu ;
- 5.1.3. si le *plan de défense* a effectivement atténué les problèmes de performance du *BES* pour lesquels il est conçu ;
- 5.1.4. si le fonctionnement du *plan de défense* a entraîné une réaction imprévue ou nuisible du *BES* ;
- 5.2. fournir à son ou ses *coordonnateurs de la fiabilité* chargés de l'examen les résultats de l'analyse de performance opérationnelle du *plan de défense* si une ou des lacunes sont signalées.
- M5. Exemples non limitatifs de pièces justificatives : documents datés décrivant les résultats de l'analyse de performance opérationnelle du *plan de défense* et communications datées avec la ou les entités propriétaires de *plan de défense* et le ou les *coordonnateurs de la fiabilité* chargés de l'examen, dans le cadre de l'exigence E5.
- E6. Chaque entité propriétaire de *plan de défense* doit participer à élaborer un *plan d'actions correctives* et soumettre celui-ci à son ou ses *coordonnateurs de la fiabilité* chargés de l'examen dans un délai de six mois civils complets :
[Facteur de risque de non-conformité : moyen] [Horizon : planification de l'exploitation et planification à long terme]
- après avoir été avisé d'une lacune dans son *plan de défense* en vertu de l'exigence E4 ; ou
 - après avoir avisé son ou ses *coordonnateurs de la fiabilité* d'une lacune en vertu de l'alinéa 5.2 de l'exigence E5 ; ou
 - après avoir découvert une lacune dans son *plan de défense* selon l'exigence E8.

- M6.** Exemples non limitatifs de pièces justificatives : *plan d'actions correctives* daté et communications datées entre chaque *coordonnateur de la fiabilité* chargé de l'examen et chaque entité propriétaire de *plan de défense*, dans le cadre de l'exigence E6.
- E7.** Chaque entité propriétaire de *plan de défense* doit, pour chacun de ses *plans d'actions correctives* élaborés conformément à l'exigence E6 :
[Facteur de risque de non-conformité : moyen] [Horizon : planification de l'exploitation et planification à long terme]
- 7.1.** mettre en œuvre le *plan d'actions correctives* ;
- 7.2.** mettre à jour le *plan d'actions correctives* en cas de changement dans ses activités ou son calendrier ;
- 7.3.** aviser chaque *coordonnateur de la fiabilité* chargé de l'examen en cas de changement dans les activités ou le calendrier du plan d'actions correctives et lorsque le *plan d'actions correctives* est achevé.
- M7.** Exemples non limitatifs de pièces justificatives : documents datés comme des *plans d'actions correctives*, des dossiers de projet ou de programme de gestion de travaux, des fiches de réglage, des ordres de travail, des dossiers d'entretien, et des communications avec le ou les *coordonnateurs de la fiabilité* chargés de l'examen documentant la mise en œuvre, la mise à jour ou l'achèvement d'un *plan d'actions correctives*, dans le cadre de l'exigence E7.
- E8.** Chaque entité propriétaire de *plan de défense* doit participer à un essai fonctionnel de chacun de ses *plans de défense* afin de vérifier la performance globale de celui-ci ainsi que le bon fonctionnement des éléments qui ne font pas partie des *systèmes de protection* :
[Facteur de risque de non-conformité : élevé] [Horizon : planification à long terme]
- au moins une fois toutes les six années civiles complètes, pour tous les *plans de défense* non désignés comme étant à impact limité ; ou
 - au moins une fois toutes les douze années civiles complètes, pour tous les *plans de défense* désignés comme étant à impact limité.
- M8.** Exemples non limitatifs de pièces justificatives : documents datés décrivant l'analyse de performance opérationnelle du *plan de défense* pour le fonctionnement correct d'un segment ou pour l'intégralité du *plan de défense* (documentation de la mesure M5), ou documents datés attestant qu'un essai fonctionnel de chaque segment du *plan de défense* ou un essai intégral a été effectué conformément à l'exigence E8.
- E9.** Chaque *coordonnateur de la fiabilité* doit mettre à jour, au moins une fois tous les douze mois civils complets, une base de données sur les *plans de défense* contenant au minimum l'information spécifiée à l'annexe 3.
[Facteur de risque de non-conformité : faible] [Horizon : planification de l'exploitation]
- M9.** Exemples non limitatifs de pièces justificatives : feuilles de chiffrier datées, relevés de base de données ou autres documents attestant qu'une base de données sur les *plans de défense* a été mise à jour conformément à l'exigence E9.

C. Conformité

1. Processus de surveillance de la conformité

1.1. Responsable de la surveillance de l'application des normes

Selon la définition des règles de procédure de la NERC, le terme « responsable de la surveillance de l'application des normes » (CEA) désigne la NERC ou l'*entité régionale* dans leurs rôles respectifs de surveillance de la conformité aux normes de fiabilité 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 justificatives 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 visée doit conserver les données ou pièces justificatives attestant sa conformité selon les modalités indiquées ci-après, à moins que son CEA lui ordonne, dans le cadre d'une enquête, de conserver certains éléments de preuve plus longtemps.

Chaque entité propriétaire de *plan de défense* (*propriétaire d'installation de transport, propriétaire d'installation de production ou distributeur*) doit conserver les données ou pièces justificatives attestant sa conformité aux exigences E1, E3, E5, E6, E7 et E8 ainsi qu'aux mesures M1, M3, M5, M6, M7 et M8 depuis l'audit le plus récent, à moins que son CEA lui ordonne, dans le cadre d'une enquête, de conserver certains éléments de preuve plus longtemps.

Chaque *coordonnateur de la fiabilité* doit conserver les données ou pièces justificatives attestant sa conformité aux exigences E2 et E9 ainsi qu'aux mesures M2 et M9 depuis l'audit le plus récent, à moins que son CEA lui ordonne, dans le cadre d'une enquête, de conserver certains éléments de preuve plus longtemps.

Chaque *coordonnateur de la planification* doit conserver les données ou pièces justificatives attestant sa conformité à l'exigence E4 et à la mesure M4 depuis l'audit le plus récent, à moins que son CEA lui ordonne, dans le cadre d'une enquête, de conserver certains éléments de preuve plus longtemps.

Si une entité propriétaire de *plan de défense* (*propriétaire d'installation de transport, propriétaire d'installation de production ou distributeur*), un *coordonnateur de la fiabilité* ou un *coordonnateur de la planification* est jugé non conforme à une exigence, il 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 dossiers de l'audit le plus récent ainsi que tous les dossiers d'audit subséquents demandés et présentés.

1.3. Programme de surveillance et de mise en application des normes

Selon la définition des règles de procédure de la NERC, l'expression « programme de surveillance et de mise en application des normes » désigne la liste des processus qui

serviront à évaluer les données ou l'information afin de déterminer les résultats de conformité à la norme de fiabilité.

Niveaux de gravité des non-conformités (VSL)

Ex.	Niveaux de gravité de la non-conformité (VSL)			
	VSL faible	VSL modéré	VSL élevé	VSL critique
E1	S. O.	S. O.	S. O.	L'entité propriétaire de <i>plan de défense</i> n'a pas fourni l'information spécifiée à l'annexe 1 à chaque <i>coordonnateur de la fiabilité</i> , conformément à l'exigence E1, avant de mettre en service un <i>plan de défense</i> nouveau ou dont le fonctionnement a été modifié ou avant de retirer un <i>plan de défense</i> existant.
E2	Le <i>coordonnateur de la fiabilité</i> chargé de l'examen a procédé à l'examen et a fourni une réponse écrite conformément à l'exigence E2, mais avec un retard d'au plus 30 jours civils complets.	Le <i>coordonnateur de la fiabilité</i> chargé de l'examen a procédé à l'examen et a fourni une réponse écrite conformément à l'exigence E2, mais avec un retard de plus de 30 jours civils complets et d'au plus 60 jours civils complets.	Le <i>coordonnateur de la fiabilité</i> chargé de l'examen a procédé à l'examen et a fourni une réponse écrite conformément à l'exigence E2, mais avec un retard de plus de 60 jours civils complets et d'au plus 90 jours civils complets.	Le <i>coordonnateur de la fiabilité</i> chargé de l'examen a procédé à l'examen et a fourni une réponse écrite conformément à l'exigence E2, mais avec un retard de plus de 90 jours civils complets. OU Le <i>coordonnateur de la fiabilité</i> chargé de l'examen n'a pas procédé à l'examen ou n'a pas fourni une réponse écrite conformément à l'exigence E2.

Ex.	Niveaux de gravité de la non-conformité (VSL)			
	VSL faible	VSL modéré	VSL élevé	VSL critique
E3	S. O.	S. O.	S. O.	L'entité <i>propriétaire de plan de défense</i> n'a pas corrigé un problème de fiabilité à la satisfaction de chaque <i>coordonnateur de la fiabilité</i> chargé de l'examen, conformément à l'exigence E3, avant de mettre en service un <i>plan de défense</i> nouveau ou dont le fonctionnement a été modifié ou avant de retirer un <i>plan de défense</i> existant.

Ex.	Niveaux de gravité de la non-conformité (VSL)			
	VSL faible	VSL modéré	VSL élevé	VSL critique
E4	Le <i>coordonnateur de la planification</i> a procédé à l'évaluation conformément à l'exigence E4, mais avec un retard d'au plus 30 jours civils complets.	Le <i>coordonnateur de la planification</i> a procédé à l'évaluation conformément à l'exigence E4, mais avec un retard de plus de 30 jours civils complets et d'au plus 60 jours civils complets.	Le <i>coordonnateur de la planification</i> a procédé à l'évaluation conformément à l'exigence E4, mais avec un retard de plus de 60 jours civils complets et d'au plus 90 jours civils complets. OU Le <i>coordonnateur de la planification</i> a procédé à l'évaluation conformément à l'exigence E4, mais en omettant un des alinéas 4.1.1 à 4.1.5.	Le <i>coordonnateur de la planification</i> a procédé à l'évaluation conformément à l'exigence E4, mais avec un retard de plus de 90 jours civils complets. OU Le <i>coordonnateur de la planification</i> a procédé à l'évaluation conformément à l'exigence E4, mais en omettant au moins deux des alinéas 4.1.1 à 4.1.5. OU Le <i>coordonnateur de la planification</i> a procédé à l'évaluation conformément à l'exigence E4, mais n'a pas fourni les résultats à une ou plusieurs des entités indiquées à l'alinéa 4.2. OU Le <i>coordonnateur de la planification</i> n'a pas procédé à l'évaluation conformément à l'exigence E4.

Ex.	Niveaux de gravité de la non-conformité (VSL)			
	VSL faible	VSL modéré	VSL élevé	VSL critique
E5	L'entité propriétaire de <i>plan de défense</i> a procédé à l'analyse conformément à l'exigence E5, mais avec un retard d'au plus 10 jours civils complets.	L'entité propriétaire de <i>plan de défense</i> a procédé à l'analyse conformément à l'exigence E5, mais avec un retard de plus de 10 jours civils complets et d'au plus 20 jours civils complets.	<p>L'entité propriétaire de <i>plan de défense</i> a procédé à l'analyse conformément à l'exigence E5, mais avec un retard de plus de 20 jours civils complets et d'au plus 30 jours civils complets.</p> <p>OU</p> <p>L'entité propriétaire de <i>plan de défense</i> a procédé à l'analyse conformément à l'exigence E5, mais en omettant un des alinéas 5.1.1 à 5.1.4.</p>	<p>L'entité propriétaire de <i>plan de défense</i> a procédé à l'analyse conformément à l'exigence E5, mais avec un retard de plus de 30 jours civils complets.</p> <p>OU</p> <p>L'entité propriétaire de <i>plan de défense</i> a procédé à l'analyse conformément à l'exigence E5, mais en omettant au moins deux des alinéas 5.1.1 à 5.1.4.</p> <p>OU</p> <p>L'entité propriétaire de <i>plan de défense</i> a procédé à l'analyse conformément à l'exigence E5, mais n'a pas fourni les résultats à un ou plusieurs <i>coordonnateurs de la fiabilité</i> chargés de l'examen conformément à l'alinéa 5.2.</p> <p>OU</p> <p>L'entité propriétaire de <i>plan de défense</i> n'a pas procédé à l'analyse conformément à l'exigence E5.</p>

Ex.	Niveaux de gravité de la non-conformité (VSL)			
	VSL faible	VSL modéré	VSL élevé	VSL critique
E6	L'entité propriétaire de <i>plan de défense</i> a élaboré un <i>plan d'actions correctives</i> et l'a soumis à son ou ses <i>coordonnateurs de la fiabilité</i> chargés de l'examen conformément à l'exigence E6, mais avec un retard d'au plus 10 jours civils complets.	L'entité propriétaire de <i>plan de défense</i> a élaboré un <i>plan d'actions correctives</i> et l'a soumis à son ou ses <i>coordonnateurs de la fiabilité</i> chargés de l'examen conformément à l'exigence E6, mais avec un retard de plus de 10 jours civils complets et d'au plus 20 jours civils complets.	L'entité propriétaire de <i>plan de défense</i> a élaboré un <i>plan d'actions correctives</i> et l'a soumis à son ou ses <i>coordonnateurs de la fiabilité</i> chargés de l'examen conformément à l'exigence E6, mais avec un retard de plus de 20 jours civils complets et d'au plus 30 jours civils complets.	<p>L'entité <i>propriétaire de plan de défense</i> a élaboré un <i>plan d'actions correctives</i> et l'a soumis à son ou ses <i>coordonnateurs de la fiabilité</i> chargés de l'examen conformément à l'exigence E6, mais avec un retard de plus de 30 jours civils complets.</p> <p>OU</p> <p>L'entité propriétaire de <i>plan de défense</i> a élaboré un <i>plan d'actions correctives</i>, mais ne l'a pas soumis à un ou plusieurs de ses <i>coordonnateurs de la fiabilité</i> chargés de l'examen conformément à l'exigence E6.</p> <p>OU</p> <p>L'entité propriétaire de <i>plan de défense</i> n'a pas élaboré de <i>plan d'actions correctives</i> conformément à l'exigence E6.</p>

Ex.	Niveaux de gravité de la non-conformité (VSL)			
	VSL faible	VSL modéré	VSL élevé	VSL critique
E7	L'entité propriétaire de <i>plan de défense</i> a mis en œuvre un <i>plan d'actions correctives</i> conformément à l'alinéa 7.1 de l'exigence E7, mais ne l'a pas mis à jour conformément à l'alinéa 7.2 en cas de changement dans ses activités ou son calendrier, ou n'a pas avisé conformément à l'alinéa 7.3 chacun des <i>coordonnateurs de la fiabilité</i> chargés de l'examen en cas de mise à jour ou à l'achèvement du <i>plan d'actions correctives</i> .	S. O.	S. O.	L'entité propriétaire de <i>plan de défense</i> n'a pas mis en œuvre un <i>plan d'actions correctives</i> conformément à l'alinéa 7.1 de l'exigence E7.
E8	L'entité propriétaire de <i>plan de défense</i> a effectué un essai fonctionnel d'un <i>plan de défense</i> conformément à l'exigence E8, mais avec un retard d'au plus 30 jours civils complets.	L'entité propriétaire de <i>plan de défense</i> a effectué un essai fonctionnel d'un <i>plan de défense</i> conformément à l'exigence E8, mais avec un retard de plus de 30 jours civils complets et d'au plus 60 jours civils complets.	L'entité propriétaire de <i>plan de défense</i> a effectué un essai fonctionnel d'un <i>plan de défense</i> conformément à l'exigence E8, mais avec un retard de plus de 60 jours civils complets et d'au plus 90 jours civils complets.	L'entité propriétaire de <i>plan de défense</i> a effectué un essai fonctionnel d'un <i>plan de défense</i> conformément à l'exigence E8, mais avec un retard de plus de 90 jours civils complets. OU L'entité propriétaire de <i>plan de défense</i> n'a pas effectué un essai fonctionnel d'un <i>plan de défense</i> conformément à l'exigence E8.

Ex.	Niveaux de gravité de la non-conformité (VSL)			
	VSL faible	VSL modéré	VSL élevé	VSL critique
E9	Le <i>coordonnateur de la fiabilité</i> a mis à jour la base de données sur les <i>plans de défense</i> conformément à l'exigence E9, mais avec un retard d'au plus 30 jours civils complets.	Le <i>coordonnateur de la fiabilité</i> a mis à jour la base de données sur les <i>plans de défense</i> conformément à l'exigence E9, mais avec un retard de plus de 30 jours civils complets et d'au plus 60 jours civils complets.	Le <i>coordonnateur de la fiabilité</i> a mis à jour la base de données sur les <i>plans de défense</i> conformément à l'exigence E9, mais avec un retard de plus de 60 jours civils complets et d'au plus 90 jours civils complets.	Le <i>coordonnateur de la fiabilité</i> a mis à jour la base de données sur les <i>plans de défense</i> conformément à l'exigence E9, mais avec un retard de plus de 90 jours civils complets. OU Le <i>coordonnateur de la fiabilité</i> n'a pas mis à jour la base de données sur les <i>plans de défense</i> conformément à l'exigence E9.

D. Différences régionales

Aucune.

E. Documents connexes

Historique des versions

Version	Date	Intervention	Suivi des modifications
0	8 février 2005	Adoption par le Conseil d'administration	
0	16 mars 2007	Désignation par la Commission comme version provisoire, sans aucune mesure prise concernant la norme	
1	13 novembre 2014	Adoption par le Conseil d'administration	
1	19 novembre 2015	Acceptation par la Commission à titre informatif seulement	
2	5 mai 2016	Adoption par le Conseil d'administration	

Annexe 1

Documentation à fournir pour l'examen d'un *plan de défense*

La liste de contrôle qui suit spécifie les informations essentielles que l'entité propriétaire de *plan de défense* doit documenter et fournir aux *coordonnateurs de la fiabilité (RC)* chargés de l'examen pour chaque *plan de défense (RAS)* nouveau ou dont le fonctionnement a été modifié². Pour tout élément de cette liste qui ne s'applique pas au *plan de défense* à examiner, on inscrira la mention « Sans objet ». Si un *plan de défense* existant est présenté pour examen et approbation d'une modification, seule la modification proposée nécessite un examen ; l'entité propriétaire de *plan de défense* doit toutefois fournir un résumé du fonctionnement préexistant. Le RC peut demander des compléments d'information sur n'importe quel aspect du *plan de défense* ainsi que sur tout problème de fiabilité connexe. Le RC peut inviter des entités supplémentaires (sans pouvoir de décision) à participer au processus d'examen du *plan de défense*.

I. Généralités

1. Éléments d'information (cartes, schémas unifilaires, schémas de poste électrique, schémas de principe, etc.) qui indiquent l'emplacement physique et électrique du *plan de défense* et des installations connexes.
2. Fonctionnement du nouveau *plan de défense* ou des modifications proposées au fonctionnement d'un *plan de défense* existant, avec documentation du fonctionnement du *plan de défense* avant et après les modifications.
3. *Plan d'actions correctives*, si des modifications d'un *plan de défense* sont proposées dans le cadre d'un *plan d'actions correctives*.
4. Données à verser dans la base de données sur les *plans de défense* :
 - a. nom du *plan de défense* ;
 - b. chaque entité propriétaire de *plan de défense* et ses coordonnées ;
 - c. date réelle ou prévue de mise en service, date d'approbation la plus récente par le RC (exigence E3), date d'évaluation la plus récente (exigence E4) et date de retrait, le cas échéant ;
 - d. problème de performance du *réseau* ou autre raison qui motive le *plan de défense* (surcharge thermique, instabilité angulaire, amortissement incorrect d'oscillations, instabilité de la tension, surtension, sous-tension, rétablissement lent de la tension, etc.) ;
 - e. description des *contingences* ou des conditions du *réseau* pour lesquelles le *plan de défense* a été conçu (conditions de déclenchement) ;
 - f. actions que doit exécuter le *plan de défense* ;

2. L'expression « dont le fonctionnement a été modifié » s'applique à toute modification apportée à un *plan de défense*, parmi les suivantes :

- changements dans les conditions ou les contingences du *réseau* surveillées par le *plan de défense* ;
- changements dans les actions que le *plan de défense* est conçu pour exécuter ;
- changements dans les composants physiques du *plan de défense*, au-delà du remplacement à l'identique, sans changement dans le fonctionnement initial de composants existants ;
- changements à la logique du *plan de défense*, au-delà de la correction d'erreurs existantes ;
- changements dans les niveaux de redondance (ajout ou retrait).

- g. désignation du *plan de défense* comme étant à impact limité³ ;
- h. tout complément d'explication qui contribue à une compréhension de haut niveau du *plan de défense*.

II. Description fonctionnelle et information relative à la planification du transport

1. *Contingences* et conditions du *réseau* auxquelles le *plan de défense* est censé remédier.
2. Actions que doit exécuter le *plan de défense* en réponse à des perturbations.
3. Résumé d'études techniques, le cas échéant, démontrant que les actions du *plan de défense* proposé répondent aux objectifs de performance du *réseau* dans le cadre des événements et des conditions du *réseau* auxquels le *plan de défense* est censé remédier. Ce résumé d'études techniques doit préciser notamment les années étudiées, les conditions du *réseau* et les *contingences* analysées pour la conception du *plan de défense*, et la date à laquelle les études techniques ont été effectuées.
4. Information sur tout projet de développement du *réseau* susceptible d'influer sur le *plan de défense*.
5. Le cas échéant, désignation « à impact limité » proposée par l'entité propriétaire du *plan de défense*, avec justification.
6. Documentation décrivant la performance du *réseau* résultant d'un fonctionnement intempestif possible du *plan de défense* (sauf si celui-ci est à impact limité) causé par la défectuosité d'un de ses éléments. En cas de défectuosité d'un élément d'un *plan de défense* non désigné comme étant à impact limité, toutes les conditions suivantes doivent être remplies :
 - a. le *BES* doit demeurer stable ;
 - b. il ne doit pas y avoir de *déclenchements en cascade* ;
 - c. les *caractéristiques assignées d'installation* pertinentes ne doivent pas être dépassées ;
 - d. les tensions du *BES* doivent demeurer en deçà des limites de tension *postcontingences* ainsi que des limites d'écart de tension *postcontingences* établies par le *planificateur de réseau de transport* et le *coordonnateur de la planification* ;
 - e. les réponses aux tensions transitoires doivent demeurer en deçà des limites acceptables établies par le *planificateur de réseau de transport* et le *coordonnateur de la planification*.
7. Évaluation confirmant que les réglages et le fonctionnement du *plan de défense* font en sorte d'éviter toute interaction nuisible avec d'autres *plans de défense* et systèmes de protection et de contrôle.
8. Indication d'autres *RC* touchés.

III. Mise en œuvre

1. Documentation décrivant tout équipement pertinent utilisé pour la détection, l'alimentation c.c., les communications, le télédéclenchement, la logique de traitement, les actions de commande et la surveillance.

3. Un *plan de défense* désigné comme étant à impact limité ne peut pas, en cas de fonctionnement intempestif ou de non-fonctionnement, donner lieu ou contribuer à des *déclenchements en cascade*, à une séparation fortuite, à une instabilité angulaire, à l'instabilité de la tension, à l'effondrement de la tension ou à des oscillations incorrectement amorties dans le *BES*.

2. Information sur les réglages ou paramètres et la logique de détection qui commandent le fonctionnement du *plan de défense*.
3. Documentation confirmant que tout dispositif multifonction affecté à des fonctions de *plan de défense* en plus d'autres fonctions (relais de protection, SCADA, etc.) ne compromet pas la fiabilité du *plan de défense* lorsque ce dispositif n'est pas en service ou est en cours d'entretien.
4. Documentation décrivant la performance du *réseau* en cas de défaillance d'un des éléments du *plan de défense* (sauf si celui-ci est à impact limité) au moment où le *plan de défense* est censé fonctionner. La défaillance d'un des éléments d'un *plan de défense* non désigné comme étant à impact limité ne doit pas empêcher le *BES* de respecter les mêmes exigences de performance (définies dans la norme de fiabilité TPL-001-4 [où elles sont appelées « critères de comportement »] ou dans toute norme qui la remplace) que celles prescrites pour les événements et les conditions pour lesquels le *plan de défense* est conçu. La documentation doit décrire ou illustrer comment la conception du *plan de défense* atteint cet objectif.
5. Documentation décrivant le processus d'essai fonctionnel.

IV. Retrait d'un *plan de défense*

La liste suivante indique les informations sur le *plan de défense* que l'entité propriétaire de *plan de défense* doit documenter et fournir à chaque *RC* chargé de l'examen.

1. Information nécessaire pour permettre au *RC* de comprendre l'emplacement physique et électrique du *plan de défense* et des installations connexes.
2. Résumé des études techniques pertinentes et des justifications techniques qui motivent le retrait du *plan de défense*.
3. Date de retrait du *plan de défense*.

Annexe 2

Liste de contrôle d'examen de *plan de défense* par le *coordonnateur de la fiabilité*

La liste de contrôle suivante indique les critères de fiabilité qui doivent guider le *coordonnateur de la fiabilité (RC)* dans son examen et sa vérification de tout *plan de défense* nouveau ou dont le fonctionnement a été modifié⁴. Le *RC* n'est pas limité dans son examen aux éléments de cette liste de contrôle ; il peut demander des compléments d'information sur n'importe quel aspect du *plan de défense* ainsi que sur tout problème de fiabilité relatif au *plan de défense*. Pour tout élément de cette liste qui ne s'applique pas au *plan de défense* examiné, on inscrira la mention « Sans objet ». Si l'examen soulève des questionnements quant à la fiabilité, celles-ci ainsi que les solutions proposées doivent être documentées avec le reste des éléments applicables de l'annexe 2.

I. Conception

1. Les actions du *plan de défense* répondent aux objectifs de performance pour l'étendue des événements et des conditions auxquels le *plan de défense* est censé remédier.
2. La temporisation des actions du *plan de défense* est appropriée aux objectifs de performance du *BES* établis pour le *plan de défense*.
3. Les conditions d'armement du *plan de défense*, le cas échéant, sont appropriées pour ses objectifs de performance du *réseau*.
4. Le *plan de défense* évite toute interaction nuisible avec d'autres *plans de défense* ou systèmes de protection et de contrôle.
5. Les effets d'un fonctionnement incorrect du *plan de défense* (y compris son fonctionnement intempestif ou son non-fonctionnement) ont été déterminés.
6. La désignation du *plan de défense* comme étant ou non à impact limité⁵. Un *plan de défense* à impact limité ne peut pas, en cas de fonctionnement intempestif ou de non-fonctionnement, donner lieu ou contribuer à des *déclenchements en cascade*, à une séparation fortuite, à une instabilité angulaire, à l'instabilité de la tension, à l'effondrement de la tension ou à des oscillations incorrectement amorties dans le *BES*.
7. Sauf dans le cas d'un *plan de défense* à impact limité (selon l'évaluation du *RC*), le fonctionnement intempestif possible du *plan de défense* par suite d'une défectuosité d'un de ses éléments doit répondre à toutes les exigences suivantes :
 - a. le *BES* doit demeurer stable ;

-
4. L'expression « dont le fonctionnement a été modifié » s'applique à toute modification apportée à un *plan de défense*, parmi les suivantes :
- changements dans les conditions ou les contingences du *réseau* surveillées par le *plan de défense* ;
 - changements dans les actions que le *plan de défense* est conçu pour exécuter ;
 - changements dans les composants physiques du *plan de défense*, au-delà du remplacement à l'identique, sans changement dans le fonctionnement initial de composants existants ;
 - changements à la logique du *plan de défense*, au-delà de la correction d'erreurs existantes ;
 - changements dans les niveaux de redondance (ajout ou retrait).
5. Un *plan de défense* désigné comme étant à impact limité ne peut pas, en cas de fonctionnement intempestif ou de non-fonctionnement, donner lieu ou contribuer à des *déclenchements en cascade*, à une séparation fortuite, à une instabilité angulaire, à l'instabilité de la tension, à l'effondrement de la tension ou à des oscillations incorrectement amorties dans le *BES*.

- b. il ne doit pas y avoir de *déclenchements en cascade* ;
 - c. les *caractéristiques assignées d'installation* pertinentes ne doivent pas être dépassées ;
 - d. les tensions du *BES* doivent demeurer en deçà des limites de tension *postcontingences* ainsi que des limites d'écart de tension *postcontingences* établies par le *planificateur de réseau de transport* et le *coordonnateur de la planification* ;
 - e. les réponses aux tensions transitoires doivent demeurer en deçà des limites acceptables établies par le *planificateur de réseau de transport* et le *coordonnateur de la planification*.
8. Les effets de modifications futures du *BES* sur la conception et le fonctionnement du *plan de défense* ont été déterminés, le cas échéant.

II. Mise en œuvre

- 1. La mise en œuvre de la logique du *plan de défense* établit une corrélation adéquate entre les actions (signaux de sortie) et les événements et conditions (signaux d'entrée).
- 2. Sauf dans le cas d'un *plan de défense* à impact limité (selon l'évaluation du *RC*), la défaillance d'un des éléments du *plan de défense* n'empêche pas le *BES* de respecter les mêmes exigences de performance que celles prescrites pour les événements et les conditions en vue desquels le *plan de défense* est conçu.
- 3. La conception du *plan de défense* facilite les opérations d'essai et d'entretien périodiques.
- 4. Le mécanisme ou la procédure d'armement du *plan de défense* est décrit clairement, et permet un armement et un fonctionnement fiables du *plan de défense* pour les événements et les conditions en vue desquels le *plan de défense* est conçu.

III. Retrait d'un *plan de défense*

L'examen du retrait proposé d'un *plan de défense* doit confirmer que le *plan de défense* n'est plus nécessaire.

Annexe 3

Information de la base de données

1. Nom du *plan de défense*.
2. Chaque entité propriétaire de *plan de défense* et ses coordonnées.
3. Date réelle ou prévue de mise en service, date d'approbation la plus récente par le *coordonnateur de la fiabilité* (exigence E3), date d'évaluation la plus récente (exigence E4) et date de retrait, le cas échéant.
4. Problème de performance du *réseau* ou autre raison qui motive le *plan de défense* (surcharge thermique, instabilité angulaire, amortissement incorrect d'oscillations, instabilité de la tension, surtension, sous-tension, rétablissement lent de la tension, etc.).
5. Description des *contingences* ou des conditions du *réseau* pour lesquelles le *plan de défense* a été conçu (conditions de déclenchement).
6. Actions que doit exécuter le *plan de défense*.
7. Désignation du *plan de défense* comme étant à impact limité ⁶.
8. Tout complément d'explication qui contribue à une compréhension de haut niveau du *plan de défense*.

6. Un *plan de défense* désigné comme étant à impact limité ne peut pas, en cas de fonctionnement intempestif ou de non-fonctionnement, donner lieu ou contribuer à des déclenchements en cascade, à une séparation fortuite, à une instabilité angulaire, à l'instabilité de la tension, à l'effondrement de la tension ou à des oscillations incorrectement amorties dans le *BES*.

Justification technique

4.1.1 Coordonnateur de la fiabilité

Le *coordonnateur de la fiabilité (RC)* est l'entité fonctionnelle la mieux placée pour procéder à l'examen du *plan de défense* : parmi toutes les entités fonctionnelles, c'est le *RC* qui a la vue d'ensemble la plus étendue en matière de fiabilité ; en outre, il est au courant des enjeux de fiabilité qui touchent les *zones de fiabilité* voisines. Sa vue d'ensemble sur la *zone étendue* facilite l'évaluation des interactions entre différents *plans de défense*, ainsi que des interactions entre les *plans de défense* et d'autres systèmes de protection et de contrôle. Par ailleurs, la désignation du *RC* pour ce rôle amenuise la possibilité d'un conflit d'intérêts découlant de relations d'affaires entre l'entité propriétaire de *plan de défense*, le *coordonnateur de la planification*, le *planificateur de réseau de transport* ou d'autres entités concernées par la planification ou la mise en service d'un *plan de défense*. Le *RC* est en outre moins susceptible d'être partie prenante à un *plan de défense*, et peut donc maintenir son impartialité.

4.1.2 Coordonnateur de la planification

Le *coordonnateur de la planification (PC)* est l'entité fonctionnelle la mieux placée pour procéder à l'évaluation du *plan de défense* : celle-ci consiste à vérifier le maintien de l'efficacité et de la coordination du *plan de défense*, ainsi qu'à connaître les impacts sur le réseau d'un fonctionnement intempestif du *plan de défense* ou de la défaillance d'un de ses éléments. Les points à évaluer sont notamment les suivants : 1) l'atténuation par le *plan de défense* de la ou des conditions ou incidents de *réseau* pour lesquelles il a été conçu ; 2) l'évitement des interactions nuisibles entre le *plan de défense* et d'autres *plans de défense* ou systèmes de protection et de contrôle ; 3) les effets d'un fonctionnement intempestif ; et 4) les effets d'une défaillance d'un élément du *plan de défense*. L'évaluation de ces points nécessite la modélisation et l'étude du réseau de transport interconnecté, à la manière des analyses de planification effectuées par les *PC*.

4.1.3 Entité propriétaire de plan de défense

L'expression « entité propriétaire de *plan de défense* » désigne tout *propriétaire d'installation de transport, propriétaire d'installation de production* ou *distributeur* qui possède la totalité ou une partie d'un *plan de défense*. Si tous les éléments d'un *plan de défense* ont un seul et même propriétaire, celui-ci assume l'entière responsabilité de toutes les activités imposées par la norme à l'entité propriétaire de *plan de défense*. Si les éléments d'un *plan de défense* ont différents propriétaires, chacun de ceux-ci est considéré comme une entité propriétaire de *plan de défense* et est tenu de participer à diverses activités prescrites par les exigences de la norme.

La norme n'impose pas de méthodes de conformité particulières. Les entités propriétaires de *plan de défense* ont l'option de collaborer entre elles afin de se conformer aux différentes exigences pertinentes. De tels efforts de collaboration et de coordination peuvent rendre plus efficace l'atteinte des objectifs de fiabilité des exigences ; cependant, chaque entité propriétaire de *plan de défense* doit pouvoir attester sa participation à l'effort de conformité. Par exemple, les différentes entités propriétaires d'un *plan de défense* pourraient collaborer afin de préparer et de soumettre ensemble l'information spécifiée à l'annexe 1 au *RC* chargé de l'examen du *plan de défense*, conformément à l'exigence E1.

Impact limité

Les *plans de défense* sont des assemblages uniques et personnalisés d'équipements de protection et de contrôle dont la complexité et l'impact sur la fiabilité du *BES* sont variables. Ces différences dans la

conception, le mode d'action et le risque pour le *BES* du *plan de défense* sont inventoriées et évaluées dans le cadre des exigences E1 à E4 de la norme PRC-012-2.

Le *RC* chargé de l'examen a le pouvoir de désigner un *plan de défense* comme étant à impact limité si celui-ci ne peut pas, en cas de fonctionnement intempestif ou de non-fonctionnement, donner lieu ou contribuer à des *déclenchements en cascade*, à une séparation fortuite, à une instabilité angulaire, à l'instabilité de la tension, à l'effondrement de la tension ou à des oscillations incorrectement amorties dans le *BES*. Il revient au *RC* chargé de l'examen de décider si un *plan de défense* mérite la désignation « à impact limité », à partir d'études et d'autres informations fournies conformément à l'annexe 1 par l'entité propriétaire du *plan de défense*.

La norme reconnaît la catégorie LAPS (automatisme de protection de zone locale) du WECC (Western Electricity Coordinating Council) et la catégorie Type III du NPCC (Northeast Power Coordinating Council) comme étant initialement appropriées pour la désignation « à impact limité ». L'information ci-après, qui décrit les catégories de *plans de défense* susmentionnées du WECC et du NPCC, est tirée de leurs documentations régionales respectives⁷. L'équipe de rédaction souligne que l'information présentée reflète l'état des processus régionaux du WECC et du NPCC au moment de l'élaboration de la norme PRC-012-2, et qu'elle peut avoir changé avant la date d'entrée en vigueur de cette norme.

WECC : catégorie LAPS (automatismes de protection de zone locale)

Plan de défense dont le non-fonctionnement n'entraînerait AUCUN des effets suivants :

- une non-conformité à la pratique régionale TPL-001-WECC-RBP, *System Performance Regional Business Practice* ;
- une perte de charge maximale d'au moins 300 MW ;
- une perte de production maximale d'au moins 1 000 MW.

NPCC : catégorie Type III

Automatisme de réseau dont le fonctionnement incorrect ou le non-fonctionnement n'entraînerait aucun **impact négatif important** à l'extérieur de la **zone locale**.

Les termes suivants sont également définis par le NPCC pour évaluer les impacts de l'*automatisme de réseau* aux fins de son classement :

Impact négatif important – En ce qui concerne la capacité de fonctionnement maximale des réseaux touchés, seront considérés comme ayant un impact négatif important une ou plusieurs des conditions ci-dessous découlant de défauts ou de perturbations :

- a. instabilité du réseau ;
- b. réponse dynamique inadmissible du réseau ou déclenchements d'équipements ;
- c. niveaux de tension contrevenant aux limites d'urgence applicables ;
- d. charges sur les installations de transport contrevenant aux limites d'urgence applicables ;
- e. perte de charge inadmissible.

Zone locale – Partie de réseau confinée électriquement ou de configuration radiale. L'étendue géographique de la zone et le nombre d'éléments de réseau qu'elle renferme varient selon les

7. WECC, *Procedure to Submit a RAS for Assessment – Information Required to Assess the Reliability of a RAS Guideline*, révision du 28 octobre 2013 | NPCC *Regional Reliability Reference Directory #7, Special Protection Systems*, version 2, 31 mars 2015.

caractéristiques du réseau. Une zone locale peut avoir une étendue relativement grande et comporter un nombre peu élevé de jeux de barres dans le cas d'un réseau à faible densité, ou une étendue assez restreinte et comporter un nombre relativement élevé de jeux de barres dans le cas d'un réseau à forte densité.

Si un *plan de défense* est mis en service avant la date d'entrée en vigueur de la norme PRC-012-2 et qu'il a été classé « LAPS » par le WECC ou « Type III » par le NPCC après avoir été soumis au processus d'examen régional pertinent, il est considéré comme un *plan de défense* à impact limité aux fins de la norme PRC-012-2 à la date d'entrée en vigueur de celle-ci, et il est soumis à toutes ses exigences pertinentes.

Pour pouvoir demander au RC chargé de l'examen de désigner un *plan de défense* existant (mis en œuvre avant la date d'entrée en vigueur de la norme PRC-012-2) comme étant à impact limité, l'entité propriétaire du *plan de défense* doit préparer et soumettre l'information prescrite à l'annexe 1, notamment la justification technique (les évaluations) que le *réseau* répond aux exigences de performance (alinéas 4.1.4 et 4.1.5 de l'exigence E4) en cas de défectuosité ou de défaillance, respectivement, d'un élément du *plan de défense*.

Rien n'empêche une entité propriétaire de *plan de défense* de travailler avec le RC chargé de l'examen pendant la période de mise en œuvre de la norme PRC-012-2, en attendant son entrée en vigueur. Cependant, même si le RC chargé de l'examen conclut que le *plan de défense* peut être désigné comme étant à impact limité, cette désignation n'est pas pertinente tant que la norme n'entre pas en vigueur. D'ici là, les processus régionaux existants continuent de s'appliquer, ainsi que les désignations existantes des *plans de défense*, ou l'absence de celles-ci.

Exemple de plan qui pourrait être considéré comme un *plan de défense* à impact limité : un système de délestage de charge ou de rejet de production servant à atténuer la surcharge d'une ligne de transport du BES. Le fonctionnement intempestif d'un tel système entraînerait la perte d'une certaine quantité de production ou de charge. L'évaluation par l'entité propriétaire du *plan de défense* devra démontrer que la perte de cette quantité de production ou de charge, sans que se produise réellement la contingence liée au fonctionnement du *plan de défense*, est acceptable et n'est pas préjudiciable à la fiabilité du BES, par exemple quant à la stabilité en fréquence et en tension. Par ailleurs, le non-fonctionnement de ce plan dans les conditions prévues pourrait entraîner la surcharge d'une ligne de transport au-delà de sa capacité acceptable. L'entité propriétaire du *plan de défense* devra démontrer que cette surcharge, bien que supérieure aux *caractéristiques assignées d'installation* de la ligne, n'est pas préjudiciable au BES à l'extérieur de la zone restreinte (prédéterminée par des études) touchée par la contingence.

Autres exemples de *plans de défense* à impact limité :

- Un plan qui sert à protéger des équipements du BES contre les dommages causés par une surtension, en commandant un rejet de production ou le déclenchement d'un équipement.
- Un plan de délestage en sous-tension à commande centralisée qui sert à protéger une zone restreinte (prédéterminée par des études) du BES contre l'effondrement de la tension.
- Un plan qui déclenche un groupe de production à la suite de certaines *contingences* dans le BES afin d'empêcher la désynchronisation de ce groupe par rapport au *réseau* ; étant entendu que si le *plan de défense* n'intervient pas et que le groupe décroche, les oscillations d'impédance apparente produites n'entraîneront pas le déclenchement d'*éléments* du *réseau* de transport à part le groupe de production et les installations qui y sont raccordées directement.

Exigence E1

Chaque *plan de défense* est unique et ses actions peuvent avoir des effets importants sur la fiabilité et l'intégrité du *système de production-transport d'électricité (BES)*. C'est pourquoi, avant de mettre en service un nouveau *plan de défense* ou un *plan de défense* existant dont le fonctionnement a été modifié, ou encore de retirer du service un *plan de défense*, il est indispensable de procéder à un examen approprié.

L'expression « dont le fonctionnement a été modifié » s'applique aux cas suivants :

- changements dans les conditions ou les *contingences* du *réseau* surveillées par le *plan de défense* ;
- changements dans les actions que le *plan de défense* est conçu pour exécuter ;
- changements dans les composants physiques du *plan de défense*, au-delà du remplacement à l'identique sans changement dans le fonctionnement initial de composants existants ;
- changements à la logique du *plan de défense*, au-delà de la correction d'erreurs existantes ;
- changements dans les niveaux de redondance (ajout ou retrait).

Pour illustrer les limites du remplacement à l'identique d'un élément de *plan de défense*, prenons le cas du remplacement d'un relais (ou autre composant) par un autre relais (ou autre composant) ayant des fonctions semblables. Par exemple, si un *plan de défense* comporte un relais CO-11 qui est remplacé par un relais IAC-53, il s'agit d'un remplacement à l'identique. Si le relais CO-11 est remplacé par un relais SEL-451 à microprocesseur ayant strictement les mêmes fonctions que le relais CO-11 d'origine, il s'agit aussi d'un remplacement à l'identique. Par contre, si le relais SEL-451 vise à ajouter une nouvelle logique par rapport à celle du relais CO-11, il s'agit dans ce cas d'une modification du fonctionnement.

Les changements aux seuils de sensibilité d'un *plan de défense* qui ne requièrent aucun autre changement ne sont pas considérés comme une modification du fonctionnement. Par exemple, les conditions du *réseau* nécessitent qu'un *plan de défense* soit armé lorsque le transit combiné sur deux lignes dépasse 500 MW ; si une évaluation périodique selon l'exigence E4 (ou toute autre évaluation) indique que le seuil d'armement devrait être réduit à 450 MW sans aucun autre changement dans le *plan de défense*, il ne s'agit pas d'une modification du fonctionnement. De même, si un *plan de défense* commande un délestage afin de réduire la charge sur une ligne au-dessous de 1 000 A, le fait de changer le seuil de délestage de 1 000 A à 1 100 A ne constitue pas une modification du fonctionnement.

Un autre exemple présente un cas où un changement dans le *réseau* nécessiterait de modifier le fonctionnement d'un *plan de défense*. Considérons un centre de production raccordé à un centre de consommation par deux lignes de transport. Ces lignes n'ont pas chacune une capacité suffisante pour faire transiter la production totale de la centrale si une des lignes est hors service. Le *plan de défense* surveille donc l'état des deux lignes et interrompt la production ou la ramène un niveau sécuritaire en cas de perte de l'une ou l'autre des lignes. Plus tard, une dérivation est raccordée à une des lignes pour alimenter une charge supplémentaire. Le *réseau* sur lequel agit le *plan de défense* comprend désormais trois lignes, et la perte d'une quelconque d'entre elles peut nécessiter une réduction de production. Il faut modifier le *plan de défense* pour surveiller les trois lignes (ajout de deux entrées d'état de ligne au *plan de défense*) et mettre à jour la logique qui sert à détecter l'indisponibilité de l'une ou l'autre des lignes ; par ailleurs, la réduction de production (signal de sortie du *plan de défense*) peut ou non être modifiée, selon la ligne qui est hors service. Ces changements au *plan de défense* constituent une modification de fonctionnement.

Toute modification du fonctionnement d'un *plan de défense* doit être examinée et approuvée selon le processus décrit aux exigences E1, E2 et E3. Le besoin de telles modifications peut être déterminé de différentes façons, notamment, sans restriction aucune, les évaluations de planification prescrites à l'exigence E4, un fonctionnement incorrect constaté selon l'exigence E5, un échec aux essais prescrits à l'exigence E8, ou encore des évaluations de planification liées à des ajouts ou à des modifications futures d'autres installations.

L'alinéa 4 a) de la section Mise en œuvre ci-après concernant l'annexe 1, à la présente section Compléments, donne des exemples d'éléments de *plan de défense* dont on peut envisager la défaillance. Le RC est libre de déterminer quels éléments doivent être considérés comme des éléments du *plan de défense* pendant son examen.

Afin de faciliter un examen qui renforce la fiabilité, la ou les entités propriétaires de *plan de défense* doivent fournir au RC chargé de l'examen suffisamment de détails sur la conception, la fonction et le fonctionnement du *plan de défense*. Ces informations et la documentation à l'appui sont précisées à l'annexe 1 de la norme ; l'exigence E1 oblige la ou les entités propriétaires de *plan de défense* à les fournir au RC chargé de l'examen. Le RC qui coordonne la zone dans laquelle est situé le *plan de défense* est chargé de l'examen. Si le *plan de défense* recoupe plusieurs *zones de fiabilité*, chaque RC concerné est chargé soit d'effectuer son propre examen, soit de participer à un examen coordonné.

L'exigence E1 ne spécifie pas combien de temps avant la mise en service la ou les entités propriétaires du *plan de défense* doivent fournir au RC chargé de l'examen l'information prescrite à l'annexe 1. Cette information devra être transmise suffisamment tôt, compte tenu du délai accordé au RC selon l'exigence E2 pour procéder à l'examen, ainsi que du temps nécessaire pour corriger tout problème de fiabilité qui pourrait être décelé, avant l'approbation finale du RC chargé de l'examen. La transmission diligente de cette information est dans l'intérêt de chaque entité propriétaire du *plan de défense* afin que la mise en service puisse être faite dans les meilleurs délais.

Exigence E2

L'exigence E2 demande au RC de procéder à l'examen de tout nouveau *plan de défense* proposé et de tout *plan de défense* existant dont une modification du fonctionnement ou le retrait est proposé dans sa *zone de fiabilité*.

Les *plans de défense* sont des assemblages uniques et personnalisés d'équipements de protection et de contrôle. Ils présentent donc le potentiel d'entraîner des risques pour la fiabilité du BES à moins d'être planifiés, conçus et installés avec soin. Un *plan de défense* peut avoir pour but de corriger un problème de fiabilité ou de produire un avantage économique ou opérationnel, mais il peut entraîner par ailleurs des risques pour la fiabilité, dont la ou les entités qui en sont propriétaires peuvent ne pas avoir conscience. Un examen indépendant par une équipe multidisciplinaire de spécialistes en planification, en exploitation, en protection, en télécommunications et en équipement est un moyen efficace de déceler les risques et de recommander des correctifs au *plan de défense* si nécessaire.

Le RC est l'entité fonctionnelle la mieux placée pour procéder à l'examen du *plan de défense* : parmi toutes les entités fonctionnelles, c'est le RC qui a la vue d'ensemble la plus étendue en matière de fiabilité ; en outre, il est au courant des enjeux de fiabilité qui touchent les *zones de fiabilité* voisines. Sa vue d'ensemble sur la *zone étendue* facilite l'évaluation des interactions entre différents *plans de défense* ainsi que des interactions entre les *plans de défense* et d'autres systèmes de protection et de contrôle.

Par ailleurs, la désignation du RC pour ce rôle amenuise la possibilité d'un conflit d'intérêts découlant de relations d'affaires entre l'entité propriétaire de *plan de défense*, le PC, le *planificateur de réseau de*

transport (TP) ou d'autres entités concernées par la planification ou la mise en service du *plan de défense*. Le RC peut demander à d'autres entités comme le ou les PC ou les groupes techniques régionaux (par exemple les *entités régionales*) de l'aider pour l'examen du *plan de défense* ; cependant, le RC demeure responsable de la conformité avec l'exigence. Il est entendu que le RC ne détient pas plus d'informations ou de compétences que ne l'indique son inscription à titre d'entité fonctionnelle selon les critères de la NERC. Le modèle fonctionnel de la NERC est un guide concernant l'élaboration des normes et leur applicabilité, et ne comporte pas d'exigences de conformité. Si une norme de fiabilité invoque des fonctions qui ne sont pas décrites dans le modèle, les exigences de la norme ont préséance sur le modèle fonctionnel. Pour de plus amples détails, consulter la section Introduction du modèle de fiabilité de la NERC, version 5, novembre 2009. L'annexe 2 de la présente norme propose une liste de contrôle pour aider le RC à déterminer les paramètres de conception et de mise en œuvre d'un *plan de défense*, et pour faciliter une démarche d'examen uniforme des différents *plans de défense* soumis pour examen. Le délai de quatre mois civils concorde avec la pratique courante dans l'industrie ; cependant, l'exigence prévoit une certaine latitude puisqu'elle permet aux parties de négocier un calendrier différent pour l'examen. Il est à noter qu'un RC peut devoir inclure cette tâche dans son ou ses plans de fiabilité pour la ou les régions de la NERC où il est situé.

Exigence E3

L'exigence E3 stipule que chaque entité propriétaire de *plan de défense* doit corriger tous les problèmes de fiabilité liés à son *plan de défense* signalés par le ou les RC chargés de l'examen. Les problèmes de fiabilité possibles concernent notamment la sûreté de fonctionnement, la sécurité ou la coordination. On considère que le *plan de défense* est approuvé lorsque les résultats d'examen transmis par le RC à chaque entité propriétaire de *plan de défense* indiquent soit que l'examen n'a décelé aucun problème de fiabilité, soit que tous les problèmes de fiabilité décelés ont été corrigés à la satisfaction du RC.

La sûreté de fonctionnement est l'une des composantes de la notion de fiabilité ; elle exprime le degré de certitude qu'un appareil interviendra dans les circonstances prévues. Si un *plan de défense* est mis en place pour assurer la conformité aux exigences de performance des normes de fiabilité de la NERC, tout non-fonctionnement de ce *plan de défense* lorsque la ou les *contingences* ou conditions de *réseau* spécifiées se produisent entraînerait un risque de non-conformité aux normes de fiabilité. Afin d'atténuer ce risque, on conçoit le *plan de défense* de façon qu'il puisse remplir sa fonction même en cas de défaillance d'un de ses éléments ; à cette fin, on opte souvent pour la redondance. D'autres stratégies visant à assurer la sûreté de fonctionnement comprennent le surdimensionnement de la coupure de charge ou de production, ou l'installation d'automatismes de relève.

La sécurité est une autre composante de la notion de fiabilité ; elle indique la confiance que l'appareil n'interviendra pas de façon intempestive. Le fonctionnement intempestif d'un *plan de défense* déclenche une action programmée sans que les conditions d'armement soient remplies, ou en dehors de la ou des *contingences* ou conditions de *réseau* spécifiées. Typiquement, un *plan de défense* commande un délestage de charge, un rejet de production ou une reconfiguration du *réseau* ; de telles actions, si elles surviennent de façon injustifiée, sont néfastes et peuvent compromettre la sécurité du *réseau*. Le pire scénario de fonctionnement intempestif est celui où toutes les actions programmées du *plan de défense* sont déclenchées. Si la performance du *réseau* est encore conforme à l'alinéa 4.3 de l'exigence E4 de la norme PRC-012-2, aucune mesure d'atténuation supplémentaire n'est requise. Des moyens de renforcement de la sécurité intrinsèque d'un *plan de défense* comme des logiques de décision sont des mesures d'atténuation acceptables contre les fonctionnements intempestifs.

Tout problème de fiabilité décelé pendant l'examen doit être corrigé avant la mise en service du *plan de défense*, afin d'éviter que le *réseau* ne soit exposé à un risque indu. L'entité propriétaire du *plan de*

défense ou le ou les RC chargés de l'examen peuvent envisager différents moyens pour corriger le problème. Quoi qu'il en soit, le critère primordial est celui de la fiabilité, et la décision finale revient au RC.

Il n'est pas nécessaire de spécifier un délai particulier pour la réponse de l'entité propriétaire du *plan de défense* à l'examen par le RC, puisqu'une réponse diligente est dans l'intérêt de chaque entité propriétaire du *plan de défense*, en principe désireuse de procéder à la mise en service dans les meilleurs délais

Il n'est pas non plus nécessaire de spécifier un délai particulier pour la réponse du RC à l'entité propriétaire du *plan de défense* à la suite de l'examen, car le RC est au courant 1) de tout problème de fiabilité qui perdure tant que le *plan de défense* n'aura pas été mis en service, et 2) du calendrier prévu par l'entité propriétaire du *plan de défense* pour mettre celui-ci en service afin de résoudre ces problèmes de fiabilité. Comme le RC est l'arbitre ultime de la fiabilité du BES, la résolution des problèmes de fiabilité est une priorité pour le RC et incite celui-ci à répondre sans délai à l'entité propriétaire du *plan de défense*.

Exigence E4

L'exigence E4 stipule que chaque *plan de défense* doit être évalué au moins une fois toutes les cinq années civiles. Cette évaluation périodique vise à confirmer le maintien de l'efficacité et de la coordination du *plan de défense*, ainsi qu'à vérifier que les exigences de performance du BES en cas de fonctionnement intempestif du *plan de défense* ou de défaillance d'un de ses éléments sont toujours remplies. Une évaluation périodique est exigée parce que des changements dans la topologie ou les conditions d'exploitation du *réseau* peuvent remettre en question l'efficacité du *plan de défense* ou la manière dont celui-ci interagit avec le BES et influe sur son fonctionnement.

Un *plan de défense* désigné comme étant à impact limité ne peut pas, en cas de fonctionnement intempestif ou de non-fonctionnement, donner lieu ou contribuer à des *déclenchements en cascade*, à une séparation fortuite, à une instabilité angulaire, à l'instabilité de la tension, à l'effondrement de la tension ou à des oscillations incorrectement amorties dans le BES. C'est pourquoi les *plans de défense* à impact limité sont dispensés des essais de défektivité et de défaillance d'un de leurs éléments (alinéas 4.1.4 et 4.1.5, respectivement). Pour ce type de *plan de défense*, de tels essais obligeraient à complexifier la conception, sans guère de bienfait pour la fiabilité du BES.

Un *plan de défense* mis en service après la date d'entrée en vigueur de la présente norme ne peut être considéré comme étant à impact limité que sur décision du RC chargé de l'examen. Si un *plan de défense* est mis en service avant la date d'entrée en vigueur de la norme PRC-012-2 et qu'il a été classé « LAPS » par le WECC ou « Type III » par le NPCC après avoir été soumis au processus d'examen régional pertinent, il est considéré comme un *plan de défense* à impact limité aux fins de la norme PRC-012-2 à la date d'entrée en vigueur de celle-ci, et il est soumis à toutes ses exigences pertinentes.

L'exigence E4 précise aussi que les essais de défaillance d'un élément et les essais de fonctionnement intempestif ne s'appliquent pas aux *plans de défense* à impact limité. Pour ce type de *plan de défense*, de tels essais obligeraient à complexifier la conception, sans guère de bienfait pour la fiabilité du BES.

Pour les *plans de défense* existants, le délai de cinq années civiles de l'exigence E4 s'applique initialement à compter de la date d'entrée en vigueur de la norme PRC-012-2. Dans le cas d'un *plan de défense* nouveau ou dont le fonctionnement est modifié, le délai de cinq années civiles s'applique initialement à compter de la date d'approbation du *plan de défense* par le RC chargé de l'examen. Le délai de cinq années civiles a été choisi comme intervalle maximal entre les évaluations à partir des valeurs adoptées pour des exigences semblables dans les normes de fiabilité PRC-006, PRC-010 et

PRC-014. On peut procéder plus tôt à l'évaluation du *plan de défense* si l'on considère que des changements importants à la topologie de *réseau* ou à ses conditions d'exploitation peuvent remettre en question l'efficacité ou la coordination du *plan de défense*. Des changements dans le *réseau* peuvent aussi amener à reconsidérer les effets d'un *plan de défense* à impact limité sur la fiabilité du *BES* ; l'alinéa 4.1.3 de l'exigence E4 demande explicitement de réévaluer périodiquement si la désignation « à impact limité » d'un *plan de défense* est toujours justifiée. L'évaluation périodique d'un *plan de défense* produit habituellement un des trois résultats suivants : 1) la confirmation que le *plan de défense* existant est adéquat ; 2) la description des correctifs à apporter au *plan de défense* ; ou 3) la justification du retrait du *plan de défense*.

Les conditions visées par l'évaluation (alinéas 4.1.1 à 4.1.5 de l'exigence E4) nécessitent des analyses de planification qui peuvent amener à modéliser le réseau de transport interconnecté afin d'évaluer la performance du *BES*. Le *PC* est l'entité fonctionnelle la mieux placée pour réaliser ces analyses puisqu'il a une bonne vue d'ensemble de la planification dans une zone étendue. Dans l'intérêt de la fiabilité, le *PC* est tenu de transmettre les résultats de son évaluation à chaque *TP* et *PC* concerné, ainsi qu'à chaque *RC* chargé de l'examen et entité propriétaire de *plan de défense*. Si le *plan de défense* recoupe les territoires de plusieurs *PC*, chaque *PC* concerné est tenu soit d'effectuer sa propre évaluation, soit de participer à une évaluation coordonnée.

L'alinéa 4.1.4 de l'exigence E4 vise à vérifier qu'un fonctionnement intempestif éventuel du *plan de défense* (sauf s'il est à impact limité) causé par une défectuosité d'un de ses éléments respecte les mêmes exigences de performance du *réseau* que pour les *contingences* ou conditions du *réseau* pour lesquelles il est conçu. Si le *plan de défense* est conçu pour répondre à un des événements de planification (P0 à P7) de la norme TPL-001-4, le fonctionnement intempestif éventuel du *plan de défense* doit respecter les exigences de performance spécifiées dans cette norme pour l'événement de planification en question. L'exigence précise que le seul cas de fonctionnement intempestif visé est celui causé par la défectuosité d'un seul des éléments du *plan de défense*. On pourra intégrer au *plan de défense* des fonctions de sécurité qui empêchent que la défectuosité d'un élément entraîne un fonctionnement intempestif ; sinon, le fonctionnement intempestif du *plan de défense* doit satisfaire à l'alinéa 4.1.4.

L'alinéa 4.1.4 de l'exigence E4 vise aussi à vérifier qu'un fonctionnement intempestif éventuel d'un *plan de défense* (sauf s'il est à impact limité) installé en prévision d'un événement extrême spécifié dans la norme TPL-001-4 ou de certaines autres *contingences* ou conditions du *réseau* non définies dans la norme TPL-001-4 (donc sans exigences de performance) respecte les exigences minimales de performance du *réseau* de la catégorie P7 du tableau 1 de la norme TPL-001-4 [où elles sont appelées « critères de comportement »]. Toutefois, au lieu de renvoyer à la norme TPL, l'exigence énonce directement les exigences de performance du *réseau* qu'un fonctionnement intempestif éventuel doit respecter. Les exigences de performance énoncées (alinéas 4.1.4.1 à 4.1.4.5 de l'exigence E4) sont celles qui sont communes à tous les événements de planification (P0 à P7) traités dans la norme TPL-001-4.

En ce qui a trait à l'alinéa 4.1.4 de l'exigence E4, soulignons que les seules différences d'exigences de performance entre les événements (P0 à P7) de la norme TPL (exigences non communes à tous ces événements) concernent la *perte de charge non subordonnée à une protection* et l'interruption de *service de transport ferme*. Il n'est pas nécessaire de spécifier à l'alinéa 4.1.4 les exigences de performance relatives à ces cas puisqu'un *plan de défense* est autorisé à délester une charge non subordonnée à une protection ou à interrompre un service de transport ferme uniquement si cette action est permise pour la *contingence* visée par le *plan de défense*. Par conséquent, le fonctionnement intempestif doit nécessairement respecter les exigences de performance applicables à une *perte de*

charge non subordonnée à une protection ou à l'interruption du *service de transport ferme* pour la ou les contingences visées par le *plan de défense*.

L'alinéa 4.1.5 de l'exigence E4 a pour objet de vérifier qu'une défaillance d'un élément du *plan de défense* (sauf dans le cas d'un *plan de défense* à impact limité), dans une situation où il est prévu que le *plan de défense* fonctionne, n'empêche pas le BES de respecter les mêmes exigences de performance (définies dans la norme de fiabilité TPL-001-4 [où elles sont appelées « critères de comportement »] ou toute norme qui la remplace) que celles prescrites pour les événements et les conditions en vue desquels le *plan de défense* est conçu. Cette vérification est nécessaire pour confirmer que des changements dans les conditions du *réseau* n'ont pas eu pour conséquence que l'exigence relative à la défaillance d'un élément du *plan de défense* n'est plus respectée.

Voici un exemple de défaillance d'un élément qui entraîne le non-respect des exigences de performance du *réseau* pour l'événement P1 visé par un *plan de défense*. Considérons le cas où un défaut triphasé (événement P1) entraînerait l'instabilité d'une centrale électrique (non-respect des exigences de performance [« critères de comportement »] du *réseau* de la norme TPL-001-4). En vue d'une telle éventualité, un *plan de défense* est mis en place afin de débrancher un seul des groupes de production et de préserver ainsi la stabilité des autres groupes de la centrale. Si la défaillance d'un élément (par exemple un relais) de ce *plan de défense* a pour effet que celui-ci ne fonctionne pas lors de l'événement P1, la centrale électrique deviendrait alors instable (ce qui contreviendrait aux exigences de performance [« critères de comportement »] du *réseau* de la norme TPL-001-4 pour un événement P1).

L'alinéa 4.1.5 de l'exigence E4 ne spécifie pas que tous les *plans de défense* doivent avoir des éléments redondants. Par exemple :

- Prenons le cas d'un *plan de défense* qui sert à atténuer un événement extrême selon la norme TPL-001-4. Il n'existe pas d'exigences de performance du *réseau* pour les événements extrêmes ; par conséquent, le *plan de défense* n'a pas besoin de redondance pour respecter les mêmes exigences de performance que celles prescrites pour les événements et les conditions en vue desquels il a été conçu.
- Prenons le cas d'un *plan de défense* qui arme une plus grande quantité de charge ou de production que nécessaire, de sorte que même si le *plan de défense* se trouve incapable de couper une partie de la charge ou de la production prévue en raison de la défaillance d'un de ses éléments, la performance du *réseau* restera satisfaisante ; par ailleurs, la coupure de la quantité totale de charge ou de production ne doit pas entraîner d'autres effets nuisibles pour la fiabilité.

L'évaluation périodique ne comprend pas un nouvel examen de la mise en œuvre physique du *plan de défense*, puisque ce point a déjà été confirmé par le RC lors de l'examen initial et validé par des essais fonctionnels subséquents. Cependant, il est possible qu'un *plan de défense* qui respectait antérieurement les exigences relatives au fonctionnement intempestif et à la défaillance d'un élément par des moyens autres que la redondance ne respecte plus ces exigences par la suite, et qu'il faille alors procéder à une réévaluation en fonction du *réseau* courant. Par exemple, si les actions d'un *plan de défense* comprennent un délestage de charge, la croissance de la charge sur une certaine période pourrait modifier la quantité de charge délestée ; ainsi, en cas de fonctionnement intempestif, la charge délestée pourrait s'avérer excessive, ce qui entraînerait des violations de *caractéristiques assignées d'installation*. Ou encore, le *plan de défense* pourrait être conçu pour délester plus de charge que nécessaire (« surdimensionnement ») afin de respecter les exigences de défaillance d'un élément. En effet, des changements dans le *réseau* pourraient faire en sorte que le volume de délestage soit

insuffisant, ce qui entraînerait une performance du *BES* inacceptable si une partie de la charge prévue n'était pas délestée.

Exigence E5

Le fonctionnement correct d'un *plan de défense* est important pour le maintien de la fiabilité et de l'intégrité du *BES*. Tout fonctionnement incorrect indique que l'efficacité ou la coordination du *plan de défense* peut avoir été compromise. Par conséquent, chaque fonctionnement d'un *plan de défense* et chaque non-fonctionnement dans une situation où il aurait dû fonctionner doivent être analysés afin de déterminer si le fonctionnement du *plan de défense* concorde bien avec le fonctionnement et la conception voulus.

L'analyse de la performance opérationnelle d'un *plan de défense* vise : 1) à vérifier si le fonctionnement du *plan de défense* concorde bien avec sa conception à la mise en service ; ou 2) à découvrir les lacunes du *plan de défense* qui se sont manifestées dans son fonctionnement incorrect ou encore son non-fonctionnement dans une situation prévue.

Le délai de 120 jours civils pour l'analyse de performance opérationnelle d'un *plan de défense* correspond au délai prescrit à l'exigence E1 de la norme PRC-004-4 pour l'enquête sur le *fonctionnement incorrect* d'un *système de protection* ; cependant, les parties sont libres de s'entendre sur un calendrier différent. Dans l'intérêt de la fiabilité, toute entité propriétaire du *plan de défense* doit transmettre les résultats d'analyse de performance opérationnelle à son ou ses *RC* chargés de l'examen si l'analyse révèle une lacune.

La ou les entités propriétaires du *plan de défense* peuvent avoir besoin de collaborer avec le *TP* concerné pour réaliser une analyse approfondie de la performance opérationnelle du *plan de défense*. En effet, l'analyse de performance opérationnelle nécessite de vérifier que le *plan de défense* a été déclenché adéquatement (alinéa 5.1.1), qu'il a fonctionné comme prévu (alinéa 5.1.2) et que la réaction du *BES* (alinéas 5.1.3 et 5.1.4) correspond bien à la conception du *plan de défense*. Si un *plan de défense* a plusieurs entités propriétaires, il serait souhaitable que celles-ci collaborent pour réaliser et soumettre une seule analyse de performance opérationnelle coordonnée.

Exigence E6

Toute lacune dans un *plan de défense* représente un risque potentiel pour la fiabilité du *BES*. De telles lacunes peuvent être découvertes lors de l'évaluation périodique effectuée par le *PC* selon l'exigence E4, de l'analyse de performance opérationnelle réalisée par l'entité propriétaire du *plan de défense* selon l'exigence E5, ou de l'essai fonctionnel effectué par l'entité propriétaire du *plan de défense* selon l'exigence E8. Afin d'atténuer les risques potentiels pour la fiabilité, l'exigence E6 stipule que chaque entité propriétaire de *plan de défense* doit participer à élaborer un *plan d'actions correctives* (*CAP*) qui établit des mesures correctives et un calendrier pour leur mise en œuvre.

La ou les entités propriétaires d'un *plan de défense* sont responsables de ses équipements ; elles sont donc les mieux placées pour établir les échéanciers et corriger les lacunes du *plan de défense*. Si nécessaire, la ou les entités propriétaires du *plan de défense* peuvent demander à d'autres entités, comme le *TP* ou le *PC*, de les aider dans l'élaboration du *CAP* ; cependant, la conformité à cette exigence incombe toujours aux entités propriétaires de *plan de défense*.

Un *CAP* peut nécessiter de modifier le fonctionnement du *plan de défense*. Dans ce cas, les exigences E1, E2 et E3 s'appliquent : l'information de l'annexe 1 doit être transmise au *RC* chargé de l'examen, et le *RC* doit procéder à l'examen et transmettre son approbation avant que l'entité propriétaire du *plan de défense* puisse mettre en service sa version modifiée.

Selon la complexité du problème, l'élaboration d'un plan d'actions correctives (*CAP*) peut nécessiter une analyse, des études d'ingénierie ou des services-conseils. Un délai de six mois civils est prévu pour donner à l'entité propriétaire du *plan de défense* le temps d'élaborer le *CAP* avec les collaborations nécessaires, tout en maintenant l'exigence d'un délai raisonnable pour corriger la lacune. Idéalement, si un *plan de défense* a plusieurs entités propriétaires, celles-ci devraient collaborer afin d'élaborer et de présenter un *CAP* commun. La lacune découverte dans le *plan de défense* peut amener le *RC* ou l'*exploitant de réseau de transport (TOP)* à imposer des restrictions d'exploitation afin d'assurer la fiabilité du *réseau* jusqu'à ce que la lacune soit corrigée. La possibilité de telles restrictions d'exploitation incitera du reste les entités propriétaires de *plan de défense* à corriger la lacune aussi rapidement que possible.

Voici quelques exemples de situations dans lesquelles un *CAP* est nécessaire :

- La détermination, après une enquête sur le fonctionnement ou le non-fonctionnement d'un *plan de défense*, que celui-ci ne répond pas aux attentes en matière d'efficacité ou n'a pas fonctionné conformément à ses critères de conception.
- Une évaluation de la planification périodique qui conclut au besoin de modifier un *plan de défense* afin de corriger des problèmes de performance ou de coordination.
- Une panne d'équipement.
- Un essai fonctionnel au cours duquel le *plan de défense* n'a pas fonctionné conformément à ses critères de conception.

Exigence E7

L'exigence E7 demande à chaque entité propriétaire de *plan de défense* de mettre en œuvre son *CAP* élaboré selon l'exigence E6 afin de corriger les lacunes décelées selon les exigences E4, E5 ou E8. Par définition, un *CAP* est « une liste des actions, avec leurs échéances, à mettre en œuvre pour remédier à un problème particulier ».

Un *CAP* peut être modifié au besoin si des changements s'avèrent nécessaires dans ses activités ou son calendrier. Si le *CAP* est modifié, l'entité propriétaire du *plan de défense* doit aviser le ou les *RC* chargés de l'examen. Une fois le *CAP* achevé, l'entité propriétaire du *plan de défense* doit aussi aviser le ou les *RC*.

La mise en œuvre d'un *CAP* bien conçu permet de corriger les lacunes du *plan de défense* dans les meilleurs délais. Par ailleurs, la lacune découverte peut amener le *RC* ou le *TOP* à imposer des restrictions d'exploitation afin d'assurer la fiabilité du *réseau* jusqu'à ce que le *CAP* soit achevé. La possibilité de telles restrictions d'exploitation incitera du reste les entités propriétaires de *plan de défense* à achever le *CAP* aussi rapidement que possible.

Exigence E8

L'objectif de fiabilité de l'exigence E8 est de mettre à l'essai les éléments du *plan de défense* qui ne font pas partie d'un *système de protection* (par exemple les automates programmables) et de vérifier la performance globale du *plan de défense* au moyen d'essais fonctionnels. Les essais fonctionnels valident le bon fonctionnement du *plan de défense* en confirmant que les états du *réseau* sont détectés et traités, et que les commandes agissent correctement et dans le délai prévu, selon les réglages et la logique de service. Les essais fonctionnels concernent la performance globale du *plan de défense*, contrairement aux essais de la norme d'entretien PRC-005, qui visent les composants eux-mêmes.

Comme l'essai fonctionnel consiste à faire fonctionner le *plan de défense* dans des conditions contrôlées avec des états de *réseau* connus et des résultats prévus d'avance, les essais et l'analyse peuvent être effectués avec un impact minimal sur le *BES* et devraient correspondre aux résultats escomptés. L'entité propriétaire du *plan de défense* est l'entité la mieux placée pour établir les procédures et le calendrier d'essai étant donné sa connaissance étendue de la conception du *plan de défense*, de son installation et de son fonctionnement. Des essais périodiques donnent à l'entité propriétaire du *plan de défense* l'assurance que les défaillances latentes peuvent être décelées ; ils favorisent aussi la découverte de changements survenus dans le *réseau* et qui pourraient avoir créé des défaillances latentes.

Les intervalles de six et douze années civiles entre les essais fonctionnels sont plus longs que pour les essais annuels ou bisannuels effectués dans certaines régions de la NERC. Ces intervalles sont en fait un compromis entre, d'une part, les ressources requises pour effectuer les essais et, d'autre part, les impacts potentiels sur la fiabilité du *BES* qui découleraient de défaillances latentes non décelées, susceptibles de causer un fonctionnement incorrect du *plan de défense*. Un intervalle d'essai plus long pour les plans de défense à impact limité est acceptable, puisque le fonctionnement incorrect ou le non-fonctionnement de ces *plans de défense* présente un risque faible pour la fiabilité du *réseau de transport d'électricité* (selon la définition de *Bulk Power System* donnée dans 16 U.S. Code § 824o).

L'essai fonctionnel prescrit n'est pas synonyme d'essai intégral. Un essai intégral est un moyen valable, mais sans doute impraticable pour de nombreux *plans de défense* ; dans de tels cas, l'entité propriétaire de *plan de défense* peut effectuer des essais fonctionnels par segment. Les segments peuvent être mis à l'essai individuellement, ce qui évite le besoin de calendriers d'entretien complexes. On peut également utiliser les fonctionnements du *plan de défense* en conditions réelles pour répondre à l'exigence d'un essai fonctionnel. Si un *plan de défense* ne fonctionne pas intégralement pendant un événement de *réseau* ou si les conditions du *réseau* ne permettent pas un essai intégral, on aura alors recours à des essais par segment. Un essai fonctionnel comprend la mise à l'essai de toutes les entrées du *plan de défense* utilisées pour la détection, l'armement, le fonctionnement et la collecte de données. Cet essai, par défaut, actionne la logique de traitement et l'infrastructure du *plan de défense*, mais met l'accent sur les entrées du *plan de défense* et sur ses commandes de sortie qui agissent sur les conditions de *réseau* pour lesquels le *plan de défense* est conçu. Tous les segments et éléments du *plan de défense* doivent être mis à l'essai ou avoir fonctionné de façon documentée au cours de l'intervalle d'essai maximal applicable afin que la conformité à l'exigence puisse être démontrée.

Pour illustrer la notion d'essai par segment, prenons l'exemple d'un contrôleur de *plan de défense* dont la fonction est remplie par un automate programmable qui reçoit les données du *réseau*, comme la charge ou l'état des lignes, à partir de dispositifs dispersés : compteurs, relais de protection, autres automates programmables, etc. Dans cet exemple de *plan de défense*, un relais de protection de ligne fournit une mesure analogique à l'automate du *plan de défense*. Un essai fonctionnel vérifierait que l'automate reçoit bien les données transmises par le relais de protection, y applique les traitements prévus et produit des sorties appropriées. Il n'y a pas lieu de vérifier la capacité du relais de protection de mesurer les grandeurs du *réseau* électrique, car il s'agit d'une exigence visant les *systèmes de protection* utilisés comme *plans de défense*, dont le détail est énoncé au tableau 1-1 (Type de composant – Relais de protection) de la norme PRC-005. L'essai fonctionnel concerne plutôt l'utilisation des données du relais de protection par l'automate programmable, y compris le chemin de communication entre le relais et l'automate si ces données sont essentielles au bon fonctionnement du *plan de défense*. En outre, si le signal de commande retourné au relais de protection est lui aussi essentiel au bon fonctionnement du *plan de défense* de cet exemple, il faudra alors vérifier aussi le chemin de retour de ce signal jusqu'au relais. L'exemple présenté ici décrit l'essai d'un segment de *plan*

de défense qui sert à vérifier l'action du *plan de défense*, la logique de commande de l'automate programmable et les communications.

La norme IEEE C37.233, *IEEE Guide for Power System Protection Testing* (2009), à la section 8 (en particulier 8.3 à 8.5), donne un aperçu des essais fonctionnels. La section 8.3 commence ainsi :

Une bonne mise en œuvre nécessite un programme d'essais bien défini et coordonné pour évaluer la performance globale du système pendant les intervalles de maintenance convenus. Le programme d'essais de maintenance, aussi appelé programme d'essais fonctionnels de système, devrait s'appliquer aux entrées et sorties, aux communications, à la logique et au temps de traitement. Les essais fonctionnels ne visent généralement pas les éléments, mais plutôt l'ensemble du système. Certains essais sur les entrées peuvent devoir précéder les essais de l'ensemble du système dans la mesure où ces entrées influent sur la performance globale. Le ou les coordonnateurs des essais doivent connaître à fond le but visé par le plan, les points d'isolement, les scénarios de simulation ainsi que les procédures de retour au fonctionnement normal.

Il s'agit de valider la performance globale du système, y compris sa logique le cas échéant, de valider les temps de traitement totaux par comparaison avec la modélisation du système pour différents types de contingence, et de vérifier la performance du système ainsi que ses entrées et sorties.

Si un *plan de défense* réussit un essai fonctionnel, il n'est pas nécessaire d'en informer le RC, puisqu'il s'agit du résultat normal attendu et qu'il n'y a aucune suite à donner. Si un segment du *plan de défense* échoue, il faut signaler (en *temps réel*) l'état dégradé de ce *plan de défense* au TOP selon l'exigence E6 de la norme PRC-001, puis au RC selon l'exigence E8 de la norme TOP-001-3. (Voir la Phase 2 du projet 2007-06 pour consulter le document de correspondances entre la norme PRC-001 et les autres normes quant à la notification du RC par le TOP si une lacune est constatée pendant les essais.) Par conséquent, il n'est pas nécessaire d'inclure une exigence semblable dans la présente norme.

L'intervalle d'essai initial commence à la date d'entrée en vigueur de la norme, selon son plan de mise en œuvre. Par la suite, l'intervalle maximal admissible entre les essais fonctionnels est de six années civiles pour les *plans de défense* qui n'ont pas la désignation « à impact limité », et de douze années civiles pour ceux qui ont cette désignation. L'intervalle commence à la date de l'essai réussi le plus récent pour un segment ou pour l'intégralité du *plan de défense*. La réussite d'un essai de segment remet à zéro l'intervalle d'essai pour ce segment seulement. L'entité propriétaire d'un *plan de défense* peut choisir de compter un fonctionnement correct du *plan de défense* comme un essai fonctionnel admissible, mais seulement pour les segments qui ont fonctionné. Si un événement *réseau* entraîne un fonctionnement correct mais partiel du *plan de défense*, les segments qui n'ont pas fonctionné doivent être soumis à des essais fonctionnels séparés avant la fin de l'intervalle d'essai maximal qui a commencé à la date du précédent essai réussi pour ces segments (qui n'ont pas fonctionné) afin qu'il y ait conformité à l'exigence E8.

Exigence E9

La base de données sur les *plans de défense* que le RC doit mettre à jour conformément à l'exigence E9 assure la disponibilité de l'information sur les plans de défense existants. L'annexe 3 spécifie l'information minimale qui doit y être versée pour chaque *plan de défense* inscrit dans la base de données. Le RC peut demander des informations plus détaillées.

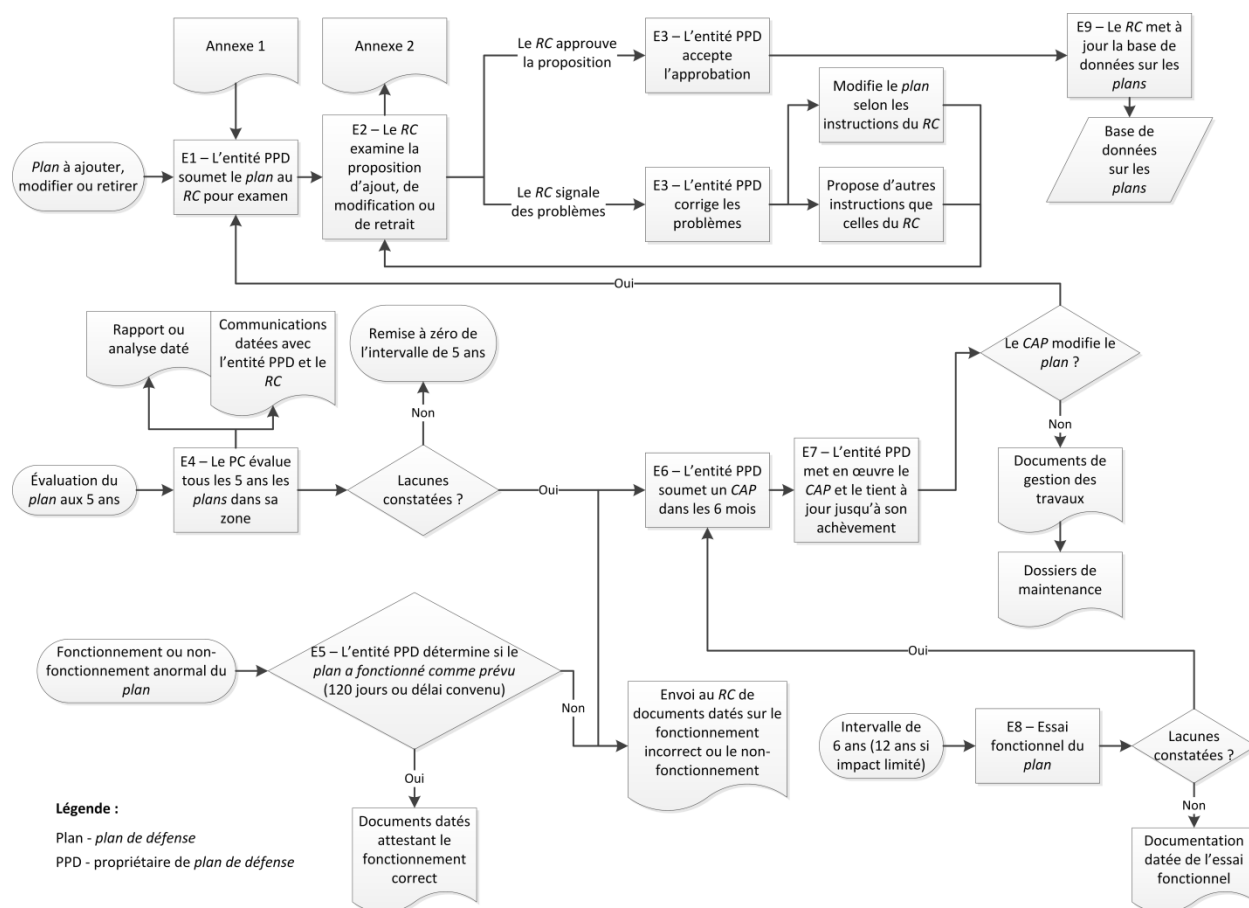
Cette base de données permet au RC de fournir à d'autres entités de l'information de haut niveau sur des *plans de défense* existants qui pourraient éventuellement influencer sur les activités d'exploitation ou

de planification de ces entités. L'information fournie est suffisante pour permettre à une entité ayant un besoin de fiabilité d'évaluer si le *plan de défense* est susceptible d'avoir un impact sur son *réseau*. Par exemple, un *plan de défense* qui effectue un rejet de production afin d'atténuer une surcharge sur une ligne de transport peut entraîner un changement de transit de puissance dans la zone d'une entité adjacente. Cette entité devrait pouvoir évaluer tout risque potentiel de ce *plan de défense* pour son réseau à partir de l'information de haut niveau disponible dans la base de données sur les *plans de défense*.

La base de données sur les *plans de défense* n'a pas à indiquer en détail les réglages d'équipement ou l'information de modélisation, mais doit contenir la description des problèmes de performance du *réseau*, les conditions du *réseau* et les actions correctives prévues. Si une entité souhaite obtenir des détails supplémentaires sur le fonctionnement d'un *plan de défense*, elle peut obtenir du RC les coordonnées de l'entité propriétaire du *plan de défense*.

Schéma de cheminement

Le schéma ci-dessous décrit le cheminement des processus liés aux exigences de la norme PRC-012-2.



Justifications techniques de l'annexe 1 – Documentation à fournir pour l'examen d'un *plan de défense*

Afin de permettre un examen adéquat des conséquences d'un *plan de défense* pour la fiabilité, il est nécessaire pour la ou les entités propriétaires du *plan de défense* de présenter au *coordonnateur de la fiabilité (RC)* chargé de l'examen une liste détaillée d'informations sur le *plan de défense*. Si le *plan de défense* a plusieurs entités propriétaires, chacune de celles-ci devra fournir l'information pertinente. Idéalement, dans de tels cas, une des entités propriétaires du *plan de défense* assumera la tâche de recueillir toutes les informations fournies afin de produire une compilation commune conforme à l'annexe 1.

Les informations nécessaires comprennent notamment un aperçu général du *plan de défense*, un résumé des résultats des études de planification du transport ainsi que des précisions sur l'équipement utilisé dans la mise en œuvre du *plan de défense*. La coordination entre le *plan de défense* et d'autres plans de défense et systèmes de protection et de contrôle sera examinée afin de déceler tout potentiel d'interaction nuisible. L'examen peut s'étendre à des aspects très variés de la conception électrique, notamment les composants utilisés, la logique, les télécommunications et d'autres équipements et commandes pertinents qui constituent le *plan de défense*.

Annexe 1

La liste de contrôle suivante indique les informations importantes que l'entité propriétaire d'un *plan de défense* nouveau ou dont le fonctionnement a été modifié⁸ doit documenter et présenter au RC chargé de l'examen, conformément à l'exigence E1. Si le *plan de défense* a été examiné antérieurement, seules les modifications proposées nécessitent un examen ; néanmoins, pour faciliter le travail du RC chargé de l'examen, l'entité propriétaire du *plan de défense* présentera un résumé du fonctionnement préexistant du *plan de défense*.

I. Généralités

1. Éléments d'information (cartes, schémas unifilaires, schémas de poste électrique, schémas de principe, etc.) qui indiquent l'emplacement physique et électrique du *plan de défense* et des installations connexes.

Fournir une description du *plan de défense* afin d'expliquer son fonctionnement global, ainsi qu'une carte indiquant son emplacement. Signaler tout autre système de protection et de contrôle qui nécessite une coordination avec le *plan de défense*. Les éléments de conception du *plan de défense* à présenter sont décrits plus bas.

Fournir un ou des schémas unifilaires pour tous les sites en cause. Ces schémas doivent être suffisamment détaillés pour permettre à l'équipe d'examen du RC d'évaluer la fiabilité de la conception, et doivent comprendre des informations comme la configuration des jeux de barres, les disjoncteurs, les équipements de commutation connexes, etc. Pour chaque site, indiquer si

8. L'expression « dont le fonctionnement a été modifié » s'applique à toute modification apportée à un *plan de défense*, parmi les suivantes :

- changements dans les conditions ou les contingences du réseau surveillées par le *plan de défense* ;
- changements dans les actions que le *plan de défense* est conçu pour exécuter ;
- changements dans les composants physiques du *plan de défense*, au-delà du remplacement à l'identique, sans changement dans le fonctionnement initial de composants existants ;
- changements à la logique du *plan de défense*, au-delà de la correction d'erreurs existantes ;
- changements dans les niveaux de redondance (ajout ou retrait).

des éléments de détection, de logique, de commande d'actions, ou toute combinaison de ceux-ci, sont présents.

2. Fonctionnement du nouveau *plan de défense* ou des modifications proposées au fonctionnement d'un *plan de défense* existant, avec documentation du fonctionnement du *plan de défense* avant et après les modifications.
3. *Plan d'actions correctives*, si des modifications d'un plan de défense sont proposées dans le cadre d'un *plan d'actions correctives*. [Référence : norme de fiabilité PRC-012-2 (exigences E5 et E7)]

Fournir la description de toute modification du fonctionnement du *plan de défense* liée à un *plan d'actions correctives (CAP)* visant à corriger des lacunes de fonctionnement signalées lors de l'évaluation périodique du *plan de défense* (exigence E4), de l'analyse de performance opérationnelle (exigence E5) ou de l'essai fonctionnel (exigence E8). Une copie du *CAP* le plus récent doit être fournie en plus des autres informations prescrites à l'annexe 1.

4. Données initiales à verser dans la base de données sur les *plans de défense*.
 - a. nom du *plan de défense* ;
 - b. chaque entité propriétaire de *plan de défense* et ses coordonnées ;
 - c. date réelle ou prévue de mise en service, date d'approbation la plus récente par le RC (exigence E3), date d'évaluation la plus récente (exigence E4) et date de retrait, le cas échéant ;
 - d. problème de performance du réseau ou autre raison qui motive le *plan de défense* (surcharge thermique, instabilité angulaire, amortissement incorrect d'oscillations, instabilité de la tension, surtension, sous-tension, rétablissement lent de la tension, etc.) ;
 - e. description des *contingences* ou des conditions du *réseau* pour lesquelles le *plan de défense* a été conçu (conditions de déclenchement) ;
 - f. actions commandées par le *plan de défense* ;
 - g. désignation du *plan de défense* comme étant à impact limité⁹ ;
 - h. tout complément d'explication qui contribue à une compréhension de haut niveau du *plan de défense*.

Remarque : Cette information est la même que celle indiquée à l'annexe 3. Le fait de la fournir à cette étape du processus d'examen assure un examen plus complet et allège le fardeau administratif éventuel du ou des RC chargés de l'examen.

II. Description fonctionnelle et information relative à la planification du transport

1. *Contingences* et conditions du *réseau* auxquelles le *plan de défense* est censé remédier. [Référence : normes de fiabilité PRC-012 (E1.2) et PRC-013 (E1.1)]
 - a. Indiquer ce qui se produirait dans le réseau en l'absence d'un *plan de défense*.

9. Un *plan de défense* désigné comme étant à impact limité ne peut pas, en cas de fonctionnement intempestif ou de non-fonctionnement, donner lieu ou contribuer à des *déclenchements en cascade*, à une séparation fortuite, à une instabilité angulaire, à l'instabilité de la tension, à l'effondrement de la tension ou à des oscillations incorrectement amorties dans le BES.

- b. Décrire les conditions du *réseau* qui commandent l'armement du *plan de défense* afin de le préparer à intervenir lorsque surviendront par la suite des *contingences* critiques de *réseau* ou d'autres conditions d'exploitation qui nécessiteraient le déclenchement du *plan de défense*. Si aucune condition d'armement n'est requise, le préciser également.
 - c. Les *plans de défense* spécifiques aux événements sont déclenchés par des *contingences* particulières qui nécessitent une intervention. Les *plans de défense* spécifiques aux conditions peuvent aussi être déclenchés par des *contingences* particulières, mais ce n'est pas forcément le cas. Les *contingences* ou les conditions de déclenchement doivent être indiquées.
2. Actions que doit exécuter le *plan de défense* en réponse à des perturbations. [Référence : normes de fiabilité PRC-012 (E1.2) et PRC-013 (E1.2)]

Le *plan de défense* exécute des actions correctives visant à assurer une performance acceptable du *réseau*. Ces actions doivent être décrites, y compris toute contrainte de temps ou toute action corrective « de réserve » prévue en cas de défaillance d'un élément du *plan de défense*.

3. Résumé d'études techniques, le cas échéant, démontrant que les actions du *plan de défense* proposé répondent aux objectifs de performance du *réseau* dans le cadre des événements et des conditions du *réseau* auxquels le *plan de défense* est censé remédier. Ce résumé d'études techniques doit préciser notamment les années étudiées, les conditions du *réseau* et les *contingences* analysées pour la conception du *plan de défense*, et la date à laquelle les études techniques ont été effectuées. [Référence : norme de fiabilité PRC-014 (E3.2)]

Présenter la raison d'être du *plan de défense* et ses effets afin de confirmer qu'il est (encore) nécessaire, qu'il répond bien au besoin visé et qu'il respecte les exigences de performance courantes. Il n'est sans doute pas nécessaire de fournir la version intégrale des études techniques, mais toute description abrégée de ces études doit être suffisamment détaillée pour permettre au RC chargé de l'examen de reconnaître le besoin du *plan de défense* et l'efficacité de ses résultats.

4. Information sur tout projet de développement du *réseau* susceptible d'influer sur le *plan de défense*. [Référence : norme de fiabilité PRC-014 (E3.2)]

Les autres responsabilités imposées au RC par les normes de fiabilité de la NERC portent sur l'*horizon d'exploitation* plutôt que sur l'*horizon de planification*. Le RC est donc moins susceptible d'avoir connaissance de plans à plus long terme qui pourraient influencer sur le *plan de défense* proposé. Une telle connaissance est utile afin d'évaluer plus justement les capacités du *plan de défense*.

5. Le cas échéant, désignation « à impact limité » proposée par l'entité propriétaire du *plan de défense*, avec justification.

Un *plan de défense* désigné comme étant à impact limité ne risque pas, en cas de fonctionnement intempestif ou de non-fonctionnement, de donner lieu ou de contribuer à des *déclenchements en cascade*, à une séparation fortuite, à une instabilité angulaire, à l'instabilité de la tension, à l'effondrement de la tension ou à des oscillations incorrectement amorties dans le BES. Si le *plan de défense* est mis en service avant la date d'entrée en vigueur de la norme PRC-012-2 et qu'il a été classé « LAPS » par le WECC ou « Type III » par le NPCC après avoir été soumis au processus d'examen régional pertinent, il est considéré comme un *plan de défense* à impact limité aux fins de la norme PRC-012-2 à la date d'entrée en vigueur de celle-ci, et il est soumis à toutes ses exigences pertinentes.

6. Documentation décrivant la performance du *réseau* résultant d'un fonctionnement intempestif possible du *plan de défense* (sauf si celui-ci est à impact limité) causé par la défectuosité d'un de ses éléments. En cas de défectuosité d'un élément d'un *plan de défense* non désigné comme étant à impact limité, toutes les conditions suivantes doivent être remplies : [Référence : norme de fiabilité PRC-012 (E1.4)]
 - a. le *BES* doit demeurer stable ;
 - b. il ne doit pas y avoir de *déclenchements en cascade* ;
 - c. les *caractéristiques assignées d'installation* pertinentes ne doivent pas être dépassées ;
 - d. les tensions du *BES* doivent demeurer en deçà des limites de tension *post-contingence* ainsi que des limites d'écart de tension *post-contingence* établies par le *planificateur de réseau de transport* et le *coordonnateur de la planification* ;
 - e. les réponses aux tensions transitoires doivent demeurer en deçà des limites acceptables établies par le *planificateur de réseau de transport* et le *coordonnateur de la planification*.
7. Évaluation confirmant que les réglages et le fonctionnement du *plan de défense* font en sorte d'éviter toute interaction nuisible avec d'autres *plans de défense* et systèmes de protection et de contrôle. [Référence : normes de fiabilité PRC-012 (E1.5) et PRC-014 (E3.4)]

Les *plans de défense* sont des plans complexes qui peuvent exécuter des actions comme une coupure de charge, un rejet de production ou une reconfiguration du *réseau*. De nombreux plans de défense ont besoin de détecter certaines configurations de *réseau* pour déterminer si leurs conditions d'armement sont remplies ou s'ils doivent intervenir. Exemple d'interaction nuisible : un *plan de défense* reconfigure le *réseau* d'une manière qui modifie aussi le courant de *défaut* applicable, ce qui peut compromettre la supervision de surintensité d'un relais de distance (« détecteur de défaut ») ainsi que la coordination des protections de surintensité à la terre.

8. Indication d'autres *RC* touchés.

Cette information est nécessaire pour les échanges d'information entre les différentes entités touchées et pour la coordination du *plan de défense* avec d'autres *plans de défense* et systèmes de protection et de contrôle.

III. Mise en œuvre

1. Documentation décrivant tout équipement pertinent utilisé pour la détection, l'alimentation c.c., les communications, le télédéclenchement, la logique de traitement, les actions de commande et la surveillance.

Détection

Les dispositifs de détection et de déclenchement, que ce soit pour l'armement ou l'exécution d'actions, doivent être conçus pour avoir un fonctionnement sûr. Plusieurs types de dispositifs sont couramment utilisés comme détecteurs de perturbation, de condition ou d'état :

- état de ligne ouverte (détecteurs d'événement) ;
- entrées et sorties de relais de protection (détecteurs d'événement et de paramètre) ;
- entrées (analogiques) de transducteur et de DEI (détecteurs de paramètre et de réponse) ;
- taux de variation (détecteurs de paramètre et de réponse).

Alimentation c.c.

Les batteries et les chargeurs, ou d'autres formes d'alimentation c.c. des *plans de défense*, sont aussi couramment utilisés pour les *systèmes de protection*. Cette pratique est acceptable ; l'entretien de telles alimentations est encadré par la norme PRC-005. Cependant, tout *plan de défense* redondant doit être alimenté à partir de circuits protégés séparément (par fusible ou par disjoncteur).

Communications : voies de télécommunications

Les voies de télécommunications utilisées pour les échanges d'information de *plan de défense* entre sites ou entre dispositifs de télédéclenchement doivent respecter au moins les mêmes critères que pour les systèmes de protection par relais. Expliquer le fonctionnement de tout système de communication non déterministe utilisé (par exemple, Ethernet).

La logique du *plan de défense* doit être conçue de façon que la perte d'une voie, la présence de bruit ou toute autre défaillance de voie ou d'équipement n'entraîne pas un fonctionnement intempestif du *plan de défense*.

Il est très souhaitable que les équipements de voie et les moyens de communication (courant porteur sur ligne de transport, liaison hertzienne, fibre optique, etc.) soient détenus et entretenus par l'entité propriétaire du *plan de défense*, ou éventuellement loués d'une autre entité bien au courant des exigences de fiabilité. Tous les équipements de voie doivent être surveillés à partir du centre de répartition et y déclencher des alarmes afin d'assurer un diagnostic et une réparation rapides en cas de défaillance. Le réseau téléphonique public commuté est généralement une option indésirable.

Les voies de communication doivent être bien étiquetées ou marquées de façon que le personnel qui y travaille puisse trouver facilement le bon circuit. Les voies entre entités doivent porter le même nom à tous les terminaux.

Télédéclenchement

L'équipement de télédéclenchement, s'il est à part des autres équipements du *plan de défense*, doit être surveillé et étiqueté de la même façon que l'équipement de voie.

Logique de traitement

Tout *plan de défense* nécessite une certaine forme de traitement logique pour déterminer les actions à exécuter en cas de déclenchement. Ces actions sont toujours subordonnées au *plan de défense*. Différentes actions peuvent correspondre à différents niveaux d'armement ou à différentes *contingences*. La logique de décision peut se limiter à des liaisons câblées entre quelques contacts auxiliaires de relais, ou prendre une forme beaucoup plus complexe.

Parmi les équipements qui ont fait leurs preuves, citons les automates programmables de divers types, les micro-ordinateurs, les relais de protection à microprocesseur, les stations terminales (RTU) et les processeurs logiques. Les relais monofonctionnels ont été utilisés dans le passé comme éléments de *plan de défense*, mais cette approche est maintenant moins répandue sauf pour de nouveaux plans de défense très simples ou pour des ajouts mineurs à des *plans de défense* existants.

Actions de commande

Les dispositifs actifs du *plan de défense* peuvent comprendre divers équipements, notamment des dispositifs de télédéclenchement et des relais de protection. Ces dispositifs reçoivent les signaux produits par la logique de traitement (parfois par l'entremise d'installations de télécommunications) et exécutent les actions du *plan de défense* aux endroits où ces actions sont requises.

Exigences minimales pour la surveillance SCADA-EMS

- État « en service » ou « hors service » du *plan de défense*.
 - Si le *plan de défense* est armé manuellement, l'état d'armement peut être le même que l'état en service ou hors service du *plan de défense*.
 - Si le *plan de défense* est armé automatiquement, ces deux états sont indépendants, car un *plan de défense* en service peut être armé ou non armé selon que les critères d'armement automatique sont remplis ou non.
 - État opérationnel courant du *plan de défense* (disponible ou non).
 - Si le *plan de défense* doit demeurer fonctionnel en cas de défaillance d'un de ses éléments (par redondance ou autrement), les indications minimales d'état doivent être fournies séparément pour chaque *plan de défense*.
 - Une indication minimale d'état est généralement suffisante du point de vue opérationnel ; cependant, si possible, il est souvent utile d'avoir d'autres informations sur des défaillances partielles ou sur l'état de composants critiques afin de permettre à l'entité propriétaire du *plan de défense* de diagnostiquer plus efficacement une défaillance signalée. L'existence ou non de cette capacité dépendra en partie de la conception et de l'âge de l'équipement du *plan de défense*. Tous les *plans de défense* doivent assurer un degré minimal de surveillance, mais les nouveaux *plans de défense* doivent être conçus pour une surveillance au moins semblable à celle des *systèmes de protection* à microprocesseur.
2. Information sur les réglages ou paramètres de la logique de détection qui commande le fonctionnement du *plan de défense*. [Référence : normes de fiabilité PRC-012 (E1.2) et PRC-013 (E1.3)]

Plusieurs méthodes permettant de déterminer l'état des lignes ou d'autres équipements sont couramment utilisées, souvent en combinaison :

- a. Contacts auxiliaires de disjoncteur et de sectionneur (52a/b et 89a/b) – Ce sont les dispositifs de surveillance les plus répandus. Le contact « a » indique l'état réel du disjoncteur, tandis que le contact « b » indique l'état opposé.
- b. Détection de minimum de courant – Une valeur faible indique un circuit ouvert, y compris à l'extrémité éloignée de la ligne ; le seuil de détection se trouve généralement juste au-dessus du courant de charge total de la ligne.
- c. Surveillance du courant de bobine de déclenchement d'un disjoncteur – Dispositif généralement utilisé si le *plan de défense* doit réagir très rapidement, mais normalement combiné avec des contacts auxiliaires ou un autre moyen de détection puisque le courant de la bobine de déclenchement est coupé lorsque le disjoncteur s'ouvre.
- d. Autres détecteurs (angle, tension, puissance, fréquence, taux de variation de ces grandeurs, perte de synchronisme, etc.), selon les besoins particuliers du *plan de défense*. Certains dispositifs peuvent remplacer ou améliorer d'autres moyens de surveillance décrits aux points a), b) et c) ci-dessus.

Le déclenchement de l'armement et des actions du *plan de défense* nécessite souvent la surveillance de grandeurs analogiques (puissance, courant, tension, etc.) à un ou plusieurs endroits. Les dispositifs de surveillance sont réglés pour détecter un niveau précis de la grandeur pertinente ; il peut s'agir de relais, d'appareils de mesure, de transducteurs, etc.

3. Documentation confirmant que tout dispositif multifonction affecté à des fonctions de *plan de défense* en plus d'autres fonctions (relais de protection, SCADA, etc.) ne compromet pas la fiabilité du *plan de défense* lorsque ce dispositif n'est pas en service ou est en cours d'entretien.

Dans ce contexte, un dispositif multifonction (relais à microprocesseur, etc.) est un composant qui remplit une fonction de *plan de défense* tout en servant de relais de protection ou de dispositif SCADA. Il est important que les autres utilisations du dispositif multifonction ne compromettent pas le fonctionnement du *plan de défense* lorsque le dispositif est en service ou encore en cours d'entretien. La liste suivante spécifie les indications à fournir lorsqu'un même relais à microprocesseur remplit à la fois une fonction de *plan de défense* et une fonction de protection d'équipement :

- a. Décrire comment le dispositif multifonction est intégré au *plan de défense*.
- b. Montrer la configuration générale et décrire comment le dispositif multifonction est étiqueté dans sa conception et son application, en distinguant la fonction de *plan de défense* et les autres fonctions du dispositif.
- c. Décrire les procédures qui permettent d'isoler la fonction de *plan de défense* des autres fonctions du dispositif.
- d. Décrire les procédures applicables lorsque chaque dispositif multifonction est retiré du service, et indiquer si une coordination avec d'autres plans de protection est requise.
- e. Décrire comment chaque dispositif multifonction est mis à l'essai, à la mise en service et lors des entretiens périodiques, pour chacune de ses fonctions.
- f. Décrire comment les essais fonctionnels et de temps de traitement périodiques du *plan de défense* sont réalisés si le dispositif multifonction est utilisé à la fois pour la protection locale et dans un *plan de défense*.
- g. Décrire comment les mises à niveau du dispositif multifonction (par exemple les mises à jour de micrologiciel) sont effectuées. Comment la fonction de *plan de défense* est-elle prise en considération ?

D'autres dispositifs qui ne sont généralement pas considérés comme des dispositifs multifonctions (relais auxiliaires, interrupteurs de commande, transformateurs de mesure, etc.) peuvent remplir plusieurs fonctions comme la protection d'équipement et la participation à un *plan de défense*. Des indications semblables à celles ci-dessus s'appliquent à de tels cas.

4. Documentation décrivant le performance du *réseau* en cas de défaillance d'un des éléments du *plan de défense* (sauf si celui-ci est à impact limité) au moment où le *plan de défense* est censé fonctionner. La défaillance d'un des éléments d'un *plan de défense* non désigné comme étant à impact limité ne doit pas empêcher le *BES* de respecter les mêmes exigences de performance (définies dans la norme de fiabilité TPL-001-4 [où elles sont appelées « *critères de comportement* »] ou dans toute norme qui la remplace) que celles prescrites pour les événements et les conditions pour lesquels le *plan de défense* est conçu. La documentation doit décrire ou illustrer comment la conception du *plan de défense* atteint cet objectif. [Référence : norme de fiabilité PRC-012 (E1.3)]

L'armement automatique du *plan de défense*, le cas échéant, est un aspect essentiel de la performance du *plan de défense* et du *réseau*, et est donc inclus dans cette exigence.

Exemples non limitatifs de méthodes permettant d'atteindre cet objectif :

- a. Assurer la redondance d'éléments du *plan de défense*, par exemple :
 - i. relais de protection ou relais auxiliaires faisant partie du *plan de défense* ;
 - ii. systèmes de communication nécessaires au bon fonctionnement du *plan de défense* ;
 - iii. capteurs servant à mesurer des grandeurs électriques ou autres pour le *plan de défense* ;
 - iv. alimentations à c.c. de poste associées à des fonctions de *plan de défense* ;
 - v. circuits de commande associés à des fonctions de *plan de défense* par l'intermédiaire de bobines de déclenchement de disjoncteur ou d'autres appareils de coupure ;
 - vi. dispositifs de traitement logique qui acceptent des entrées concernant le *réseau* à partir d'éléments de *plan de défense* ou d'autres sources, prennent des décisions à partir de ces entrées ou produisent des signaux de commande d'actions correctives.
 - b. Armer une plus grande quantité de charge ou de production que nécessaire, afin que si la défaillance d'un des éléments du *plan de défense* empêche de couper une partie de la charge ou de la production prévue, la performance du réseau reste satisfaisante ; toutefois, la coupure de la quantité totale prévue ne doit pas entraîner d'autres effets nuisibles pour la fiabilité.
 - c. Utiliser d'autres moyens automatiques pour pallier les défaillances individuelles d'éléments du *plan de défense*.
 - d. Recourir à des interventions manuelles en utilisant des réglages du *réseau* planifiés, comme des changements à la configuration du *transport* ou à la répartition de la production, si de tels réglages sont exécutables en deçà du délai applicable aux *caractéristiques assignées d'installation*.
5. Documentation décrivant le processus d'essai fonctionnel.

IV. Retrait d'un *plan de défense*

Pour tout *plan de défense* existant à retirer du service, la liste de contrôle suivante spécifie les informations importantes que l'entité propriétaire du *plan de défense* doit documenter et fournir au RC pour examen, conformément à l'exigence E1.

1. Information nécessaire pour permettre au RC de comprendre l'emplacement physique et électrique du *plan de défense* et des installations connexes.
2. Résumé des études techniques pertinentes et des justifications techniques qui motivent le retrait du *plan de défense*.
3. Date de retrait du *plan de défense*.

La documentation nécessaire pour évaluer le retrait d'un *plan de défense* n'est pas aussi exhaustive que pour l'ajout d'un *plan de défense* ou pour la modification du fonctionnement d'un *plan de défense* existant ; néanmoins, il est essentiel qu'après le retrait du *plan de défense*, la performance du réseau continue de respecter les exigences appropriés (habituellement celles des normes TPL) pour les *contingences* ou les conditions du *réseau* qui étaient visées par le *plan de défense* en question.

Justification technique du contenu de l'annexe 2

Liste de contrôle d'examen de *plan de défense* par le *coordonnateur de la fiabilité*

L'annexe 2 est une liste de contrôle qui favorise une démarche d'examen uniforme, à l'échelle du continent, pour les *plans de défense* nouveaux ou dont le fonctionnement a été modifié ; cet examen est exigé avant la mise en service du *plan de défense*. Cette liste de contrôle aidera le RC à déterminer les critères de fiabilité pertinents aux divers aspects de la conception et de la mise en œuvre du *plan de défense*.

Justification technique du contenu de l'annexe 3

Information de la base de données

L'annexe 3 spécifie l'information minimale que le RC doit verser dans sa base de données pour chaque *plan de défense* de sa zone.

1. Nom du *plan de défense*.
 - Nom utilisé pour désigner le *plan de défense*.
2. Chaque entité propriétaire de *plan de défense* et ses coordonnées.
 - Un numéro de téléphone ou une adresse courriel fiable doit permettre de joindre chaque entité propriétaire du *plan de défense* afin d'obtenir des compléments d'information.
3. Date réelle ou prévue de mise en service, date d'approbation la plus récente par le *coordonnateur de la fiabilité* (exigence E3), date d'évaluation la plus récente (exigence E4) et date de retrait, le cas échéant.
 - Indiquer chaque date applicable.
4. Problème de performance du *réseau* ou autre raison qui motive le *plan de défense* (surcharge thermique, instabilité angulaire, amortissement incorrect d'oscillations, instabilité de la tension, surtension, sous-tension, rétablissement lent de la tension, etc.).
 - Une brève description de la raison d'être du *plan de défense* est suffisante, pourvu qu'elle permette à une entité ayant un besoin de fiabilité de comprendre les principaux problèmes de réseau visés par le *plan de défense*.
5. Description des *contingences* ou des conditions du *réseau* pour lesquelles le *plan de défense* a été conçu (conditions de déclenchement).
 - Résumé de haut niveau des conditions ou des *contingences*. Il n'est pas nécessaire d'énumérer toutes les combinaisons de conditions.
6. Actions commandées par le *plan de défense*.
 - Brève description des actions commandées. Si le *plan de défense* commande un délestage de charge ou un rejet de production, préciser le nombre maximal de mégawatts.
7. Désignation du *plan de défense* comme étant à impact limité¹⁰.
 - Spécifier si le *plan de défense* est désigné ou non comme étant à impact limité.

10. Un *plan de défense* désigné comme étant à impact limité ne peut pas, en cas de fonctionnement intempestif ou de non-fonctionnement, donner lieu ou contribuer à des *déclenchements en cascade*, à une séparation fortuite, à une instabilité angulaire, à l'instabilité de la tension, à l'effondrement de la tension ou à des oscillations incorrectement amorties dans le BES.

Compléments

8. Tout complément d'explication qui contribue à une compréhension de haut niveau du *plan de défense*.
 - Si on le juge nécessaire, ajouter des renseignements supplémentaires dans cette section. Ces renseignements ne sont pas obligatoires.

Justification des exigences

Justification de l'exigence E1 : Chaque *plan de défense* est unique et ses actions peuvent avoir des effets importants sur la fiabilité et l'intégrité du *système de production-transport d'électricité (BES)*. C'est pourquoi, avant de mettre en service un nouveau *plan de défense* ou un *plan de défense* existant dont le fonctionnement a été modifié, ou encore de retirer du service un *plan de défense*, il est indispensable de procéder à un examen approprié.

L'expression « dont le fonctionnement a été modifié » s'applique aux cas suivants :

- changements dans les conditions ou les *contingences* du *réseau* surveillées par le *plan de défense* ;
- changements dans les actions que le *plan de défense* est conçu pour exécuter ;
- changements dans les composants physiques du *plan de défense*, au-delà du remplacement à l'identique, sans changement dans le fonctionnement initial de composants existants ;
- changements à la logique du *plan de défense*, au-delà de la correction d'erreurs existantes ;
- changements dans les niveaux de redondance (ajout ou retrait).

Afin de faciliter un examen qui renforce la fiabilité, l'entité propriétaire de *plan de défense* doit fournir au *coordonnateur de la fiabilité (RC)* chargé de l'examen suffisamment de détails sur la conception, la fonction et le fonctionnement du *plan de défense*. Ces informations et la documentation à l'appui sont précisées à l'annexe 1 de la norme ; l'exigence E1 oblige la ou les entités propriétaires de *plan de défense* à les fournir au *RC* chargé de l'examen. Le *RC* qui coordonne la zone dans laquelle est situé le *plan de défense* est chargé de l'examen. Si un *plan de défense* a plusieurs entités propriétaires, il serait souhaitable que celles-ci collaborent afin de soumettre ensemble au *RC* chargé de l'examen du *plan de défense* l'information spécifiée à l'annexe 1. Si le *plan de défense* recoupe plusieurs *zones de fiabilité*, chaque *RC* concerné est chargé soit d'effectuer son propre examen, soit de participer à un examen coordonné.

Justification de l'exigence E2 : Le *RC* est l'entité fonctionnelle la mieux placée pour procéder à l'examen du *plan de défense* : parmi toutes les entités fonctionnelles, c'est le *RC* qui a la vue d'ensemble la plus étendue en matière de fiabilité ; en outre, il est au courant des enjeux de fiabilité qui touchent les zones de fiabilité voisines. Sa vue d'ensemble sur la *zone étendue* facilite l'évaluation des interactions entre différents *plans de défense* ainsi que des interactions entre les *plans de défense* et d'autres systèmes de protection et de contrôle. En outre, l'examen par le *RC* amenuise la possibilité d'un conflit d'intérêts découlant de relations d'affaires entre l'entité propriétaire de *plan de défense*, le *coordonnateur de la planification*, le *planificateur de réseau de transport* ou d'autres entités concernées par la planification ou la mise en service d'un *plan de défense*. Le *RC* n'est pas censé détenir davantage d'informations ou de compétences que ne l'indique son inscription fonctionnelle selon les critères de la NERC. Le *RC* peut demander à d'autres entités, comme le *coordonnateur de la planification (PC)* ou les groupes techniques régionaux, de l'aider pour l'examen du *plan de défense* ; cependant, le *RC* demeure responsable de la conformité à l'exigence.

L'annexe 2 de la présente norme propose une liste de contrôle pour aider le *RC* à déterminer les paramètres de conception et de mise en œuvre d'un *plan de défense*, et pour favoriser une démarche d'examen uniforme des *plans de défense*. Le délai de quatre mois civils concorde avec la pratique courante dans l'industrie ; cependant, l'exigence prévoit une certaine latitude puisqu'elle permet aux *RC* et aux entités propriétaires de *plan de défense* de négocier un calendrier différent pour l'examen.

Remarque : Un RC peut devoir inclure cette tâche dans son ou ses plans de fiabilité pour la ou les régions de la NERC où il est situé.

Justification de l'exigence E3 : L'examen par le RC est destiné à déceler les problèmes de fiabilité à corriger avant la mise en service du *plan de défense*. Les problèmes de fiabilité possibles concernent notamment la sûreté de fonctionnement, la sécurité ou la coordination.

Il n'est pas nécessaire de spécifier le délai de réponse de l'entité propriétaire du *plan de défense* au RC chargé de l'examen lorsque celui-ci signale un problème de fiabilité, puisque l'entité propriétaire du *plan de défense* a tout intérêt à obtenir rapidement l'approbation de son *plan de défense* et à le mettre en service dans les meilleurs délais.

Il n'est pas non plus nécessaire de spécifier un délai particulier pour la réponse du RC à l'entité propriétaire du *plan de défense* à la suite de l'examen, car le RC est au courant 1) de tout problème de fiabilité qui perdure tant que le *plan de défense* n'aura pas été mis en service, et 2) du calendrier prévu par l'entité propriétaire du *plan de défense* pour mettre celui-ci en service afin de résoudre ces problèmes de fiabilité. Comme le RC est l'arbitre ultime de la fiabilité du BES, la résolution des problèmes de fiabilité est une priorité pour le RC et incite celui-ci à répondre sans délai à l'entité propriétaire du *plan de défense*.

Justification de l'exigence E4 : L'exigence E4 stipule que chaque *plan de défense* doit être évalué au moins une fois toutes les cinq années civiles. Cette évaluation périodique vise à confirmer le maintien de l'efficacité et de la coordination du *plan de défense*, ainsi qu'à vérifier qu'en cas de défectuosité ou de défaillance d'un des éléments du *plan de défense*, les exigences de performance du BES seraient toujours remplies. Une évaluation périodique est exigée parce que des changements dans la topologie ou les conditions d'exploitation du *réseau* peuvent remettre en question l'efficacité du *plan de défense* ou son influence sur le BES.

Les *plans de défense* sont des assemblages uniques et personnalisés d'équipements de protection et de contrôle dont la complexité et l'impact sur la fiabilité du BES sont variables. Compte tenu de ses particularités, un *plan de défense* peut être désigné par le ou les RC chargés de l'examen comme étant à impact limité. Un *plan de défense* à impact limité ne peut pas, en cas de fonctionnement intempestif ou de non-fonctionnement, donner lieu ou contribuer à des *déclenchements en cascade*, à une séparation fortuite, à une instabilité angulaire, à l'instabilité de la tension, à l'effondrement de la tension ou à des oscillations incorrectement amorties dans le BES. L'expression « dans le BES » dans la phrase qui précède s'applique à tous les éléments de l'énumération. Les *plans de défense* à impact limité sont dispensés des essais de défectuosité et de défaillance d'un de leurs éléments (alinéas 4.1.4 et 4.1.5, respectivement) ; de tels essais obligeraient à complexifier la conception du *plan de défense*, sans guère de bienfait pour la fiabilité du BES. Pour plus de détails sur la désignation « à impact limité », se reporter à la section Compléments.

La norme reconnaît la catégorie LAPS (automatisme de protection de zone locale) du WECC (Western Electricity Coordinating Council) et la catégorie Type III du NPCC (Northeast Power Coordinating Council) comme étant initialement appropriées pour la désignation « à impact limité ». Si un *plan de défense* est mis en service avant la date d'entrée en vigueur de la norme PRC-012-2 et qu'il a été classé « LAPS » par le WECC ou « Type III » par le NPCC après avoir été soumis au processus d'examen régional pertinent, il est considéré comme un *plan de défense* à impact limité aux fins de la norme PRC-012-2 à la date d'entrée en vigueur de celle-ci, et il est soumis à toutes ses exigences pertinentes.

Pour les *plans de défense* existants, le délai de cinq années civiles de l'exigence E4 s'applique initialement à compter de la date d'entrée en vigueur de la norme PRC-012-2. Dans le cas d'un *plan de défense* nouveau ou dont le fonctionnement est modifié, ce délai s'applique initialement à compter de

la date d'approbation du *plan de défense* par le RC chargé de l'examen. Le délai de cinq années civiles a été choisi comme intervalle maximal entre les évaluations à partir des valeurs adoptées pour des exigences semblables dans les normes de fiabilité PRC-006, PRC-010 et PRC-014. On peut procéder plus tôt à l'évaluation du *plan de défense* si l'on considère que des changements importants à la topologie de *réseau* ou à ses conditions d'exploitation peuvent remettre en question l'efficacité ou la coordination du *plan de défense*. Des changements dans le *réseau* peuvent aussi amener à reconsidérer les effets d'un *plan de défense* à impact limité sur la fiabilité du *BES* ; l'alinéa 4.1.3 de l'exigence E4 demande explicitement de réévaluer périodiquement si la désignation « à impact limité » d'un *plan de défense* est toujours justifiée (la façon de procéder à cette évaluation est laissée à la discrétion du PC). L'évaluation périodique d'un *plan de défense* produit habituellement un des trois résultats suivants : 1) la confirmation que le *plan de défense* existant est adéquat ; 2) la description des correctifs à apporter au *plan de défense* ; ou 3) la justification du retrait du *plan de défense*.

Les conditions visées par l'évaluation (alinéas 4.1.1 à 4.1.5 de l'exigence E4) nécessitent des analyses de planification qui peuvent amener à modéliser le réseau de transport interconnecté afin d'évaluer la performance du *BES*. Le PC est l'entité fonctionnelle la mieux placée pour procéder à l'évaluation puisqu'il a une bonne vue d'ensemble de la planification dans une zone étendue. Dans l'intérêt de la fiabilité, le PC est tenu de transmettre les résultats de son évaluation à chaque *planificateur de réseau de transport* (TP) et PC concerné, ainsi qu'à chaque RC chargé de l'examen et entité propriétaire de *plan de défense*. Si le *plan de défense* recoupe les territoires de plusieurs PC, chaque PC concerné est tenu soit d'effectuer sa propre évaluation, soit de participer à une évaluation coordonnée.

Dans la version précédente (PRC-012-1) de la norme, l'alinéa 1.4 de l'exigence E1 stipule que « ...le fonctionnement intempestif d'un *plan de défense* doit respecter les mêmes exigences de performance (TPL-001-0, TPL-002-0 et TPL-003-0) que pour la contingence visée par le *plan de défense*, et ne pas dépasser les limites prescrites à la norme TPL-003-0. » L'exigence E4 précise que le fonctionnement intempestif visé découle uniquement de la défectuosité d'un seul des éléments du *plan de défense*, ce qui amène à intégrer à la conception du *plan de défense* des fonctions de sécurité qui empêcheront tout fonctionnement intempestif causé par la défectuosité d'un seul élément. Pour le reste, conformément à l'alinéa 1.4 de l'exigence E1 de la norme PRC-012-1, le *plan de défense* doit être conçu de façon qu'un fonctionnement intempestif partiel ou complet causé par la défectuosité d'un de ses éléments respecte les exigences de performance du *réseau* pour la *contingence* visée par le *plan de défense*.

Si le *plan de défense* a été installé en prévision d'un événement extrême spécifié dans la norme TPL-001-4 ou de certaines autres *contingences* ou conditions du *réseau* non définies dans la norme TPL-001-4 (donc sans exigences de performance), son fonctionnement intempestif doit quand même respecter les exigences minimales de performance du *réseau*. Toutefois, au lieu de renvoyer à la norme TPL-001-4, l'exigence E4 énonce directement les exigences de performance du *réseau* qu'un fonctionnement intempestif éventuel doit respecter. Les exigences de performance énoncées aux alinéas 4.1.4.1 à 4.1.4.5 sont celles qui sont communes à tous les événements de planification (P0 à P7) traités dans la norme TPL-001-4.

Justification de l'exigence E5 : Le fonctionnement correct d'un *plan de défense* est important pour le maintien de la fiabilité et de l'intégrité du *BES*. Tout fonctionnement incorrect indique que l'efficacité ou la coordination du *plan de défense* a été compromise. Par conséquent, chaque fonctionnement d'un *plan de défense* et chaque non-fonctionnement dans une situation où il aurait dû fonctionner doivent être analysés afin de déterminer si le fonctionnement du *plan de défense* concorde bien avec ses caractéristiques de conception.

L'analyse de la performance opérationnelle d'un *plan de défense* vise : 1) à vérifier si le fonctionnement du *plan de défense* concorde bien avec sa conception à la mise en service ; ou 2) à découvrir les lacunes

du *plan de défense* qui se sont manifestées dans son fonctionnement incorrect ou encore son non-fonctionnement dans une situation prévue.

Le délai de 120 jours civils pour l'analyse de performance opérationnelle d'un *plan de défense* correspond au délai prescrit à l'exigence E1 de la norme PRC-004-4 pour l'enquête sur le *fonctionnement incorrect* d'un *système de protection*. Dans l'intérêt de la fiabilité, chaque entité propriétaire du *plan de défense* doit transmettre les résultats d'analyse de performance opérationnelle à son ou ses RC chargés de l'examen si l'analyse révèle une lacune.

Les entités propriétaires du *plan de défense* peuvent avoir besoin de collaborer avec le TP concerné pour réaliser une analyse de performance opérationnelle approfondie. En effet, l'analyse de performance opérationnelle nécessite de vérifier que le *plan de défense* a été déclenché adéquatement (alinéa 5.1.1), qu'il a fonctionné comme prévu (alinéa 5.1.2) et que la réaction du BES (alinéas 5.1.3 et 5.1.4) correspond bien à la conception du *plan de défense*. Si un *plan de défense* a plusieurs entités propriétaires, il serait souhaitable que celles-ci collaborent pour réaliser et soumettre une seule analyse de performance opérationnelle coordonnée.

Justification de l'exigence E6 : Les lacunes découvertes lors de l'évaluation périodique du *plan de défense* réalisée par le PC selon l'exigence E4, lors de l'analyse de performance opérationnelle effectuée par l'entité propriétaire du *plan de défense* selon l'exigence E5 ou lors de l'essai fonctionnel effectué par l'entité propriétaire du *plan de défense* selon l'exigence l'exigence E8 présentent un risque potentiel pour la fiabilité du BES. Afin d'atténuer ce risque, l'exigence E6 stipule que chaque entité propriétaire de *plan de défense* doit élaborer un *plan d'actions correctives (CAP)* visant à corriger toute lacune. Le CAP indique les mesures correctives et précise leur calendrier de mise en œuvre. L'entité propriétaire du *plan de défense* peut demander à d'autres entités, comme son TP ou son PC, de l'aider dans l'élaboration du CAP ; cependant, la conformité à cette exigence incombe toujours à l'entité propriétaire du *plan de défense*.

Si le CAP indique que le fonctionnement du *plan de défense* doit être modifié, l'entité propriétaire du *plan de défense* doit fournir au RC chargé de l'examen l'information spécifiée à l'annexe 1 avant de pouvoir mettre en service le *plan de défense* modifié, conformément à l'exigence E1.

Selon la complexité des lacunes signalées, l'élaboration du CAP peut nécessiter des analyses, des études d'ingénierie ou des services-conseils. Un délai maximal de six mois civils est prévu pour donner à l'entité propriétaire du *plan de défense* le temps d'élaborer le CAP avec les collaborations nécessaires. Idéalement, si un *plan de défense* a plusieurs entités propriétaires, celles-ci devraient collaborer afin d'élaborer et de présenter un CAP commun.

Justification de l'exigence E7 : L'exigence E7 demande à chaque entité propriétaire de *plan de défense* de mettre en œuvre son CAP, élaboré selon l'exigence E6 afin de corriger les lacunes décelées selon les exigences E4, E5 ou E8. Par définition, un CAP est « une liste des actions, avec leurs échéances, à mettre en œuvre pour remédier à un problème particulier ». La mise en œuvre d'un CAP bien conçu permet de corriger la ou les lacunes du *plan de défense* dans les meilleurs délais. Chaque RC chargé de l'examen doit être avisé en cas de changement dans les mesures correctives du CAP ou dans leur calendrier, ainsi qu'à l'achèvement du CAP.

Justification de l'exigence E8 : Étant donné la grande variété des *plans de défense* quant à leur conception et à leur mise en œuvre, ainsi que leur potentiel d'impact sur la fiabilité du BES, il est important de les soumettre à des essais fonctionnels périodiques. Un essai fonctionnel permet de confirmer que le *plan de défense* fonctionne conformément à ses critères de conception ; il permet aussi de vérifier le bon fonctionnement des éléments du *plan de défense* qui ne font pas partie d'un *système de protection* (composants de commande) et qui ne sont pas visés par la norme PRC-005. Les

composants de *système de protection* qui font partie d'un *plan de défense* sont soumis aux exigences d'entretien de la norme PRC-005.

L'intervalle de six ou douze années civiles (qui commence à la date d'entrée en vigueur de la norme PRC-012-2 selon son plan de mise en œuvre) représente un compromis entre, d'une part, les ressources requises pour effectuer les essais et, d'autre part, les impacts potentiels sur la fiabilité du *BES* qui découleraient de défaillances latentes non décelées, susceptibles de causer un fonctionnement incorrect du *plan de défense*. Des intervalles plus longs augmenteraient indûment les risques liés aux défaillances latentes. L'entité propriétaire du *plan de défense* est l'entité la mieux placée pour établir les procédures et le calendrier d'essai étant donné sa connaissance étendue de la conception du *plan de défense*, de son installation et de son fonctionnement. Les essais fonctionnels peuvent être effectués de bout en bout (essai intégral) ou par segment ; dans ce dernier cas, chacun des segments du *plan de défense* doit être mis à l'essai. Le fait de pouvoir mettre à l'essai individuellement des segments qui se chevauchent permet de simplifier le calendrier d'entretien et d'interruptions.

L'intervalle maximal admissible entre les essais fonctionnels est de six années civiles pour les *plans de défense* qui n'ont pas la désignation « à impact limité », et de douze années civiles pour ceux qui ont cette désignation. L'intervalle commence à la date de l'essai réussi le plus récent pour un segment ou pour l'intégralité du *plan de défense*. La réussite d'un essai de segment remet à zéro l'intervalle d'essai pour ce segment seulement. Un bon fonctionnement d'un *plan de défense* peut être compté comme un essai fonctionnel pour les segments du *plan de défense* qui ont effectivement fonctionné (la conformité à l'alinéa 5.1 de l'exigence E5 doit être documentée). Si un événement entraîne un fonctionnement correct mais partiel du *plan de défense*, les segments qui n'ont pas fonctionné doivent être soumis à des essais fonctionnels séparés avant la fin de l'intervalle d'essai maximal qui a commencé à la date du précédent essai réussi pour ces segments.

Justification de l'exigence E9 : La base de données sur les *plans de défense* regroupe l'information sur tous les *plans de défense* en service dans une *zone de fiabilité*. Cette base de données permet au *RC* de fournir à d'autres entités de l'information de haut niveau sur des *plans de défense* existants qui pourraient éventuellement influencer sur les activités d'exploitation ou de planification de ces entités. L'annexe 3 spécifie l'information minimale qui doit y être versée pour chaque *plan de défense*, notamment un résumé des conditions de déclenchement du *plan de défense*, des actions correctives et des problèmes de *réseau* auxquels on cherche à remédier. Cette information permet à toute entité d'évaluer le besoin de fiabilité qui peut l'amener à demander une information plus détaillée aux entités propriétaires de *plan de défense* dont les coordonnées figurent dans la base de données. Le *RC* est l'entité la mieux placée pour tenir à jour cette base de données, puisqu'il reçoit l'information voulue lorsqu'un *plan de défense* nouveau ou modifié est soumis pour examen. Le délai de douze mois civils concorde avec la pratique courante dans l'industrie ; il donne au *RC* suffisamment de temps pour recueillir l'information appropriée auprès des entités propriétaires de *plan de défense* et mettre à jour la base de données.

Annexe QC-PRC-012-2
Dispositions particulières de la norme PRC-012-2 applicables au Québec

Cette annexe établit les dispositions particulières d'application de la norme au Québec. Les dispositions de la norme et de son annexe doivent obligatoirement être lues conjointement pour fins de compréhension et d'interprétation. En cas de divergence entre la norme et l'annexe, l'annexe a préséance.

A. Introduction

1. **Titre :** Plans de défense
2. **Numéro :** PRC-012-2
3. **Objet :** Aucune disposition particulière
4. **Applicabilité :**
 - 4.1. **Entités fonctionnelles**
Aucune disposition particulière
 - 4.2. **Installations**
Aucune disposition particulière
5. **Date d'entrée en vigueur :**
 - 5.1. Adoption de la norme par la Régie de l'énergie : XX mois 2018
 - 5.2. Adoption de l'annexe par la Régie de l'énergie : XX mois 2018
 - 5.3. Date d'entrée en vigueur de la norme et de l'annexe au Québec : 1^{er} janvier 2019

Exigence	Date de mise en application au Québec
E1, E2, E3, E5, E6 et E7	1 ^{er} janvier 2022
E4	<ul style="list-style-type: none">1^{er} janvier 2024 : date limite pour la réalisation et l'envoi d'une première évaluation.
E8	<ul style="list-style-type: none">1^{er} janvier 2025 : date limite pour la réalisation d'un premier essai des <i>plans de défense</i> qui ne sont pas désignés comme étant à impact limité.1^{er} janvier 2031 : date limite pour la réalisation d'un premier essai des <i>plans de défense</i> qui sont désignés comme étant à impact limité.
E9	<ul style="list-style-type: none">1^{er} janvier 2022 : date limite pour l'établissement d'une base de données pour les plans de défense.

B. Exigences et mesures

Remplacer toutes les références au terme « *BES* » par « *RTP* ».

À l'alinéa 4.1.5., l'expression « exigences de performance » est identique à « critères de comportement » définie dans la norme de fiabilité TPL-001-4.

C. Conformité

1. **Processus de surveillance de la conformité**
 - 1.1. **Responsable de la surveillance de l'application des normes**
Au Québec, la Régie de l'énergie est responsable de la surveillance de la conformité avec la norme de fiabilité et l'annexe qu'elle adoptées.
 - 1.2. **Conservation des pièces justificatives**

Aucune disposition particulière

1.3. Programme de surveillance et de mise en application des normes

Aucune disposition particulière

Niveaux de gravité des non-conformités (VSL)

Aucune disposition particulière

D. Différences régionales

Aucune disposition particulière

E. Documents connexes

Aucune disposition particulière

Annexe 1

Remplacer toutes les références au terme « *BES* » par « *RTP* ».

Annexe 2

Remplacer toutes les références au terme « *BES* » par « *RTP* ».

Annexe 3

Aucune disposition particulière

Justification technique

Remplacer toutes les références au terme « *BES* » par « *RTP* ».

Page 23, remplacer le troisième paragraphe par celui-ci (modifications soulignées) :

Pour pouvoir demander au *RC* chargé de l'examen de désigner un *plan de défense* existant (mis en œuvre avant la date d'entrée en vigueur de la norme PRC-012-2) comme étant à impact limité, l'entité propriétaire du *plan de défense* doit préparer et soumettre l'information prescrite à l'annexe 1, notamment la justification technique (les évaluations) que le *réseau* répond aux exigences de performance (alinéa 4.1.3 de l'exigence E4) en cas de défectuosité ou de défaillance, respectivement, d'un élément du *plan de défense*.

Page 26, remplacer le cinquième paragraphe par celui-ci (modifications soulignées) :

La sécurité est une autre composante de la notion de fiabilité ; elle indique la confiance que l'appareil n'interviendra pas de façon intempestive. Le fonctionnement intempestif d'un *plan de défense* déclenche une action programmée sans que les conditions d'armement soient remplies, ou en dehors de la ou des *contingences* ou conditions de *réseau* spécifiées. Typiquement, un *plan de défense* commande un délestage de charge, un rejet de production ou une reconfiguration du *réseau* ; de telles actions, si elles surviennent de façon injustifiée, sont néfastes et peuvent compromettre la sécurité du *réseau*. Le pire scénario de fonctionnement intempestif est celui où toutes les actions programmées du *plan de défense* sont déclenchées. Si la performance du *réseau* est encore conforme à l'alinéa 4.1.4 de l'exigence E4 de la norme PRC-012-2, aucune mesure d'atténuation supplémentaire n'est requise. Des moyens de renforcement de la sécurité intrinsèque d'un *plan de défense* comme des logiques de décision sont des mesures d'atténuation acceptables contre les fonctionnements intempestifs.

Historique des révisions

Révision	Date	Intervention	Suivi des modifications
0	XX mois 201X	Nouvelle annexe	–