



Document d'orientation sur la conception des nouvelles centrales nucléaires

GD-337

Septembre 2012



Document d'orientation sur la conception des nouvelles centrales nucléaires

Document d'orientation GD-337

© Ministre de Travaux publics et Services gouvernementaux Canada 2012

Numéro de catalogue XXXXX

ISBN XXXXX

Publié par la Commission canadienne de sûreté nucléaire

La reproduction d'extraits du présent document à des fins personnelles est autorisée à condition d'en citer la source en entier. Toutefois, sa reproduction en tout ou en partie à des fins commerciales ou de redistribution nécessite l'obtention préalable d'une autorisation écrite de la Commission canadienne de sûreté nucléaire.

This document is also published in English under the title: Guidance for the Design of New Nuclear Power Plants

Disponibilité du document

Les personnes intéressées peuvent consulter le document sur le site Web de la Commission canadienne de sûreté nucléaire à la page suretenucleaire.gc.ca

Pour obtenir un exemplaire du document en français ou en anglais, veuillez communiquer avec :

Commission canadienne de sûreté nucléaire

280, rue Slater

Case postale 1046, Succursale B

Ottawa (Ontario) K1P 5S9

CANADA

Tél. : 613-995-5894 ou 1-800-668-5284 (Canada seulement)

Télécopieur : 613-995-5086

Courriel : info@cnsccsn.gc.ca

Site Web : suretenucleaire.gc.ca

Historique de publication :

[mois, année]

Version 1.0

Préface

Le présent document énonce les attentes et fournit des orientations sur la façon de répondre aux exigences stipulées dans la version 2 du document d'application de la réglementation RD-337, *Conception des nouvelles centrales nucléaires*.

Le présent document et la version 2 du document RD-337 constituent l'adoption par la CCSN des principes mis de l'avant par l'Agence internationale de l'énergie atomique (AIEA) dans le document SSR 2/1 intitulé *Sûreté des centrales nucléaires : Conception* (la version révisée du document NS-R-1). Il est possible d'obtenir de l'orientation complémentaire en consultant les codes et normes canadiens pertinents, ainsi que les normes internationales appropriées, telles que les publications de l'AIEA.

Le présent document est structuré de manière à ce que les numéros de section coïncident avec ceux de la version 2 du document RD-337. Il traite d'un grand nombre de sujets liés à la conception des nouvelles centrales nucléaires, tels que les objectifs et concepts de sûreté, la gestion de la sûreté durant la conception, les attentes générales en matière de sûreté, les attentes relatives aux systèmes et l'analyse de la sûreté.

Aux fins du présent document, « doit » est employé pour exprimer une exigence, c'est-à-dire une disposition qu'un titulaire ou demandeur de permis est tenu de respecter pour se conformer aux exigences du présent document d'orientation. « Devrait » dénote une orientation ou une mesure conseillée. « Pourrait » exprime une option ou un élément permmissible dans les limites du présent document. « Peut » exprime une possibilité ou une capacité.

Aucun élément dans ce document ne doit être interprété par le titulaire de permis comme une autorisation de déroger aux exigences pertinentes. Il appartient au titulaire de permis d'identifier tous les règlements et conditions de permis applicables et de s'y conformer.

Table des matières

1.0	Objet.....	6
2.0	Portée	6
3.0	Législation pertinente	6
4.0	Objectifs et concepts de sûreté.....	7
4.1	Objectif général en matière de sûreté nucléaire	7
4.1.1	Objectif en matière de radioprotection	7
4.1.2	Objectifs en matière de sûreté technique	8
4.1.3	Objectif en matière de protection environnementale	8
4.2	Application des objectifs de sûreté technique.....	8
4.2.1	Critères d'acceptation des doses	8
4.2.2	Objectifs en matière de sûreté.....	8
4.2.3	Analyses de la sûreté.....	9
4.2.4	Atténuation et gestion des accidents	9
4.3	Concepts de sûreté	10
4.3.1	Défense en profondeur.....	10
4.3.2	Examen des barrières physiques	10
4.3.3	Limites et conditions d'exploitation	10
4.3.4	Interface entre la sûreté, la sécurité et les garanties	10
5.0	Gestion de la sûreté dans la conception	10
5.1	Autorité en matière de conception	10
5.2	Gestion de la conception.....	11
5.3	Mesures de contrôle de la conception.....	11
5.4	Méthodes d'ingénierie éprouvées	12
5.5	Expérience opérationnelle et recherche en matière de sûreté	12
5.6	Évaluation de la sûreté.....	13
5.7	Documentation sur la conception.....	13
6.0	Orientations relatives aux exigences en matière de sûreté.....	13
6.1	Application du concept de défense en profondeur.....	13
6.1.1	Examen des barrières physiques	14
6.2	Fonctions de sûreté	15
6.3	Prévention des accidents et caractéristiques de sûreté de la centrale.....	15

6.4	Radioprotection et critères d'acceptation.....	15
6.5	Zone d'exclusion.....	15
6.6	Plan de l'installation	17
6.6.1	Exigences pour les centrales à tranches multiples	17
7.0	Orientation relative aux exigences générales de la conception.....	18
7.1	Classification des SSC.....	18
7.2	Enveloppe de conception de la centrale.....	19
7.3	États de la centrale	20
7.3.1	Exploitation normale.....	20
7.3.2	Incident de fonctionnement prévu	21
7.3.3	Accident de dimensionnement.....	22
7.3.4	Conditions additionnelles de dimensionnement	22
7.4	Événements initiateurs hypothétiques.....	24
7.4.1	Dangers internes	24
7.4.2	Dangers externes.....	25
7.4.3	Combinaisons d'événements	27
7.5	Règles et limites de conception.....	27
7.6	Fiabilité	28
7.6.1	Défaillances d'origine commune	29
7.6.2	Critère de défaillance simple	30
7.6.3	Conception à sûreté intégrée.....	31
7.6.4	Indisponibilité d'équipement	31
7.6.5	Systèmes partagés.....	32
7.7	SSC sous pression.....	32
7.8	Qualification environnementale de l'équipement	34
7.8.1	Identification de l'équipement devant être qualifié pour des environnements hostiles	34
7.8.2	Identification des conditions opérationnelles de l'équipement.....	34
7.8.3	Méthodes de qualification.....	34
7.8.4	Évaluation de l'équipement et de l'instrumentation en cas de CAD.....	35
7.8.5	Barrières de protection.....	35
7.9	Instrumentation et contrôle	36
7.9.1	Généralités	36
7.9.2	Utilisation de systèmes ou d'équipement informatisés.....	38

7.9.3	Instrumentation servant à la surveillance des accidents.....	39
7.10	Systèmes de support en matière de sûreté.....	40
7.11	État d'arrêt garanti	40
7.12	Sûreté contre les incendies.....	41
7.12.1	Dispositions générales	41
7.12.2	Sûreté des personnes.....	42
7.12.3	Protection environnementale et sûreté nucléaire	42
7.13	Qualification sismique	43
7.13.1	Conception et classification sismiques	43
7.14	Essais, entretien, réparations, inspection et surveillance en cours d'exploitation.....	46
7.15	Structures de génie civil.....	48
7.15.1	Conception.....	48
7.15.2	Surveillance	50
7.15.3	Levage de charges lourdes.....	51
7.16	Construction et mise en service	51
7.17	Vieillesse et usure	52
7.18	Contrôle des corps étrangers.....	52
7.19	Transport et emballage de combustible et de déchets radioactifs	52
7.20	Voies d'évacuation d'urgence et moyens de communications	53
7.21	Facteurs humains	53
7.22	Robustesse contre des actes malveillants.....	56
7.22.1	Principes de conception	57
7.22.2	Méthodes de conception	57
7.22.3	Critères d'acceptation	58
7.22.4	Cybersécurité.....	62
7.23	Garanties	65
7.24	Déclassement	66
8.0	Exigences relatives aux systèmes	66
8.1	Cœur du réacteur.....	66
8.1.1	Éléments et assemblages de combustible	73
8.1.2	Système de contrôle du cœur du réacteur	75
8.2	Système de refroidissement du réacteur	77
8.2.1	Inspection de l'enveloppe sous pression en cours d'exploitation	78
8.2.2	Inventaire	78

8.2.3	Nettoyage.....	79
8.2.4	Évacuation de la chaleur résiduelle du cœur du réacteur.....	79
8.3	Système d'alimentation en vapeur d'eau	79
8.3.1	Conduites de vapeur.....	79
8.3.2	Tuyauterie et cuves des systèmes de vapeur et d'eau d'alimentation.....	79
8.3.3	Turbo-alternateurs.....	79
8.4	Systèmes d'arrêt d'urgence.....	80
8.4.1	Paramètres de déclenchement des systèmes d'arrêt d'urgence.....	81
8.4.2	Fiabilité.....	83
8.4.3	Surveillance et interventions de l'opérateur	83
8.5	Système de refroidissement d'urgence du cœur du réacteur.....	83
8.6	Confinement.....	85
8.6.1	Orientation relative aux exigences générales.....	85
8.6.2	Résistance de la structure de confinement	85
8.6.3	Capacité relative aux essais de pressurisation	86
8.6.4	Fuites.....	86
8.6.5	Pénétrations de l'enceinte de confinement	86
8.6.6	Isolation du confinement	86
8.6.7	Sas du confinement.....	87
8.6.8	Structures internes du confinement.....	87
8.6.9	Pression de l'enceinte de confinement et gestion de l'énergie	87
8.6.10	Contrôle et nettoyage de l'atmosphère de l'enceinte de confinement	88
8.6.11	Revêtements et matériaux.....	88
8.6.12	Conditions additionnelles de dimensionnement	88
8.7	Transfert de chaleur vers une source froide ultime.....	89
8.8	Système d'évacuation d'urgence de la chaleur	89
8.9	Systèmes d'alimentation électrique	90
8.9.1	Systèmes d'alimentation électrique de relève et d'urgence	92
8.9.2	Source d'alimentation de remplacement en CA	93
8.10	Salles de commande.....	94
8.10.1	Salle de commande principale.....	94
8.10.2	Salle de commande auxiliaire.....	95
8.10.3	Centre de soutien d'urgence	96
8.10.4	Directives relatives à l'équipement en cas d'accidents	96
8.11	Traitement et contrôle des déchets.....	97

8.11.1	Contrôle des rejets liquides dans l'environnement.....	97
8.11.2	Contrôle des matières présentes dans l'air à l'intérieur de la centrale.....	97
8.11.3	Contrôle des rejets gazeux dans l'environnement	97
8.12	Manutention et stockage du combustible.....	98
8.12.1	Manutention et stockage de combustible non irradié	98
8.12.2	Manutention et stockage de combustible irradié	98
8.12.3	Détection de combustible défectueux.....	99
8.13	Radioprotection.....	99
8.13.1	Conception relative à la radioprotection.....	100
8.13.2	Contrôle de l'accès et des déplacements	100
8.13.3	Surveillance	100
8.13.4	Sources	100
8.13.5	Surveillance de l'incidence environnementale	100
9.0	Analyses de la sûreté.....	101
9.1	Généralités	101
9.2	Objectifs de l'analyse.....	101
9.3	Analyse des dangers.....	101
9.4	Analyse déterministe de la sûreté	102
9.5	Analyse probabiliste de la sûreté	102
10.0	Protection environnementale et atténuation	103
10.1	Conception relative à la protection de l'environnement	103
10.2	Rejet de substances nucléaires et dangereuses.....	103
11.0	Autres méthodes.....	103
	Abréviations.....	104
	Glossaire.....	105
	Références de la CCSN.....	113
	Renseignements supplémentaires	115

Document d'orientation sur la conception des nouvelles centrales nucléaires

1.0 Objet

Le présent document énonce les attentes et fournit des orientations sur la façon de répondre aux exigences stipulées dans la version 2 du document d'application de la réglementation RD-337, *Conception des nouvelles centrales nucléaires*.

2.0 Portée

Ce document d'orientation fournit des renseignements sur les méthodes et les approches prises en considération dans la conception des nouvelles centrales nucléaires (CN ou centrales). Il traite d'un grand nombre de sujets liés à la conception des nouvelles centrales nucléaires, tels que les objectifs et concepts de sûreté, la gestion de la sûreté durant la conception, les attentes générales en matière de sûreté, les attentes relatives aux systèmes et l'analyse de la sûreté.

Le présent document et la version 2 du document RD-337 constituent l'adoption par la CCSN des principes mis de l'avant par l'Agence internationale de l'énergie atomique (AIEA) dans le document SSR 2/1 intitulé *Sûreté des centrales nucléaires : Conception* (qui constitue la version révisée du document NS-R-1). Il est possible d'obtenir de l'orientation complémentaire en consultant les codes et normes canadiens pertinents, ainsi que les normes internationales appropriées, telles que les publications de l'AIEA.

3.0 Législation pertinente

Les dispositions de la *Loi sur la sûreté et la réglementation nucléaires* (LSRN) et de ses règlements qui s'appliquent au présent document d'orientation englobent les éléments suivants :

1. Le paragraphe 24(4) de la LSRN stipule que « la Commission ne délivre, ne renouvelle, ne modifie ou ne remplace une licence ou un permis que si elle est d'avis que l'auteur de la demande, à la fois : a) est compétent pour exercer les activités visées par la licence ou le permis; b) prendra, dans le cadre de ces activités, les mesures voulues pour préserver la santé et la sécurité des personnes, pour protéger l'environnement, pour maintenir la sécurité nationale et pour respecter les obligations internationales que le Canada a assumées »
2. Le paragraphe 24(5) de la LSRN autorise la Commission à inclure dans une licence ou un permis toute condition qu'elle estime nécessaire à l'application de la LSRN
3. L'alinéa 3(1)i) du *Règlement général sur la sûreté et la réglementation nucléaires* stipule qu'une demande de permis doit contenir, en plus d'autres renseignements, « une description et les résultats des épreuves, analyses ou calculs effectués pour corroborer les renseignements compris dans la demande »
4. Selon l'alinéa 12(1)f) du *Règlement général sur la sûreté et la réglementation nucléaires*, le titulaire de permis doit prendre « toutes les précautions raisonnables pour contrôler le rejet de substances nucléaires radioactives ou de substances dangereuses que l'activité autorisée peut entraîner là où elle est exercée et dans l'environnement »
5. Les alinéas 3b), 5a), d), e), f), i) et 6a), b), h) et 7f) du *Règlement sur les installations nucléaires de catégorie I* stipulent qu'une demande de permis visant une installation nucléaire de catégorie 1, autre qu'un permis d'abandon, doit contenir, en plus d'autres renseignements : 3b) « des plans indiquant l'emplacement, le périmètre, les aires, les ouvrages et les systèmes de l'installation nucléaire »

- 5a) « une description de la conception proposée pour l'installation nucléaire, y compris la façon dont elle tient compte des caractéristiques physiques et environnementales de l'emplacement »
- 5d) « une description des ouvrages à construire pour l'installation nucléaire, y compris leur conception et leurs caractéristiques de conception »
- 5e) « une description des systèmes et de l'équipement qui seront aménagés à l'installation nucléaire, y compris leur conception et leurs conditions nominales de fonctionnement »
- 5f) « un rapport préliminaire d'analyse de la sûreté démontrant que la conception de l'installation nucléaire est adéquate »
- 5i) « les effets sur l'environnement ainsi que sur la santé et la sécurité des personnes que peuvent avoir la construction, l'exploitation et le déclassement de l'installation nucléaire »
- 6a) « une description des ouvrages de l'installation nucléaire, y compris leur conception et leurs conditions nominales d'exploitation »
- 6b) « une description des systèmes et de l'équipement de l'installation nucléaire, y compris leur conception et leurs conditions nominales de fonctionnement »
- 6h) « les effets sur l'environnement ainsi que sur la santé et la sécurité des personnes que peuvent avoir l'exploitation et le déclassement de l'installation nucléaire, ... »
- 7f) « les effets que les travaux de déclassement peuvent avoir sur l'environnement ainsi que sur la santé et la sécurité des personnes, de même que les mesures qui seront prises pour éviter ou atténuer ces effets »
6. D'autres articles du *Règlement sur les installations nucléaires de catégorie I*, ainsi que des articles du *Règlement sur la radioprotection* et du *Règlement sur la sécurité nucléaire* qui se rapportent à la conception d'une nouvelle centrale nucléaire.

4.0 Objectifs et concepts de sûreté

4.1 Objectif général en matière de sûreté nucléaire

L'objectif général en matière de sûreté nucléaire adopté dans le document RD-337 (version 2) est compatible avec l'objet de la LSRN, qui vise « la limitation, à un niveau acceptable, des risques liés au développement, à la production et à l'utilisation de l'énergie nucléaire, ainsi qu'à la production, la possession et l'utilisation des substances nucléaires, de l'équipement réglementé et des renseignements réglementés, tant pour la préservation de la santé et de la sécurité des personnes et la protection de l'environnement que pour le maintien de la sécurité nationale, et le respect par le Canada de ses obligations internationales ».

L'objectif général en matière de sûreté nucléaire de la version 2 du document RD-337 est tiré de la publication de l'AIEA intitulée *La sûreté des installations nucléaires* (Collection sécurité n° 110), qui indique que l'objectif général de sûreté nucléaire est de « protéger les individus, la société et l'environnement en établissant et en maintenant dans les installations nucléaires des défenses efficaces contre les risques radiologiques ».

4.1.1 Objectif en matière de radioprotection

L'objectif en matière de radioprotection de la version 2 du document RD-337 est également tiré du document de l'AIEA intitulé *La sûreté des installations nucléaires*, qui indique que l'objectif de radioprotection consiste à « faire en sorte, dans toutes les conditions de fonctionnement, que la radioprotection à l'intérieur de l'installation et celle due à tout rejet programmé de matières radioactives à l'extérieur de l'installation soient maintenues au-dessous des limites prescrites et au niveau le plus bas qu'il est raisonnablement possible d'atteindre, et faire en sorte que soient atténuées les conséquences radiologiques des accidents ».

Comme l'indique *La sûreté des installations nucléaires*, l'objectif de radioprotection « n'exclut pas une radioexposition limitée de personnes ni le rejet depuis les installations de quantités légalement autorisées de matières radioactives dans l'environnement dans les conditions de fonctionnement. Cependant, de telles radioexpositions et de tels rejets doivent être sous contrôle strict et conformes aux limites d'exploitation et aux normes de radioprotection ».

4.1.2 Objectifs en matière de sûreté technique

Les objectifs en matière de sûreté technique de la version 2 du document RD-337 sont également tirés de *La sûreté des installations nucléaires*, qui indique que les objectifs de sûreté technique consistent à « prendre toutes les mesures raisonnablement praticables pour prévenir les accidents dans les installations nucléaires et pour en atténuer les conséquences s'il devait s'en produire; garantir, avec un haut niveau de confiance, que pour tous les accidents possibles pris en compte dans la conception de l'installation, même ceux de très faible probabilité, les conséquences radiologiques, s'il y en a, soient de faible importance et inférieures aux limites prescrites; et faire en sorte que la probabilité d'accidents avec conséquences radiologiques importantes soit extrêmement faible ».

4.1.3 Objectif en matière de protection environnementale

L'objectif en matière de protection environnementale assure l'exhaustivité dans le contexte canadien afin de garantir que la conception comporte des dispositions adéquates en matière de protection de l'environnement.

4.2 Application des objectifs de sûreté technique

Les objectifs en matière de sûreté technique définis ci-dessus établissent les objectifs généraux à atteindre pour assurer un niveau de sûreté élevé. Toutefois, ils n'indiquent pas la façon de mesurer l'atteinte de tels objectifs de manière quantitative. À cette fin, la version 2 du document RD-337 fournit des critères et des buts quantitatifs pour la conception des centrales nucléaires sous forme de critères d'acceptation des doses et d'objectifs de sûreté.

4.2.1 Critères d'acceptation des doses

Une analyse déterministe de sûreté est réalisée pour démontrer que les critères d'acceptation des doses liés aux accidents de dimensionnement sont atteints avec un haut niveau de confiance. L'analyse démontre que les fonctions de sûreté fondamentales sont remplies par les systèmes de sûreté en utilisant des hypothèses prudentes. Les fonctions de sûreté fondamentales sont décrites à la section 6.2 de la version 2 du document RD-337.

Les valeurs adoptées dans la version 2 du document RD-337 pour les critères d'acceptation des doses relatifs aux incidents de fonctionnement prévus (IFP) et aux accidents de dimensionnement (AD) sont conformes aux pratiques internationales reconnues et tiennent compte des recommandations de l'AIEA et de la Commission internationale de protection radiologique.

4.2.2 Objectifs en matière de sûreté

Les objectifs en matière de sûreté ont été établis pour permettre d'apprécier l'acceptabilité de la conception d'une centrale nucléaire à l'aide d'une approche tenant compte des risques. La publication de l'AIEA intitulée *Basic Safety Principles for Nuclear Power Plants (75-INSAG-3 rév. 1, INSAG-12)* indique que pour comparer les risques posés par les centrales nucléaires et les autres risques industriels auxquels les personnes et l'environnement sont exposés, l'analyse de risque doit utiliser des modèles de calcul. Elle mentionne également que pour tirer pleinement parti de ces techniques et appuyer la réalisation de l'objectif général en matière de sûreté nucléaire, il importe de formuler des objectifs quantitatifs, c.-à-d. *objectifs en matière de sûreté*.

Objectifs qualitatifs en matière de sûreté

Les objectifs qualitatifs en matière de sûreté ont été établis dans la version 2 du document RD-337 pour s'assurer que l'exploitation d'une centrale nucléaire n'expose les membres du public à aucun risque significatif en plus des autres risques auxquels ils sont normalement exposés. Ces objectifs sont atteints grâce à l'application des objectifs qualitatifs en matière de sûreté.

Application quantitative des objectifs en matière de sûreté

Pour démontrer que la conception répond aux objectifs quantitatifs en matière de sûreté énoncés dans la version 2 du document RD-337 en ce qui concerne la fréquence des dommages causés au cœur du réacteur, la fréquence des petites émissions radioactives et la fréquence des grandes émissions radioactives, on utilise des techniques probabilistes.

Comme indiqué dans la version 2 du document RD-337, « *la fréquence des dommages causés au cœur du réacteur est une mesure des capacités de prévention des accidents de la centrale. Les fréquences des petites émissions radioactives et les fréquences des grandes émissions radioactives sont des mesures des capacités d'atténuation des accidents de la centrale. Elles représentent aussi des mesures de risque pour la société et l'environnement en raison de l'exploitation d'une centrale nucléaire* ».

Les valeurs adoptées dans la version 2 du document RD-337 pour les objectifs qualitatifs en matière de sûreté sont conformes aux pratiques internationales reconnues pour les nouvelles centrales nucléaires.

Une étude probabiliste de sûreté (EPS) complète tient compte de la probabilité, de la progression et des conséquences des défaillances de l'équipement ou de conditions transitoires pour calculer des estimations numériques de la sûreté de la centrale. La fréquence des dommages causés au cœur du réacteur est déterminée par une EPS de niveau 1 qui identifie et quantifie la séquence d'événements pouvant conduire à une dégradation importante du cœur du réacteur. La fréquence des petites émissions radioactives et la fréquence des grandes émissions radioactives sont déterminées par une EPS de niveau 2 qui s'appuie sur les résultats de l'EPS de niveau 1, analyse le comportement du confinement, évalue les radionucléides libérés par le combustible défectueux et quantifie les rejets dans l'environnement.

Des détails supplémentaires sur les EPS se trouvent à la section 9.5 du présent document et dans la norme d'application de la réglementation de la CCSN S-294, *Études probabilistes de sûreté (EPS) pour les centrales nucléaires*.

4.2.3 Analyses de la sûreté

De l'orientation sur les analyses de la sûreté se trouve à la section 9.0 du présent document et des informations complémentaires sont fournies dans les documents de la CCSN RD-310, *Analyses de la sûreté pour les centrales nucléaires*, et GD-310, *Document d'orientation sur les analyses de la sûreté des centrales nucléaires*.

4.2.4 Atténuation et gestion des accidents

Cette section est traitée de manière suffisante par la version 2 du document RD-337, *Conception des nouvelles centrales nucléaires*. Il n'est donc pas nécessaire de fournir de l'orientation supplémentaire à ce sujet.

4.3 Concepts de sûreté

4.3.1 Défense en profondeur

Le document INSAG-10 de l'AIEA, intitulé *La défense en profondeur en sûreté nucléaire*, fournit de l'orientation à ce sujet. On trouvera également de l'orientation complémentaire à la section 6.1 du présent document.

4.3.2 Examen des barrières physiques

Consulter la section 6.1.1.

4.3.3 Limites et conditions d'exploitation

Les approches et les terminologies utilisées pour les limites et les conditions d'exploitation (LCE) varient parfois en fonction des pratiques et des systèmes de réglementation établis dans le pays d'origine de la conception de la centrale. Indépendamment des approches et des terminologies utilisées, l'autorité responsable de la conception devrait fournir des définitions claires des terminologies utilisées pour les LCE. La conception devrait également comprendre des objectifs et des buts clairs pour les LCE.

L'information liée aux LCE devrait donner la liste de toutes les normes (nationales et internationales) pertinentes utilisées et documenter la façon dont les exigences de ces normes ont été respectées.

Les LCE peuvent varier en fonction de la conception du réacteur nucléaire, de la philosophie générale en matière de sûreté et de la configuration d'exploitation de la centrale.

Les LCE doivent être définies pour un ensemble approprié de configurations limitatives d'exploitation de la centrale et être fondées sur la conception approuvée de la centrale.

Renseignements supplémentaires

D'autres renseignements sont disponibles dans les documents suivants :

- Norme CSA N290.15-F10, *Exigences relatives aux limites d'exploitation sûre des centrales nucléaires*, Association canadienne de normalisation [2010]
- Guide de sûreté de l'AIEA NS-G-2.2, *Operational Limits and Conditions and Operating Procedures for Nuclear Power Plants* [2000]

4.3.4 Interface entre la sûreté, la sécurité et les garanties

Cette section est traitée de manière suffisante par la version 2 du document RD-337, *Conception des nouvelles centrales nucléaires*. Il n'est donc pas nécessaire de fournir de l'orientation supplémentaire à ce sujet.

5.0 Gestion de la sûreté dans la conception

5.1 Autorité en matière de conception

Renseignements supplémentaires

D'autres renseignements sont disponibles dans les documents suivants :

- AIEA, collection Normes de sûreté n° GS-G-3.5, *The Management System for Nuclear Installations Safety Guide* [2009]
- AIEA, INSAG-19, *Maintaining the Design Integrity of Nuclear Installations throughout their Operating Life* [2003]

5.2 Gestion de la conception

Cette section est traitée de manière suffisante par la version 2 du document RD-337, *Conception des nouvelles centrales nucléaires*. Il n'est donc pas nécessaire de fournir de l'orientation supplémentaire à ce sujet.

5.3 Mesures de contrôle de la conception

Les mesures de contrôle de la conception (processus, procédures et pratiques) comprennent les éléments suivants :

- le lancement, la spécification de la portée et la planification de la conception
- la spécification des exigences de conception
- la sélection d'un personnel convenablement qualifié et expérimenté
- le contrôle des travaux et la planification des activités de conception
- la spécification et le contrôle des intrants de conception
- l'examen et la sélection des concepts de conception
- la sélection d'outils et de logiciels de conception
- la réalisation de l'analyse conceptuelle
- la réalisation d'une conception détaillée et la production de documents et de dossiers sur la conception
- la réalisation d'une analyse de sûreté détaillée
- la définition de toute condition limitative à l'exploitation sûre
- la vérification et la validation de la conception
- l'indépendance des personnes ou des groupes effectuant les vérifications, les validations et les approbations
- la gestion de la configuration
- la gestion de la conception et le contrôle des changements apportés à la conception
- l'identification et le contrôle des interfaces de conception

La norme CSA N286-05F, *Exigences relatives au système de gestion des centrales nucléaires*, est la norme canadienne identifiant les exigences relatives au système de gestion en ce qui concerne la conception, l'acquisition, la construction, l'installation, l'exploitation et le déclassement des centrales nucléaires. La norme CSA N286.7-F99, *Assurance de la qualité des programmes informatiques scientifiques, d'analyse et de conception des centrales nucléaires*, fournit des exigences complémentaires pour les programmes informatiques scientifiques, d'analyse et de conception.

Les organisations de pays n'utilisant pas les documents susmentionnés devraient identifier les codes, les normes et les spécifications sur lesquels reposent leurs mesures de contrôle de la conception et de l'analyse de la sûreté, qu'ils soient nationaux ou internationaux, tels que la norme de sûreté de l'AIEA GS-G-3.5, *The Management System for Nuclear Installations Safety Guide* et les publications citées en référence, ainsi que la norme ISO 9001:2008, *Systèmes de management de la qualité – Exigences*. De telles mesures de contrôle devraient être reliées aux clauses requises par la norme CSA N286-05 pour démontrer qu'elles satisfont aux exigences canadiennes. En cas d'identification de lacunes, il faudrait décrire les mesures prises pour les combler.

Les procédures et les processus organisationnels peuvent être propres à la conception et à l'analyse de la sûreté, ou peuvent faire partie d'un système de gestion global (ou d'un programme d'assurance de la qualité) appliqué à d'autres activités du cycle de vie de la centrale nucléaire. Dans ce dernier cas, l'organisation devrait identifier les processus et procédures applicables à la conception et à l'analyse de la sûreté.

Il n'y a pas d'exigences particulières à l'égard des plateformes, des styles ou des formats utilisés pour documenter les mesures de contrôle de la conception. Toutefois, les organisations chargées de la conception devraient identifier les types de documents, le style, le format et le support (papier, électronique ou application Internet) qu'ils envisagent d'utiliser pour contrôler leurs activités de conception.

Renseignements supplémentaires

D'autres renseignements sont disponibles dans les documents suivants :

- CSA N286.7.1-09, *Guideline for the application of N286.7-99, Quality assurance of analytical, scientific, and design computer programs for nuclear power plants* [2009]
- AIEA, GS-R-3, *Système de gestion des installations et des activités* [2006]
- Nuclear Information and Records Management Association/American National Standards Institute (NIRMA/ANSI), *Standard Configuration Management (CM), 1.0* [2007]

5.4 Méthodes d'ingénierie éprouvées

Cette section est traitée de manière suffisante par la version 2 du document RD-337, *Conception des nouvelles centrales nucléaires*. Il n'est donc pas nécessaire de fournir de l'orientation supplémentaire à ce sujet.

5.5 Expérience opérationnelle et recherche en matière de sûreté

Tel qu'indiqué dans la version 2 du document RD-337, « *la conception d'une CN doit être basée sur l'expérience opérationnelle acquise dans l'industrie nucléaire, ainsi que sur les résultats de programmes de recherche pertinents* ».

L'autorité responsable de la conception doit décrire les principaux changements, caractéristiques et améliorations apportés à la conception en raison de l'expérience opérationnelle et des recherches en matière de sûreté, y compris :

- les réponses apportées aux questions de sûreté concernant les conceptions de réacteurs existantes
- les améliorations apportées à la conception à la suite des progrès réalisés au niveau des matériaux et de leurs caractéristiques
- l'amélioration des méthodes de conception et d'évaluation de la sûreté
- l'amélioration des procédés de construction et de fabrication
- les améliorations relatives à la fiabilité, à l'exploitabilité et à la capacité d'entretien
- l'amélioration des méthodes permettant de réduire la fréquence des erreurs humaines et d'atténuer les conséquences de celles-ci
- l'amélioration des méthodes permettant de maintenir les doses « au niveau le plus bas qu'il soit raisonnablement possible d'atteindre » (principe ALARA, de l'anglais *as low as reasonably achievable*)

Des informations relatives à l'expérience opérationnelle se trouvent dans des documents tels que ceux publiés chaque année par l'AIEA et intitulés *Operating Experience with Nuclear Power Stations in Member States*.

Renseignements supplémentaires

D'autres renseignements sont disponibles dans le document suivant :

- AIEA, norme de sûreté NS-G-2.11, *A System for the Feedback of Experience from Events in Nuclear Installation* [2006]

5.6 Évaluation de la sûreté

La réalisation de l'évaluation de la sûreté devrait utiliser un processus formel. Les aspects pris en considération dans l'évaluation de la sûreté comprennent :

- les dispositions liées à la défense en profondeur
- la pertinence des marges de sûreté
- les barrières multiples
- l'analyse de la sûreté, comprenant à la fois des approches déterministe et probabiliste, ainsi que la portée générale, la méthode, les critères de sûreté, l'analyse des incertitudes et des vulnérabilités, l'utilisation des programmes informatiques et le recours à l'expérience opérationnelle
- les risques radiologiques
- les fonctions de sûreté
- les caractéristiques de l'emplacement
- la radioprotection
- les aspects d'ingénierie
- les facteurs humains
- la sûreté à long terme

Tel qu'indiqué dans la version 2 du document RD-337, avant la présentation de la conception, un examen indépendant doit être effectué. L'examen indépendant est réalisé par des personnes convenablement qualifiées et expérimentées, différentes de celles ayant effectué l'évaluation de la sûreté.

Renseignements supplémentaires

D'autres renseignements sont disponibles dans le document suivant :

- AIEA, GSR Part 4, *Évaluation de la sûreté des installations et activités* [2009]

5.7 Documentation sur la conception

Il faudrait préparer une série de documents relatifs à la conception après avoir établi un cadre de référence global énumérant l'ensemble des documents importants pour la conception. Les documents relatifs à la conception devraient faire partie d'un cadre logique et facile à gérer.

Renseignements supplémentaires

D'autres renseignements sont disponibles dans le document suivant :

- CCSN, RD/GD-369, *Guide de présentation d'une demande de permis : Permis de construction d'une centrale nucléaire* [2011]

6.0 Orientations relatives aux exigences en matière de sûreté

6.1 Application du concept de défense en profondeur

La version 2 du document RD-337 stipule que « un mécanisme de défense en profondeur doit être établi à l'étape de conception grâce à l'application de dispositions propres aux cinq niveaux de défense ».

Le document INSAG-10 de l'AIEA, intitulé *La défense en profondeur en sûreté nucléaire*, est un rapport du Groupe consultatif international pour la sûreté nucléaire qui fournit des renseignements conduisant au concept et à l'application de la défense en profondeur.

On trouvera de l'orientation relative à la réalisation d'une évaluation systématique de la défense en profondeur dans le document n° 46 de la collection Rapports de sûreté de l'AIEA intitulé *Assessment of Defence in Depth for Nuclear Power Plants*.

L'application de la défense en profondeur à l'étape de la conception devrait assurer les éléments suivants :

- La méthode de défense en profondeur utilisée dans la conception devrait garantir que tous les aspects de la conception ont été traités au niveau des SSC, en accordant une attention particulière aux SSC importants pour la sûreté.
- La défense en profondeur ne devrait pas subir de dégradation importante si les SSC ont des fonctions multiples (p. ex. pour les réacteurs CANDU, le modérateur et les systèmes de refroidissement des boucliers d'extrémité peuvent assumer la fonction d'un système fonctionnel et comprendre les fonctions d'atténuation des effets des conditions additionnelles de dimensionnement [CAD]).
- Le principe de barrières physiques multiples contre le rejet de matières radioactives devrait être incorporé dans la conception; il devrait y avoir un nombre limité de cas où il y a réduction du nombre de barrières physiques (comme dans le cas où certains composants transportant des matières radioactives servent également de confinement) et une justification adéquate devrait être fournie pour de tels choix de conception.
- La conception (p. ex. dans les guides de conception de la sûreté, les programmes du système de gestion) devrait fournir :
 - les niveaux de défense en profondeur abordés par chaque SSC
 - les analyses et les calculs justificatifs
 - l'évaluation des procédures d'exploitation
- L'analyse de sûreté devrait démontrer que les facteurs susceptibles de menacer l'intégrité des barrières physiques ne dépassent pas les capacités physiques de celles-ci.
- Il faudrait établir la structure des dispositions relatives à la défense en profondeur pour chaque niveau de défense pour une conception de réacteur donnée. Il faudrait également procéder à l'évaluation de la conception dans une perspective de maintien de chaque fonction de sûreté. Cette évaluation devrait prendre en compte chacune des dispositions d'atténuation d'un mécanisme de mise à l'épreuve donné et confirmer que ces dispositions sont bien fondées, suffisantes, réalistes et correctement conçues.
- Il faudrait porter une attention particulière au caractère réaliste d'une disposition donnée et à l'existence d'analyses de sûreté justificatives. Tout manque d'exhaustivité des analyses de sûreté justificatives devrait être documenté et considéré comme une question à vérifier.

6.1.1 Examen des barrières physiques

Il faudrait assurer l'indépendance des différents niveaux de défense, en particulier, par des dispositions diverses. Le renforcement de chacun de ces niveaux séparément permettrait d'aboutir, autant que réalisable au renforcement global de la défense en profondeur. Par exemple, l'utilisation de systèmes dédiés destinés à faire face aux CAD assure l'indépendance du quatrième niveau de défense.

Pour assurer l'efficacité de l'indépendance des différents niveaux de défense, les caractéristiques de conception visant à prévenir un accident et les caractéristiques de conception visant à atténuer les conséquences du même accident ne devraient pas appartenir au même niveau de défense.

6.2 Fonctions de sûreté

Cette section est traitée de manière suffisante par la version 2 du document RD-337, *Conception des nouvelles centrales nucléaires*. Il n'est donc pas nécessaire de fournir de l'orientation supplémentaire à ce sujet.

6.3 Prévention des accidents et caractéristiques de sûreté de la centrale

Cette section est traitée de manière suffisante par la version 2 du document RD-337, *Conception des nouvelles centrales nucléaires*. Il n'est donc pas nécessaire de fournir de l'orientation supplémentaire à ce sujet.

6.4 Radioprotection et critères d'acceptation

Une évaluation détaillée des doses de rayonnement devrait comprendre une estimation des doses efficaces et des doses équivalentes annuelles collectives et individuelles reçues par les employés du site et les membres du public en mode d'exploitation normal, les doses éventuelles de rayonnement reçues par le public en cas d'IFP et d'AD et les rejets potentiels dans l'environnement en cas de CAD.

Le processus d'évaluation devrait être clairement documenté et comprendre le processus permettant d'examiner et d'évaluer la diminution des doses de rayonnement en fonction des changements apportés à la conception de la centrale nucléaire. Ceci est effectué pour veiller à ce que les doses reçues par les employés du site et les membres du public respectent le principe ALARA et qu'elles ne dépasseront pas les limites de doses pertinentes précisées dans le *Règlement sur la radioprotection* ainsi que les critères d'acceptation des doses et les objectifs de sûreté pertinents de la version 2 du document RD-337. Les doses de rayonnement découlant de l'exploitation de la centrale devraient être réduites au moyen de contrôles spécifiquement conçus et de mesures de radioprotection, à des niveaux tels que des dépenses supplémentaires pour la conception, la construction et des mesures opérationnelles ne seraient pas justifiées par la diminution prévue des doses de rayonnement.

Le processus d'évaluation des doses de rayonnement devrait comprendre le taux d'occupation estimé dans les zones de rayonnement de la centrale ainsi qu'une estimation des doses annuelles (exprimées en Sv) reçues par les personnes associées aux principales activités, y compris la manipulation des déchets radioactifs, l'entretien normal, l'entretien en conditions particulières, le rechargement du combustible et les inspections en cours d'exploitation. Des telles évaluations devraient comprendre des renseignements sur la façon d'utiliser le principe ALARA et l'expérience opérationnelle dans la conception pour traiter les facteurs qui contribuent de façon importante aux doses de rayonnement.

Renseignements supplémentaires

D'autres renseignements sont disponibles dans les documents suivants :

- CCSN, G-129, révision 1, *Maintenir les expositions et les doses au « niveau le plus bas qu'il soit raisonnablement possible d'atteindre (ALARA) »* [2004]
- CAN/CSA-N288.2-M91 (R2008), *Guidelines for Calculating Radiation Doses to the Public from a Release of Airborne Radioactive Material under Hypothetical Accident Conditions in Nuclear Reactors* [2008]

6.5 Zone d'exclusion

Conformément à la définition donnée par le *Règlement sur les installations nucléaires de catégorie I*, une zone d'exclusion est « une parcelle de terrain qui relève de l'autorité légale du titulaire de

permis, qui est située à l'intérieur ou autour d'une installation nucléaire, et où il ne se trouve aucune habitation permanente ».

Historiquement, la zone d'exclusion des centrales nucléaires au Canada a été fixée à 914 mètres à partir du bâtiment du réacteur. Plutôt que de prescrire une zone d'exclusion de taille particulière, la version 2 du document RD-337 définit les facteurs devant être pris en considération pour établir une zone de taille appropriée, comprenant les besoins d'évacuation, les besoins d'utilisation des terres, les exigences de sécurité et les facteurs environnementaux.

Besoins d'évacuation

La conception devrait tenir compte des exigences relatives aux interventions d'urgence en fonction de la taille de la zone d'exclusion, des installations et des infrastructures se trouvant à l'intérieur de la zone. De manière générale, une zone d'exclusion plus grande exigera un temps de réponse plus long et une plus grande capacité d'intervention.

Les limites de la zone d'exclusion devraient être définies en tenant compte des capacités des organismes d'intervention d'urgence sur le site et hors du site. La conception tient également compte des changements projetés au fil du temps dans l'utilisation des terres et la densité de la population, changements qui pourraient avoir une incidence négative sur le temps d'intervention ou la capacité d'évacuer et de mettre à l'abri les personnes se trouvant sur le site même et celles situées dans les régions de planification d'urgence.

Les besoins d'évacuation reposent généralement sur les plans provinciaux d'intervention en cas d'urgence nucléaire existants.

Besoins d'utilisation des terres

La conception devrait veiller à ce que la zone d'exclusion soit suffisamment vaste pour contenir le site de la centrale nucléaire (en tenant compte du nombre maximal de tranches que l'on propose de construire sur le site, qu'elles soient construites immédiatement ou pas).

Les activités de conception devraient veiller à optimiser l'utilisation des terres par la centrale dans le cadre de la détermination de la zone d'exclusion.

Exigences de sécurité

La conception devrait fournir les exigences de sécurité en fonction de la taille de la zone d'exclusion, des installations et des infrastructures se trouvant à l'intérieur de la zone, ainsi que de la conception de l'installation. De manière générale, une zone d'exclusion plus grande exigera davantage de capacités en matière de sécurité afin d'éviter de prolonger les délais d'intervention. Les caractéristiques physiques du site en tant que tel (dont les caractéristiques géographiques, comme la proximité par rapport à un terrain élevé) jouent également un rôle dans la détermination de ces exigences.

L'autorité responsable de la conception peut décider de prévoir des mesures d'atténuation de ces risques tout en maintenant une zone d'exclusion plus petite, en choisissant une conception hautement robuste pour l'installation, en appliquant des mesures de sécurité spécifiquement conçues sur le site et en mettant en place un programme de sécurité bien conçu. Ces mesures spécifiquement conçues devraient être décrites.

Au moment d'établir le rayon des limites de la zone d'exclusion, la conception devrait tenir compte des éléments suivants :

- le rapport sur l'évaluation des menaces et des risques dans le choix de l'emplacement
- la robustesse de l'installation contre les événements externes naturels et anthropiques (y compris les actes malveillants)

- la capacité du programme de sécurité sur le site ainsi que les ressources de sécurité hors site qui compléteront le programme de sécurité sur le site

Pour chacun des paramètres évoqués ci-dessus, la conception devrait tenir compte des changements au fil du temps dans l'utilisation des terres et la densité de la population, changements qui pourraient avoir une incidence négative sur ces paramètres. La conception devrait faire en sorte que le rayon de la zone d'exclusion, tel qu'établi à l'étape de la conception, soit durable pour le cycle de vie complet de l'installation.

L'acceptabilité des renseignements à présenter à l'appui des éléments précités est discutée à la section 7.22 du présent document.

Facteurs environnementaux

Les facteurs environnementaux susceptibles d'exercer une influence sur la taille de la zone d'exclusion comprennent les conditions météorologiques locales pouvant influencer sur la dose de rayonnement reçue par les membres du public. En l'absence d'un site spécifique, l'autorité responsable de la conception peut utiliser des données génériques en utilisant des hypothèses conservatrices concernant les conditions météorologiques.

Le *Règlement sur la radioprotection* établit une limite de dose efficace de 1 mSv par année pour les membres du public. Cette limite implique qu'un membre du public hypothétique vivant pendant un an à la périphérie de la zone d'exclusion (étant donné qu'aucune habitation permanente n'est autorisée à l'intérieur de la zone d'exclusion) n'accumulera pas une dose supérieure à 1 mSv en raison de l'exploitation de la centrale nucléaire.

Les critères d'acceptation des doses décrits à la section 4.2.1 de la version 2 du document RD-337 doivent être respectés à la périphérie du site.

Renseignements supplémentaires

D'autres renseignements sont disponibles dans le document suivant :

- CCSN, RD-346, *Évaluation de l'emplacement des nouvelles centrales nucléaires* [2008]

6.6 Plan de l'installation

Cette section est traitée de manière suffisante par la version 2 du document RD-337, *Conception des nouvelles centrales nucléaires*. Il n'est donc pas nécessaire de fournir de l'orientation supplémentaire à ce sujet.

6.6.1 Exigences pour les centrales à tranches multiples

Tel qu'indiqué dans la version 2 du document RD-337, « *la conception doit tenir compte des défis que pose un site à tranches multiples. Plus particulièrement, il faut prendre en considération les risques associés aux événements d'origine commune qui touchent aux moins deux tranches en même temps* ». De tels événements pourraient aggraver les défis posés au personnel de la centrale en cas d'accident. Les événements et les conséquences d'un accident dans une tranche peuvent affecter la progression de l'accident ou entraver les activités de gestion des accidents à la tranche voisine, et les ressources disponibles (personnel, équipement, carburant) devraient être partagées entre plusieurs tranches.

7.0 Orientation relative aux exigences générales de la conception

7.1 Classification des SSC

La méthode utilisée pour établir la classification de sûreté des SSC importants pour la sûreté devrait être principalement fondée sur des méthodes déterministes, complétées (au besoin) par des méthodes probabilistes. La classification de sûreté des SSC devrait être un processus itératif qui continue tout au long du processus de conception.

Le processus de classification des SSC devrait comprendre les activités suivantes :

- l'examen et la définition des événements initiateurs hypothétiques (EIH)
- l'identification des caractéristiques de sûreté de prévention et des fonctions de sûreté d'atténuation propres à la centrale, fondées sur le système ou le sous-système connexe
- le classement des caractéristiques de sûreté de prévention et des fonctions de sûreté d'atténuation en fonction de leur importance sur le plan de la sûreté et du rôle qu'elles jouent pour remplir les fonctions de sûreté fondamentales
- l'identification des SSC qui assurent les caractéristiques de sûreté de prévention et les fonctions de sûreté d'atténuation
- l'attribution aux SSC d'une classe de sûreté correspondant à la catégorie de sûreté
- la vérification de la classification des SSC
- l'identification des règles de conception technique des SSC classés

Cette approche devrait être utilisée pour tous les SSC, y compris les composants sous pression, les équipements électriques, les systèmes d'instrumentation et de contrôle (IC) et les structures de génie civil.

Les EIH identifiés devraient être groupés en cas limites, qui sont appelés EIH limitatifs ou enveloppe des EIH. Une fois que ces EIH limitatifs sont connus et bien compris, il est possible d'identifier les fonctions de sûreté requises. Chaque fonction de sûreté peut être affectée à une caractéristique de sûreté de prévention ou à une fonction de sûreté d'atténuation. Le nombre de catégories et de classes peut être choisi pour obtenir des règles de conception graduelles.

Tel qu'indiqué dans la version 2 du document RD-337, « *tous les SSC doivent être identifiés comme étant soit importants ou non importants au plan de la sûreté. Les critères servant à déterminer leur importance au plan de la sûreté sont fondés sur :*

1. *les fonctions de sûreté à exécuter*
2. *la conséquence d'une défaillance*
3. *la probabilité que les SSC soient sollicités pour exécuter la fonction de sûreté*
4. *le délai suivant un EIH avant que les SSC ne soient appelés à intervenir et la durée prévue de cette opération »*

On pourrait considérer que la redondance et la diversité s'appliquent aux facteurs 3 et 4 susmentionnés.

Le délai suivant un EIH identifié au facteur 4 reproduit le besoin d'une intervention automatique pour les délais très courts ou d'interventions manuelles acceptables pour les mesures à plus long terme. La durée prévue de l'opération est également importante dans la mesure où certains systèmes sont parfois appelés à fonctionner durant plusieurs mois alors que d'autres (comme les systèmes d'arrêt d'urgence) peuvent accomplir leur mission en l'espace de quelques secondes.

Il faudrait évaluer la gravité potentielle des conséquences d'une fonction défaillante. Lors de l'évaluation, il est possible de supposer que la caractéristique ou la fonction de sûreté à classer dans

une catégorie subisse une défaillance, et que d'autres caractéristiques et fonctions de sûreté demeurent fonctionnelles.

Voici quelques directives spécifiques en matière de classification des SSC :

- s'il y a des SSC dont la défaillance ne peut être acceptée parce qu'elle entraînerait avec certitude des conséquences inacceptables, alors ces SSC devraient être affectés à la classe de sûreté la plus élevée
- en règle générale, les SSC de support devraient être affectés à la même classe que celle des SSC de première ligne à appuyer
- si un SSC particulier contribue à l'exécution de plusieurs fonctions de sûreté de catégories différentes, il devrait être affecté à la classe correspondant à la catégorie de sûreté la plus élevée, en exigeant les règles de conception les plus prudentes
- la classification des SSC devrait rester la même, indépendamment du mode de fonctionnement du SSC (qu'il soit actif, passif, ou une combinaison des deux)
- tout SSC ne faisant pas partie d'un groupe de fonctions de sûreté mais dont la défaillance pourrait avoir une incidence négative sur la capacité de ce groupe à accomplir ses fonctions de sûreté (si la chose ne peut être empêchée par la conception), devrait être classé conformément à la catégorie de sûreté de ce groupe de fonctions de sûreté
- lorsque des SSC reliés entre eux ou en interaction les uns avec les autres appartiennent à des classes de sûreté différentes (y compris lorsqu'un SSC appartenant à une classe de sûreté est relié à un autre SSC sans importance au plan de la sûreté), l'interférence entre les SSC devrait être séparée par un dispositif (p. ex. un isolateur physique ou optique) rangé dans une classe de sûreté plus élevée afin de s'assurer que la défaillance du SSC de la classe de sûreté moins élevée ne se propage pas au SSC de la classe de sûreté supérieure

Bien que la probabilité d'une sollicitation des SSC en cas de CAD soit très faible, la défaillance des fonctions de sûreté destinées à atténuer les CAD pourrait avoir des conséquences très graves. Par conséquent, ces fonctions de sûreté devraient être considérées comme une catégorie de sûreté de niveau élevé.

La pertinence de la classification de sûreté devrait être vérifiée à l'aide d'une analyse déterministe de la sûreté qui devrait couvrir tous les EIH et toutes les fonctions de sûreté validées. Cette vérification devrait être complétée, au besoin, par les informations fournies par l'étude probabiliste de sûreté et par le jugement technique.

Tel qu'indiqué à la section 7.5, les règles et limites de conception appropriées sont spécifiées conformément à la classe de sûreté des SSC.

7.2 Enveloppe de conception de la centrale

Tel qu'indiqué dans la version 2 du document RD-337, « l'autorité responsable de la conception doit établir l'enveloppe de conception de la centrale, laquelle comprend tous les états pris en compte dans la conception, soit l'exploitation normale, les IFP, les AD et les CAD ».

Le dimensionnement de chaque SSC important pour la sûreté devrait être défini et justifié de façon systématique. La conception devrait également fournir toute l'information permettant à l'organisme exploitant de faire fonctionner la centrale de façon sécuritaire.

Les conditions qui s'écartent des principes de conception déterministes prudents devraient être clairement énoncées, y compris les fondements permettant de justifier de tels écarts au cas par cas. De tels fondements peuvent comprendre une méthode de calcul plus perfectionnée, qui a été bien établie, ou de multiples façons permettant d'exécuter une fonction particulière.

La conception devrait adopter des principes de conception déterministes présentant un niveau de conservatisme approprié. Par exemple, les SSC devraient être robustes, tolérer une vaste gamme de défauts avec une dégradation graduelle de leur efficacité, et ne devraient pas subir de défaillance catastrophique dans les divers états de fonctionnement et en conditions d'accident.

Une caractéristique de conception complémentaire est une caractéristique de conception ajoutée à la conception en tant que SSC autonome ou en tant que capacité ajoutée à un SSC existant pour faire face aux CAD.

Les principes de conception liés aux caractéristiques de conception complémentaires destinées à faire face aux CAD n'ont pas nécessairement besoin d'incorporer la même marge de prudence que celles appliquées à la conception pour tous les états de fonctionnement, y compris en cas d'AD. Toutefois, il faut obtenir une assurance raisonnable que les caractéristiques de conception complémentaires exécuteront leurs fonctions prévues lorsqu'elles doivent servir.

7.3 États de la centrale

Comme le montre la figure 1 de la version 2 du document RD-337, les états de la centrale se divisent en états de fonctionnement et en conditions d'accident. Les exigences de conception des SSC devraient donc être élaborées pour s'assurer que la centrale est capable de répondre aux exigences déterministes et probabilistes applicables à chaque état de la centrale.

La conception devrait comprendre les éléments suivants :

- les critères pour le retour à l'exploitation normale à la suite d'un IFP ou d'un AD (p. ex. les fonctions de sûreté sont assurées et les LCE pour les configurations d'exploitation sont respectées)
- les principaux paramètres et caractéristiques des divers états de fonctionnement, y compris les valeurs nominales et les écarts dus aux incertitudes et aux réglages des instruments, des systèmes de commande, des systèmes de déclenchement, du délai d'intervention des équipements, ou dus aux fluctuations des processus
- les conditions admissibles pour différentes configurations d'exploitation (p. ex. réacteur froid ou sous pression), y compris la durée des conditions transitoires (p. ex. le niveau de puissance du réacteur ou de la turbine, la durée de la variation de puissance normale prévue, les vitesses d'échauffement et de refroidissement) tout au long de la durée de vie utile de la centrale nucléaire
- les méthodes utilisées pour faire passer la centrale d'une configuration d'exploitation à l'autre
- les configurations sécuritaires finales à la suite d'IFP, d'AD et de CAD

7.3.1 Exploitation normale

La conception veille à ce que l'exploitation normale soit exécutée de manière sûre et, par conséquent, confirme que les doses de rayonnement auxquelles sont exposés les travailleurs et les membres du public, ainsi que tout rejet prévu de matières radioactives en provenance de la centrale, respecteront les limites autorisées précisées dans le *Règlement sur la radioprotection* et satisferont aux exigences de la section 4.1.1 du document RD-337 (version 2).

Les configurations d'exploitation en mode d'exploitation normale sont traitées par les LCE décrites à la section 4.3.3. Celles-ci comprennent habituellement :

- le démarrage normal du réacteur (de l'état d'arrêt à la pleine puissance en passant par la criticité)

- l'exploitation en puissance, y compris les régimes d'exploitation à pleine puissance et à faible puissance
- les changements dans la puissance du réacteur, y compris les régimes en suivi de charge et le retour au régime d'exploitation à pleine puissance après avoir été pendant une longue période à faible puissance
- l'exploitation lors du passage d'une configuration à l'autre, comme la mise à l'arrêt du réacteur après l'exploitation en puissance (arrêt chaud, refroidissement)
- le rechargement du combustible en mode d'exploitation normale, le cas échéant
- l'arrêt en mode de rechargement du combustible ou dans une autre condition d'entretien qui ouvre l'enceinte de refroidissement ou l'enveloppe de confinement
- la manutention du combustible frais ou irradié

Les principaux paramètres et les caractéristiques uniques de chaque configuration opérationnelle, ainsi que toute disposition de conception particulière visant à maintenir la configuration, devraient être cernés. Les périodes admissibles d'exploitation dans diverses configurations (p. ex., la charge) dans l'éventualité d'un écart par rapport aux configurations d'exploitation normale devraient aussi être identifiées.

7.3.2 Incident de fonctionnement prévu

Conformément aux exigences formulées à la section 4.3.1 de la version 2 du document RD-337 pour les niveaux 2 et 3 de défense en profondeur, la conception devrait inclure les résultats des analyses des IFP et des AD afin de démontrer la robustesse de la tolérance à la défaillance dans la conception technique ainsi que l'efficacité des systèmes de sûreté. L'analyse devrait couvrir toute la gamme des événements pour tout l'éventail de puissance du réacteur. L'analyse devrait également couvrir toutes les configurations en mode d'exploitation normale, y compris en régime d'exploitation à faible puissance et en état d'arrêt.

Pour une vaste gamme d'IFP, la conception devrait fournir une garantie raisonnable que tout écart du mode d'exploitation normale peut être détecté, et qu'on peut s'attendre à ce que les systèmes de contrôle ramènent la centrale dans un état sûr, sans avoir normalement à activer les systèmes de sûreté. En ce qui concerne les IFP et les AD, le niveau de confiance que les systèmes qualifiés (comme il est précisé à la section 5.4.4 du document d'application de la réglementation RD-310) fonctionnant seuls peuvent atténuer l'événement devrait être élevé.

Pour chaque groupe d'EIH, il peut être suffisant d'analyser seulement un nombre limité d'événements initiateurs limitatifs qui peuvent représenter une réponse limitative pour un groupe d'événements. La raison d'être du choix de ces événements limitatifs devrait être indiquée. Les paramètres de la centrale qui sont importants pour le résultat des analyses de sûreté devraient également être précisés. Parmi ces paramètres se trouvent généralement :

- la puissance du réacteur et sa distribution
- la température du cœur du réacteur
- l'oxydation et la déformation de la gaine de combustible
- les pressions dans les systèmes primaires et secondaires
- les paramètres de confinement
- les températures et les débits
- les coefficients de réactivité
- les paramètres cinétiques du réacteur
- la valeur de réactivité des dispositifs de réactivité

Les caractéristiques des systèmes de sûreté, y compris les conditions d'exploitation dans lesquelles les systèmes sont actionnés, les retards dans le temps, et la capacité des systèmes après le déclenchement indiquée dans la conception, devraient être précisés et démontrés de façon à être conformes aux exigences fonctionnelles et de performance générales des systèmes.

On trouvera des exemples d'IFP dans le document GD-310, *Document d'orientation sur les analyses de la sûreté des centrales nucléaires*.

7.3.3 Accident de dimensionnement

La conception identifie l'ensemble des AD et des conditions connexes pour lesquelles la CN est conçue, y compris le déclenchement manuel des systèmes ou d'autres interventions de l'opérateur.

On trouvera des exemples d'AD dans le document GD-310, *Document d'orientation sur les analyses de la sûreté des centrales nucléaires*.

7.3.4 Conditions additionnelles de dimensionnement

Pour identifier les CAD, il faudrait tenir compte des éléments suivants :

- les facteurs liés à la progression de l'accident (c.-à-d. les conditions physiques, les processus et les phénomènes physiques)
- les scénarios d'accidents hors dimensionnement ou d'accidents graves provoqués par des événements initiateurs, des interventions humaines et l'exploitabilité des SSC (réussite ou défaillance)
- la sélection d'événements limitatifs envisagés dans la conception et la détermination des valeurs limites ou des ensembles de paramètres de ces événements

La conception devrait identifier les caractéristiques conçues pour servir à prévenir ou atténuer les événements pris en considération dans les CAD, ou celles qui sont capables de le faire. Ces caractéristiques comprennent des caractéristiques de conception complémentaires et d'autres SSC susceptibles d'être validés pour les CAD. Ces caractéristiques devraient :

- être indépendantes, dans la mesure du praticable, de celles utilisées dans les accidents plus fréquents
- présenter une fiabilité correspondant aux fonctions qu'elles doivent remplir

Le choix des CAD à analyser devrait être expliqué et justifié, en indiquant s'il a été fondé sur une EPS ou une autre analyse permettant de cerner les vulnérabilités possibles de la centrale.

La version 2 du document RD-337 indique que « *la conception doit identifier un terme source pour un accident radiologique avec un gaz combustible pour fins d'utilisation dans la spécification des caractéristiques de conception complémentaires pour les CAD* ». Ce terme source de référence devrait être calculé pour un ensemble de scénarios d'accidents représentatifs, fondés sur les modèles de la « meilleure estimation ». La conception devrait tenir compte des incertitudes liées aux principaux paramètres et des changements possibles des processus physiques qui les régissent.

Les accidents de cette catégorie sont habituellement des séquences comportant plus d'une défaillance (à moins qu'on en ait tenu compte dans l'AD à l'étape de la conception). De telles séquences peuvent inclure des AD accompagnés d'un rendement affaibli d'un système de sûreté et des séquences susceptibles de provoquer le contournement de l'enceinte de confinement. L'analyse de ces accidents peut :

- avoir recours aux modèles et aux hypothèses de la « meilleure estimation »
- prendre le mérite du fonctionnement et du rendement réalistes des systèmes au-delà des fonctions initiales prévues, y compris les systèmes sans importance pour la sûreté
- prendre le mérite des interventions réalistes des opérateurs

Si cela n'est pas possible, des hypothèses raisonnablement conservatrices devraient être formulées, dans lesquelles les incertitudes relatives à la compréhension des processus physiques modélisés seront prises en compte. L'analyse devrait justifier l'approche qui a été adoptée.

On trouvera des exemples d'AHD dans le document GD-310, *Document d'orientation sur les analyses de la sûreté des centrales nucléaires*.

7.3.4.1 Accident grave

Les accidents graves sont des conditions d'accident qui entraînent une détérioration importante du combustible, que ce soit à l'intérieur du cœur du réacteur ou au niveau du stockage du combustible.

Une analyse détaillée devrait être réalisée et consignée par écrit afin de déterminer et de caractériser les accidents susceptibles d'entraîner des dommages importants au cœur ou des rejets de matières radioactives hors du site (accidents graves). En outre, il faudrait effectuer des évaluations de la capacité des caractéristiques de conception complémentaires à faire face aux CAD. Les difficultés que présentent de tels événements pour la centrale et la mesure selon laquelle la conception peut raisonnablement atténuer leurs conséquences, devraient être prises en considération lors de l'établissement des lignes directrices initiales de gestion des accidents graves qui permettront de répondre aux attentes énoncées dans le document G-306, *Programmes de gestion des accidents graves touchant les réacteurs nucléaires*.

La conception devrait inclure l'analyse réalisée pour évaluer la progression et les conséquences des accidents graves, y compris des évaluations sur les questions majeures, le cas échéant, comme la stratification du corium, l'interaction thermo-chimique entre le corium et le métal de la cuve, le transfert de chaleur entre le corium et la cuve ou le bouclier d'extrémité, la combustion de l'hydrogène, les vapocraquages provoqués par l'interaction entre le combustible en fusion et le liquide de refroidissement, et l'interaction entre le corium et le béton. Les résultats de l'analyse des accidents graves devraient être pris en compte lors de l'élaboration des lignes directrices initiales de gestion des accidents graves et la planification des mesures d'urgence.

La version 2 du document RD-337 indique que « *la conception doit inclure des points de connexion redondants en vue d'acheminer l'eau et l'électricité qui pourraient être nécessaires pour appuyer les mesures de gestion d'un accident grave* ». Les points de connexion redondants devraient utiliser des raccords standard et être facilement accessibles. Ils devraient également être séparés physiquement afin de réduire le plus possible les risques posés par les événements d'origine commune. La conception devrait faciliter l'utilisation d'équipements et de fournitures venant d'endroits situés sur le site et hors du site, tels que l'alimentation en carburant, les batteries, les pompes temporaires sur le site et hors site, les génératrices et les chargeurs de batteries.

Renseignements supplémentaires

D'autres renseignements sont disponibles dans les documents suivants :

- CCSN, G-225, *Planification d'urgence dans les installations nucléaires de catégorie I, les mines d'uranium et les usines de concentration d'uranium* [2001]
- CCSN, RD-327, *Sûreté en matière de criticité nucléaire*, section 16, Planification et intervention d'urgence en cas d'accident de criticité nucléaire [2010]

7.4 Événements initiateurs hypothétiques

Les événements initiateurs hypothétiques (EIH) sont identifiés en faisant appel au jugement d'ingénierie et à des évaluations déterministes et probabilistes. Il faudrait fournir une justification de l'étendue de l'utilisation des analyses déterministes de sûreté et des études probabilistes de sûreté afin de montrer que tous les événements prévisibles ont été pris en considération.

Il faudrait fournir des renseignements suffisants concernant les méthodes utilisées pour identifier les EIH, leur portée et leur classification. Si on s'est servi d'outils analytiques (p. ex. des diagrammes logiques maîtres, des analyses de l'opérabilité et des risques, une analyse des modes de défaillances et de leurs effets) pour les méthodes d'identification, l'information fournie devrait être suffisamment détaillée.

Une méthode systématique de classement des événements devrait prendre en considération tous les événements internes et externes, toutes les configurations en mode d'exploitation normale, les différentes conditions de la centrale et du site, et les défaillances survenant dans d'autres systèmes de la centrale (p. ex. dans le stockage du combustible irradié et dans les réservoirs de stockage pour les gaz radioactifs).

La conception devrait tenir compte de la défaillance des équipements ne faisant pas partie de la CN si cette défaillance a une incidence importante sur la sûreté nucléaire.

La portée des EIH devrait être établie de façon à correspondre aux attentes du document RD-310, *Analyses de la sûreté pour les centrales nucléaires*, et les événements devraient être classés selon leur fréquence prévue, ainsi que d'autres facteurs s'il y a lieu, conformément aux attentes du document RD-310.

L'analyse de sûreté des EIH identifiés devrait être réalisée en se fondant sur les directives présentées à la section 9.0.

7.4.1 Dangers internes

La conception tient compte des charges et des conditions environnementales particulières (température, pression, humidité, rayonnement) posées aux structures ou aux composants par les dangers internes.

La conception tient compte des effets des défaillances des canalisations, telles que les forces d'impact d'un jet, l'effet de fouet des tuyaux, les forces de réaction, les forces liées aux ondes de pression, l'accumulation de pression, l'humidité et le rayonnement sur les composants, les structures des bâtiments, les équipements électriques et les équipements d'IC.

Il faudrait prendre en considération les facteurs potentiels de déclenchement d'inondations suivants : les fuites et ruptures des composants sous pression, les inondations causées par l'eau provenant des bâtiments voisins, l'actionnement inopiné du système de lutte contre l'incendie, le remplissage excessif de réservoirs ou la défaillance de dispositifs d'isolation.

La conception prend en considération les missiles internes qui peuvent être produits par la défaillance de composants rotatifs (comme les turbines) ou par la défaillance de composants sous pression. Pour ces missiles potentiels considérés comme étant crédibles, la conception devrait inclure les éléments suivants :

- La réalisation d'une évaluation réaliste de la taille et de l'énergie du missile prévu, et de ses trajectoires potentielles
- l'identification des composants potentiellement touchés, liés aux systèmes nécessaires pour atteindre et maintenir l'état d'arrêt sûr
- l'évaluation de la perte de ces composants potentiellement touchés afin de déterminer s'il subsiste une redondance suffisante pour atteindre et maintenir un état d'arrêt sûr

La conception tient compte des charges créées par les dangers internes dans la catégorie des charges environnementales conformément à la section 7.15.

7.4.2 Dangers externes

La conception devrait tenir compte de toutes les caractéristiques de l'emplacement qui pourraient avoir une incidence sur la sûreté de la centrale, et devrait identifier les éléments suivants :

- l'évaluation des dangers spécifiques au site en lien avec des événements externes (d'origine naturelle ou humaine)
- les hypothèses ou les valeurs de conception en ce qui a trait à la probabilité de récurrence des événements externes
- la définition du dimensionnement pour les événements externes
- la collecte des données de référence sur le site pour la conception de la centrale (géotechniques, sismologiques, hydrologiques, hydrogéologiques et météorologiques)
- l'évaluation des incidences des questions relatives au site dont on doit tenir compte dans la demande en ce qui a trait aux mesures d'urgence et à la gestion des accidents
- les arrangements relatifs à la surveillance des paramètres du site tout au long de la vie de la centrale

Les dangers externes d'origine naturelle, autres que les tremblements de terre, peuvent être classés comme :

- des dangers susceptibles d'endommager des SSC importants pour la sûreté
- des dangers qui ont été évalués et éliminés

Les dangers externes d'origine naturelle qui ont été évalués et éliminés peuvent se fonder sur les critères suivants :

- un phénomène qui survient lentement ou s'accompagne d'une alerte adéquate en ce qui concerne le temps requis pour prendre des mesures de protection appropriées
- un phénomène qui, en tant que tel, n'a aucune incidence importante sur l'exploitation d'une centrale nucléaire et son dimensionnement
- un phénomène isolé présentant une probabilité d'occurrence très faible
- la centrale nucléaire est située à une distance suffisante ou à une altitude suffisamment élevée par rapport au phénomène postulé (p. ex. incendie, inondation)
- un phénomène qui est déjà inclus par la conception dans un autre phénomène. Par exemple, les marées de tempête et les seiches sont incluses dans les inondations, et l'écrasement accidentel d'un petit avion est inclus dans les charges liées aux tornades

Les dangers externes d'origine naturelle pris en considération dans la conception comprennent :

- les tremblements de terre

- les conditions météorologiques extrêmes liées à la température, la neige, la pluie verglaçante, la grêle, le gel, le gel souterrain et la sécheresse
- les inondations provoquées par les marées, les tsunamis, les seiches, les ondes de tempête, les trombes marines, la formation de digues et les ruptures de barrages, la fonte des neiges, les glissements de terrain dans les plans d'eau, les modifications apportées aux chenaux et les travaux réalisés dans ceux-ci
- les cyclones (p. ex. tornades, ouragans et typhons) et les vents directs
- les tempêtes de poussière abrasive et de sable
- les éclairs
- les volcans (l'emplacement est suffisamment éloigné des volcans)
- les phénomènes biologiques
- la collision de débris flottants (p. ex. glace, troncs) avec des structures accessibles liées à la sûreté, telles que des prises d'eau et des composants d'une source froide ultime (SFU)
- les orages géomagnétiques (éruptions solaires et impulsions électromagnétiques)
- les combinaisons de conditions météorologiques extrêmes dont on peut raisonnablement présumer qu'elles se produisent au même moment

Les dangers d'origine humaine pris en considération dans la conception comprennent :

- les accidents d'avion (aviation générale)
- les explosions (déflagrations et détonations) accompagnées ou non d'un incendie, avec ou sans missiles secondaires, provenant de sources se trouvant sur le site et hors site (mais à l'extérieur des bâtiments liés à la sûreté), comme les stocks de matières dangereuses ou de matières sous pression, les transformateurs, les cuves sous pression ou les équipements tournant à des vitesses élevées
- les rejets de gaz dangereux (asphyxiants ou toxiques) provenant d'entrepôts se trouvant sur le site et hors site
- les rejets de gaz et de liquides corrosifs provenant d'entrepôts se trouvant sur le site et hors site
- le rejet de matières radioactives provenant de sources se trouvant hors site
- les incendies produits par des sources se trouvant hors site (principalement pour la fumée et les gaz toxiques qu'ils sont susceptibles de produire)
- la collision de bateaux ou de débris flottants avec des structures accessibles liées à la sûreté, telles que des prises d'eau et des composants d'une SFU
- la collision de véhicules avec des SSC situés sur le site
- les interférences électromagnétiques produites à l'extérieur du site (centres de communication, antennes de téléphones portables, etc.) et sur le site (activation d'un appareil de commutation électrique à haute tension, câbles non blindés, etc.)
- toute combinaison des éléments précités, provoqués par un même événement initiateur (comme une explosion avec incendie et rejet de fumée et de gaz dangereux)

Les actes malveillants, y compris les écrasements d'avions, sont pris en considération séparément à la section 7.22.

Les dangers d'origine humaine classés comme des AD sont pris en considération en tant que charges dans la catégorie des charges environnementales anormales ou extrêmes, conformément à la section 7.15. Les dangers d'origine humaine moins fréquents sont considérés comme faisant partie des CAD.

Renseignements supplémentaires

D'autres renseignements sont disponibles dans les documents suivants :

- CCSN, RD-346, *Évaluation de l'emplacement des nouvelles centrales nucléaires*, 2008
- *Code national du bâtiment du Canada (CNBC)* [2010]
- American Nuclear Society (ANS) 2.3- 2011, *Estimating Tornado, Hurricane, and Extreme Straight Line Wind Characteristics at Nuclear Facility Sites* [2011]
- AIEA, NS-G-3.1, *Les événements externes d'origine humaine dans l'évaluation des sites de centrales nucléaires* [2006] (révision du guide de sûreté n° 50-SG-S5)

7.4.3 Combinaisons d'événements

Lorsque les résultats du jugement d'ingénierie, des analyses déterministes de sûreté et des études probabilistes de sûreté indiquent que des combinaisons d'événement pourraient dégénérer en IFP ou en accidents, de telles combinaisons d'événements devraient être considérées comme étant des AD ou devraient être intégrées aux CAD, selon leur probabilité d'occurrence.

7.5 Règles et limites de conception

Tel qu'indiqué dans la version 2 du document RD-337, « *l'autorité responsable de la conception doit préciser les règles de conception technique pour l'ensemble des SSC. Ces règles doivent être conformes aux pratiques d'ingénierie généralement reconnues* ». De tels SSC devraient comprendre les composants sous pression, l'équipement électrique, les équipements d'IC et les structures de génie civil.

Lors de la conception, il convient d'appliquer des méthodes permettant d'assurer une conception robuste et de respecter les méthodes d'ingénierie éprouvées afin de veiller à ce que les fonctions de sûreté fondamentales soient remplies dans l'ensemble des états de fonctionnement et des conditions d'accidents.

Les règles de conception technique de tous les SSC devraient être déterminées en se fondant sur leur importance sur le plan de la sûreté, qui sera déterminée à l'aide des critères énoncés à la section 7.1. Les règles de conception devraient comprendre, le cas échéant :

- les codes et les normes identifiés
- des marges de sûreté prudentes
- la fiabilité et la disponibilité
 - la sélection des matériaux
 - le critère de défaillance simple
 - la redondance
 - la diversité
 - l'indépendance
 - la conception à sûreté intégrée
- la qualification de l'équipement
 - la qualification environnementale
 - la qualification sismique

- les interférences électromagnétiques (IEM)
- les considérations relatives à l'exploitation
 - la testabilité
 - la possibilité d'effectuer des inspections
 - la facilité d'entretien
 - le vieillissement
- le système de gestion

Les caractéristiques de conception complémentaires devraient être conçues de manière à permettre d'effectuer efficacement les interventions validées dans l'analyse de sûreté, et ce avec un degré de confiance raisonnable. Les autres SSC validés pour les CAD devraient également répondre à cette attente.

Les règles de conception devraient inclure l'ensemble des normes et codes nationaux et internationaux pertinents. En cas de SSC dépourvus de normes ou de codes appropriés, il est possible d'appliquer une approche s'inspirant des normes et des codes existants pour des SSC similaires. En l'absence de tels codes et normes, il est possible d'appliquer les résultats de l'expérience, d'essais et d'analyses ou une combinaison de ceux-ci, et cette approche devrait être justifiée.

Un ensemble de limites de conception conforme aux principaux paramètres physiques de chaque SSC important pour la sûreté de la centrale nucléaire est spécifié pour tous les états de fonctionnement et pour les conditions d'accidents. Les limites de conception spécifiées sont conformes aux normes et codes nationaux et internationaux pertinents.

7.6 Fiabilité

Sur le plan de la fiabilité, la conception se fonde sur le respect des exigences réglementaires et des normes industrielles applicables. La conception devrait donner l'assurance que l'exploitation satisfera aux exigences de la norme d'application de la réglementation de la CCSN S-98, rév.1, *Programmes de fiabilité pour les centrales nucléaires*.

Les principes suivants sont appliqués pour les SSC importants pour la sûreté :

- la centrale est conçue, construite et exploitée de manière conforme aux hypothèses et à l'importance des risques liés à ces SSC
- ces SSC ne se dégradent pas dans des proportions inacceptables durant l'exploitation de la centrale
- la fréquence des états transitoires posant des difficultés aux SSC est minimisée
- ces SSC fonctionnent de façon fiable lorsqu'ils sont confrontés à des difficultés

La fiabilité des SSC supposée à l'étape de la conception doit être réaliste et réalisable.

Il est possible d'utiliser une analyse déterministe ou d'autres méthodes si l'EPS manque de modèles ou de données efficaces.

7.6.1 Défaillances d'origine commune

7.6.1.1 Séparation

La séparation physique peut être obtenue par des barrières, par la distance (tant horizontale que verticale) ou par une combinaison des deux. Par exemple, la conception peut prévoir des équipements redondants placés à des hauteurs différentes pour protéger contre les inondations et assurer l'étanchéité.

7.6.1.2 Diversité

La conception devrait prévoir une diversité adéquate des systèmes de sûreté, telle que :

- la diversité des conceptions
- la diversité des équipements
- la diversité fonctionnelle
- la diversité humaine

La conception des systèmes d'instrumentation et de contrôle (IC) devrait également prendre en considération :

- la diversité des signaux
- la diversité des logiciels

En ce qui concerne les systèmes d'IC importants pour la sûreté, on recommande d'utiliser un système de secours automatique diversifié. Il est possible de faire appel à un système de secours manuel diversifié. Sa justification devrait comporter une analyse de l'ingénierie des facteurs humains.

Les diverses stratégies suivantes devraient être prises en considération :

- différentes technologies
- différentes méthodes au sein de la même technologie
- différentes architectures au sein de la même technologie

Il faudrait effectuer une analyse de la diversité et de la défense en profondeur pour évaluer les vulnérabilités de la conception à l'égard des défaillances d'origine commune (DOC). Si l'analyse de la défense en profondeur révèle que certaines fonctions de sûreté pourraient être touchées par des DOC, la conception devrait prévoir un système de secours diversifié pour remplir les fonctions touchées par les DOC.

7.6.1.3 Indépendance

Les moyens permettant d'assurer l'indépendance comprennent la séparation physique, l'indépendance fonctionnelle et l'indépendance par rapport aux effets des erreurs de transmission des données. Il faudrait généralement appliquer une combinaison de ces méthodes afin d'obtenir un niveau d'indépendance acceptable.

L'indépendance fonctionnelle (telle que l'isolation électrique) devrait servir à réduire la probabilité d'interactions nuisibles entre les équipements et les composants de systèmes redondants ou de systèmes raccordés, résultant du fonctionnement normal ou de la défaillance d'un composant des systèmes.

Les SSC importants pour la sûreté devraient être indépendants des effets de l'événement auxquels ils doivent répondre. Par exemple, un événement ne devrait pas provoquer la défaillance ou la panne d'un système de sûreté ou d'une fonction de sûreté nécessaire pour atténuer les conséquences de cet événement.

Les parties redondantes d'un groupe de sûreté devraient être indépendantes les unes des autres afin de s'assurer que le groupe de sûreté puisse remplir sa fonction de sûreté durant (et après) tout événement qui exige cette fonction.

La défaillance fonctionnelle des dispositifs de soutien d'un système de sûreté ne devrait pas compromettre l'indépendance entre les parties redondantes d'un système de sûreté, ou entre un système de sûreté et un système rangé dans une classe de sûreté moins élevée.

Il faudrait évaluer le risque d'interactions entre ces SSC importants pour la sûreté susceptibles de devoir fonctionner simultanément, et il faudrait prévenir les effets de toute interaction nuisible.

Lors de l'analyse des risques d'interactions nuisibles entre les SSC importants pour la sûreté, il faudrait tenir dûment compte des interconnexions physiques et des effets possibles de l'exploitation, de la mauvaise utilisation ou du mauvais fonctionnement d'un système sur les conditions environnementales locales des autres systèmes essentiels. Ceci permettrait d'assurer que les changements apportés aux conditions environnementales n'aient aucune incidence sur la fiabilité des systèmes ou des composants et que ceux-ci puissent fonctionner comme prévu.

Renseignements supplémentaires

D'autres renseignements sont disponibles dans les documents suivants :

- U.S. NRC NUREG/CR-6303, *Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems* [1994]
- U.S. NRC NUREG/CR-7007, *Diversity Strategies for Nuclear Power Plant Instrumentation and Control Systems* [2010]
- U.S. NRC Branch Technical Position (BTP) 7-19, *Guidance for Evaluation of Diversity and Defense-in-Depth and in Digital Computer-Based Instrumentation and Control Systems* [2007]

7.6.2 Critère de défaillance simple

L'application du critère de défaillance simple (CDS) dans la conception devrait suivre une approche systématique appliquée à tous les groupes de sûreté. Cette approche devrait être vérifiée de manière adéquate à l'aide d'une méthode systématique telle que l'analyse des modes de défaillances et des effets.

Tel qu'indiqué dans la version 2 du document RD-337, « *tous les groupes de sûreté doivent pouvoir fonctionner en cas de défaillance simple* ». Les SSC faisant partie du groupe de sûreté devraient inclure à la fois les SSC primaires et les SSC de support.

La justification à l'appui d'une exception au CDS devrait prendre en considération les conséquences de la défaillance, la faisabilité des solutions de rechange, le surcroît de complexité et des considérations relatives à l'exploitation. L'effet intégré de toutes les exceptions ne devrait pas dégrader la sûreté de manière importante. Il faudrait particulièrement préserver la défense en profondeur.

En ce qui concerne les composants passifs exempts de CDS, les éléments qui suivent devraient être pris en considération pour faire preuve d'un niveau de rendement élevé :

- essais adéquats au cours de la phase de fabrication
- essais par échantillonnage des composants reçus du fabricant
- essais adéquats au cours des phases de construction et de mise en service
- essais nécessaires pour vérifier la fiabilité des composants qui ont été retirés du service durant la phase d'exploitation

Toute considération relative à une exception au CDS durant les activités d'essai et d'entretien devrait relever de l'une des catégories admissibles suivantes :

- la fonction de sûreté est assurée par deux systèmes redondants indépendants (p. ex. deux moyens de refroidissement redondants, parfaitement efficaces et indépendants)
- la durée prévue des activités d'essai et d'entretien est inférieure au laps de temps disponible avant que le composant ne doive remplir sa fonction à la suite d'un événement initiateur (p. ex. refroidissement de la piscine de stockage du combustible irradié)
- la perte de la fonction de sûreté est partielle et peu susceptible d'entraîner une augmentation importante des conséquences, même en cas de défaillance (p. ex. isolation d'une petite zone de confinement)
- la perte de redondance des systèmes a peu d'importance sur le plan de la sûreté (p. ex. filtration de l'air de la salle de commande)
- la perte de redondance des systèmes peut légèrement accroître la fréquence des EIH, mais n'a aucune influence sur la progression des accidents (p. ex. la détection de fuites)

Une demande d'exception durant les activités d'essai et d'entretien devrait également être justifiée par un argument de fiabilité satisfaisant, couvrant la durée d'indisponibilité admissible.

Les LCE devraient clairement énoncer la durée admissible des activités d'essai et d'entretien, ainsi que toute restriction opérationnelle complémentaire, telles que la suspension des autres activités d'essais et d'entretien sur un système de secours durant toute la durée de l'exception.

Renseignements supplémentaires

D'autres renseignements sont disponibles dans les documents suivants :

- AIEA, collection Rapports de sûreté n° 50-P-1, *Application of the Single Failure Criterion* [1990]
- Institute of Electrical and Electronics Engineers (IEEE), Standard 379-1988, *Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems* [1988]

7.6.3 Conception à sûreté intégrée

La connaissance des modes de défaillance des SSC est importante pour appliquer la notion de conception à sûreté intégrée aux SSC importants pour la sûreté. Il faudrait effectuer une analyse, telle que l'analyse des modes de défaillances et des effets, pour identifier les modes potentiels de défaillance des SSC importants pour la sûreté.

La défaillance des SSC importants pour la sûreté devrait pouvoir être détectée par des essais périodiques, ou être révélée par des alarmes ou d'autres indications fiables.

7.6.4 Indisponibilité d'équipement

Si la conception ne permet pas l'entretien et l'essai en fonction d'un équipement particulier, la conception devrait démontrer que l'équipement reste en mesure d'atteindre son objectif de fiabilité entre chaque indisponibilité.

Le temps consacré à chaque indisponibilité d'équipement et les interventions nécessaires à cet égard devraient être spécifiés dans les LCE.

7.6.5 Systèmes partagés

Cette section est traitée de manière suffisante par la version 2 du document RD-337, *Conception des nouvelles centrales nucléaires*. Il n'est donc pas nécessaire de fournir de l'orientation supplémentaire à ce sujet.

7.7 SSC sous pression

En ce qui concerne la conception des systèmes et composants sous pression, l'autorité responsable de la conception devrait veiller à la sélection adéquate des codes et des normes afin de donner l'assurance que les défaillances de la centrale sont réduites au minimum. Ceci est réalisé en utilisant des normes industrielles (telles que la norme CSA N285.0-08, *Exigences générales relatives aux systèmes et aux composants sous pression des centrales nucléaires CANDU* et la publication de l'American Society of Mechanical Engineers intitulée *ASME Boiler and Pressure Vessel Code*) pour satisfaire aux exigences relatives aux différentes classes de systèmes, de composants et de conduites sous pression, ainsi que de leurs dispositifs d'ancrage. Il est possible d'utiliser d'autres codes et normes si cela permet d'obtenir un niveau de sûreté équivalent ou supérieur. Dans ce cas, il faudrait fournir des justifications.

La conception devrait prévoir des dispositions adéquates pour limiter les contraintes et la déformation des SSC importants pour la sûreté durant et après les EIH. La liste des EIH devrait être complète et les charges créées par ceux-ci devraient être incorporées dans l'analyse de la conception. Les charges créées par ces EIH devraient être intégrées dans les analyses des contraintes requises par la conception.

Tel qu'indiqué dans la version 2 du document RD-337, « *la conception doit réduire au minimum la probabilité d'anomalies au niveau des enveloppes sous pression* ». Par exemple, l'enveloppe sous pression du système de refroidissement du réacteur devrait être conçue avec des marges suffisantes pour s'assurer que, dans toutes les configurations d'exploitation, les matériaux sélectionnés ne soient pas cassants et réduisent au maximum le risque de propagation rapide des fractures.

Les composants de l'enveloppe sous pression d'une centrale nucléaire contiennent presque toujours des fluides de procédé circulant à des températures et des pressions très élevées. La conception devrait tenir compte de l'emplacement des conduites à haute pression par rapport aux SSC importants pour la sûreté afin de limiter ou de réduire les problèmes liés à l'effet de fouet des tuyaux. Ceci comprend la prise en considération des éléments suivants :

- les composants des moyens d'arrêt d'urgence
- les pompes du circuit caloporteur primaire
- les collecteurs
- les conduites du système de refroidissement d'urgence du cœur (SRUC)
- les générateurs de vapeur
- les conduites de vapeur
- les turbines

Fuite avant rupture

La conception des systèmes répondant au principe de fuite avant rupture (FAR) permettra à l'autorité responsable de la conception d'optimiser les dispositifs de protection (comme les mesures de protection contre les jets ou le fouettement de conduites) et de modifier la conception des composants raccordés aux conduites, leurs dispositifs d'ancrage et leurs éléments internes.

La méthode liée au concept de FAR devrait comprendre les éléments suivants :

- Le concept de FAR ne devrait être appliqué qu'aux conduites sous haute pression appartenant aux classes 1 ou 2 du Code de l'American Society of Mechanical Engineers (ASME), ou aux conduites équivalentes. Il est possible d'appliquer ce concept à d'autres conduites sous haute pression en se fondant sur une évaluation de la conception proposée et sur les exigences relatives aux inspections en cours d'exploitation.
- Pour répondre au principe de FAR, les canalisations ne devraient présenter aucun mécanisme de dégradation active.
- Une évaluation des phénomènes tels que les coups de bélier, les dommages liés au fluage, la corrosion accélérée par l'écoulement et la fatigue devrait être réalisée pour couvrir toute la durée de vie des canalisations sous haute pression. Pour démontrer que les coups de bélier ne constituent pas un facteur important contribuant à la rupture des conduites, cette évaluation peut faire appel à la fréquence historique des événements liés aux coups de bélier dans certaines canalisations, accompagnée de l'examen des procédures et des conditions d'exploitation.
- Les méthodes de détection des fuites utilisées pour le caloporteur primaire devraient s'assurer que l'évaluation déterministe des conditions de propagation des fissures présente des marges de détection adéquates du défaut hypothétique traversant la paroi. Les marges devraient couvrir les incertitudes liées à l'identification des fuites provenant d'une canalisation.
- Les analyses des contraintes subies par les canalisations devant répondre au principe de FAR devraient être conformes aux exigences de la section III du code de l'ASME.
- L'évaluation des FAR devrait utiliser les charges de dimensionnement et, après la construction, être mise à jour pour utiliser la configuration de la canalisation « telle que construite » plutôt que la configuration prévue par la conception.
- La méthode devrait tenir compte des risques de dégradation (par érosion, corrosion et érosion/cavitation) en raison de conditions d'écoulement défavorables et des propriétés chimiques de l'eau.
- La méthode devrait tenir compte de la sensibilité des matériaux à la corrosion, des risques de contraintes résiduelles importantes et des conditions environnementales susceptibles d'entraîner une dégradation causée par la fissuration par corrosion sous contrainte.

En outre, les méthodes de détection des fuites utilisées pour le caloporteur primaire devraient être examinées pour s'assurer que l'évaluation déterministe des conditions de propagation des fissures présente des marges de détection adéquates du défaut hypothétique traversant la paroi.

Méthodes des éléments finis

L'autorité responsable de la conception utilise habituellement des méthodes des éléments finis pour montrer que tous les composants des enveloppes sous pression (aussi bien les cuves que les canalisations) répondent aux exigences relatives à l'intégrité structurale imposées par les codes et normes de conception applicables. En cas d'utilisation de méthodes des éléments finis pour les analyses de conception couvrant les composants appartenant à toutes les classes du code de l'ASME, il faudrait fournir les paramètres suivants :

- les hypothèses de modélisation et d'analyse des éléments finis sont vérifiées pour s'assurer qu'elles sont judicieuses et prudentes
- le maillage des éléments finis est correctement défini (forme et rapport de longueur des éléments) afin de rendre compte des discontinuités géométriques structurales;
- les charges et les conditions limites sont correctes et convenablement appliquées dans les modèles des éléments finis
- les combinaisons de charges et les facteurs d'échelle appliqués aux cas de charges unitaires sont conformes aux spécifications de la conception ou des charges

- les résultats de la linéarisation des contraintes, obtenus à partir des combinaisons de charges, sont comparés aux limites admissibles du code de l'ASME

7.8 Qualification environnementale de l'équipement

Le concepteur devrait fournir des directives détaillées concernant le programme de qualification environnementale (QE) de l'équipement destiné à qualifier l'équipement lié à la sûreté qui est associé aux systèmes essentiels à l'exécution des fonctions de sûreté validées définies dans la version 2 du document RD-337. Le programme de QE devrait traiter des critères et des méthodes de qualification utilisés et de toutes les conditions environnementales prévues sur lesquelles se fonde la qualification de l'équipement (mécanique, électrique, instrumentation et contrôle, et certains dispositifs de surveillance post-accidentelle).

Le concepteur identifie les normes et codes liés à la QE (p. ex. CSA, IEEE, ASME). On donnera la préférence aux dernières éditions des normes applicables servant à la qualification de l'équipement. Tout écart devrait être justifié.

Il faudrait à tout le moins fournir les éléments du programme de QE de base décrits ci-dessous.

7.8.1 Identification de l'équipement devant être qualifié pour des environnements hostiles

La conception devrait identifier :

- les systèmes et équipements devant remplir des fonctions de sûreté dans un environnement hostile, y compris leurs fonctions de sûreté et les AD applicables
- les équipements non liés à la sûreté dont la défaillance due à un environnement post-accidentel hostile pourrait empêcher un équipement lié à la sûreté d'accomplir ses fonctions de sûreté
- l'équipement de surveillance des accidents

7.8.2 Identification des conditions opérationnelles de l'équipement

Les conditions opérationnelles devraient être identifiées pour déterminer les méthodes de qualification requises dans la mesure où elles s'appliquent aux différents types de qualification (p. ex. environnements hostiles, environnements normaux, environnements uniquement hostiles sur le plan radiologique).

La conception devrait prévoir :

- une distinction entre les environnements normaux et les environnements hostiles (p. ex. certains critères permettant de définir si l'environnement de la centrale est normal ou hostile)
- une liste d'AD hostiles limitatifs pour la qualification de l'équipement
- les conditions environnementales (p. ex. la température, la pression, le rayonnement, l'humidité, la vapeur, les produits chimiques, l'immersion) de chaque AD applicable auquel l'équipement est exposé à différents endroits de la centrale
- les profils de température, de pression et de rayonnement destinés à la qualification pour les environnements hostiles
- le temps de mission habituel de l'équipement en cas d'AD
- les conditions environnementales normales (p. ex. la température, la pression, l'humidité, le rayonnement) pour tous les états de fonctionnement, y compris la durée supposée des IFP auxquels l'équipement est exposé à différents endroits de la centrale

7.8.3 Méthodes de qualification

La conception devrait décrire les méthodes utilisées pour démontrer le rendement des équipements liés à la sûreté soumis à un ensemble de conditions environnementales dans les divers états de

fonctionnement ou en cas d'AD. Les méthodes devraient déterminer si l'équipement doit être qualifié pour des environnements hostiles ou des environnements normaux.

En ce qui concerne la qualification pour les environnements hostiles, la conception devrait comprendre les éléments suivants :

- pour l'équipement et les composants situés dans un environnement d'AD hostile, les essais de type (en particulier pour l'équipement électrique) constituent la méthode privilégiée par rapport aux autres méthodes de qualification. Lorsque les essais de types ne sont pas réalisables, on peut le justifier en utilisant une analyse ou l'expérience opérationnelle (ou une combinaison des deux)
- l'équipement devrait être examiné en ce qui concerne la conception, le fonctionnement, les matériaux et l'environnement pour identifier les mécanismes de vieillissement importants causés par les conditions opérationnelles et environnementales survenant en mode d'exploitation normale. En cas d'identification d'un mécanisme de vieillissement important, ce vieillissement devrait être pris en compte dans la qualification de l'équipement
- la qualification devrait systématiquement tenir compte de la séquence des effets des conditions au cours de la durée de vie, y compris les effets séquentiels, simultanés et synergiques, ainsi que les méthodes utilisées pour accélérer les effets de la dégradation liée au rayonnement
- des marges appropriées, comme celles indiquées dans les normes liées à la QE, devraient être appliquées aux conditions environnementales spécifiées
- pour certains équipements (p. ex. les équipements d'instrumentation et de contrôle numériques et les nouveaux appareils électroniques analogiques perfectionnés), il faudrait tenir compte de conditions environnementales supplémentaires, telles que les interférences électromagnétiques (IEM), les interférences aux fréquences radioélectriques (RFI) et les surtensions

En ce qui concerne la qualification pour les environnements normaux, la conception devrait comprendre les éléments suivants :

- l'équipement situé dans un environnement normal peut être considéré comme qualifié pour autant que les conditions environnementales soient précisées dans une spécification de la conception et que le fabricant fournisse un certificat indiquant que l'équipement satisfait à la spécification.

7.8.4 Évaluation de l'équipement et de l'instrumentation en cas de CAD

Une démonstration de l'opérabilité de l'équipement et de l'instrumentation devraient comprendre les éléments suivants :

- les fonctions qui, en cas d'accident, doivent être exécutées dans un certain délai pour atteindre un état d'arrêt sûr pour les CAD
- le délai d'exécution de chaque fonction à la suite d'un d'accident
- le type et l'emplacement de l'équipement utilisé pour exécuter les fonctions nécessaires dans les délais prescrits
- l'environnement hostile limitatif des CAD au sein de chaque période
- une assurance raisonnable que l'équipement restera prêt à exécuter ses fonctions à la suite d'un accident dans l'environnement des CAD

7.8.5 Barrières de protection

La conception devrait tenir compte des barrières de protection, le cas échéant. Lorsque des barrières de protection sont conçues pour isoler l'équipement des conditions environnementales hostiles éventuelles, les barrières elles-mêmes devraient être prises en compte dans un programme de qualification. Exemples de barrières de protection acceptables :

- les salles et les enceintes à l'épreuve de la vapeur
- les portes de protection contre la vapeur
- les salles à l'épreuve de l'eau (en cas d'inondation)

Renseignements supplémentaires

D'autres renseignements sont disponibles dans les documents suivants :

- Norme CSA N293-F07, *Protection contre l'incendie dans les centrales nucléaires CANDU* [2009]
- IEEE-627-2010, *IEEE Standard for Qualification of Equipment Used in Nuclear Facilities* [2010]
- IEEE-323-2003, *IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations* [2003]
- ASME QME-1-2002, *Qualification of Active Mechanical Equipment Used in Nuclear Power Plants* [2002]
- Commission électrotechnique internationale (CEI), CEI 60780, deuxième édition, *Centrales nucléaires – Équipements électriques de sûreté – Qualification* [1998]
- AIEA, collection Rapports de sûreté n° 3, *Equipment qualification in operational nuclear power plants: upgrading, preserving and reviewing* [1998]
- Electric Power Research Institute (EPRI) technical report, *Nuclear Power Plant Equipment Qualification Reference Manual*, Revision 1 [2010]

7.9 Instrumentation et contrôle

7.9.1 Généralités

Tel qu'indiqué dans la version 2 du document RD-337, la conception doit prévoir « *l'instrumentation servant à mesurer les variables pouvant influencer sur le procédé de fission, l'intégrité du cœur du réacteur, les systèmes de refroidissement du réacteur et l'enceinte de confinement, ainsi que l'instrumentation servant à obtenir d'autres données nécessaires sur la centrale pour en assurer le fonctionnement fiable et sécuritaire* ».

Une attention particulière devrait être accordée aux conditions relatives aux instruments de démarrage.

La surveillance ne devrait pas se limiter aux variables de processus des systèmes de sûreté et des systèmes liés à la sûreté. Elle devrait s'étendre à la surveillance des rayonnements, de l'hydrogène, des aléas sismiques, des parties lâches, des vibrations et de la fatigue.

Les mesures devraient comprendre les variables continues et discontinues de la centrale. La détection et les essais devraient également tenir compte des défaillances, de la dégradation, des conditions dangereuses, des écarts par rapport aux limites spécifiées, des erreurs des opérateurs et des autodiagnostic. Une correction des fonctions ou des données invalides, non authentiques ou corrompues devrait être appliquée pour maintenir la fiabilité des systèmes.

Tel qu'indiqué dans la version 2 du document RD-337, « *la conception doit être telle que les systèmes de sûreté et tout autre système de support requis peuvent fonctionner de façon fiable et autonome, en mode automatique ou manuel, au moment voulu* ». La commutation entre le mode automatique et le mode manuel devrait se faire sans à-coups.

Une fois que les systèmes de sûreté ont été enclenchés, la remise à zéro des fonctions des systèmes de sûreté devrait nécessiter une intervention distincte de l'opérateur pour chaque fonction au niveau

des systèmes. Une intervention délibérée de l'opérateur devrait être exigée pour ramener les systèmes de sûreté en position normale. Toutefois, ceci ne devrait pas empêcher l'utilisation de dispositifs de protection des équipements essentiels (comme la protection des composants électriques ou mécaniques) ou la possibilité d'interventions délibérées de l'opérateur (telles que le déclenchement et l'isolation du matériel de commutation). Le scellement du dispositif de déclenchement des systèmes de sûreté est généralement requis au niveau des systèmes ou des sous-systèmes, mais n'est pas exigé au niveau de chaque canal.

La conception devrait prévoir la capacité d'enregistrer, de conserver et d'afficher des renseignements historiques lorsque de tels affichages permettent au personnel de la centrale d'identifier les profils et les tendances, de comprendre l'état passé et actuel du système, de réaliser des analyses post-accidentelles ou de prédire les progressions futures.

La conception devrait tenir compte de la redondance, de l'indépendance, des défaillances d'origine commune, des interactions avec d'autres systèmes et de la validation des signaux de manière à atteindre les objectifs de fiabilité.

Lorsqu'un système de sûreté a été mis hors service pour procéder à des essais ou à son entretien, il faudrait fournir des indications claires concernant la durée des activités d'essai et d'entretien. En cas de contournement d'un système de sûreté, cette condition devrait également être clairement annoncée.

Si l'utilisation d'un système aux fins d'essais ou d'entretien est susceptible de nuire au fonctionnement d'un système d'instrumentation et de contrôle (IC), les interfaces devraient être soumises à un verrouillage du matériel pour s'assurer que l'interaction avec le système d'essai ou d'entretien soit impossible sans intervention manuelle délibérée.

Si l'équipement d'essai fait partie du système et reste raccordé quand il n'est pas utilisé pour les essais, la classe de sûreté de cet équipement devrait être identique à celle du système de sûreté.

Les systèmes de verrouillage importants pour la sûreté devraient soit réduire la probabilité d'occurrence de certains événements, soit maintenir la disponibilité des systèmes de sûreté en cas d'accident. Les systèmes de verrouillage devraient être signalés et justifiés.

Il faudrait prévoir des moyens de déclenchement et de contrôle automatiques de toutes les mesures de sûreté, à l'exception de celles pour lesquelles seule une intervention manuelle a été justifiée. Voici quelques exemples de situations où seule une intervention manuelle pourrait être justifiée :

- le déclenchement de tâches liées à la sûreté après l'exécution de séquences automatiques
- le déclenchement de mesures de sûreté qui ne sont pas nécessaires tant qu'un laps de temps considérable ne s'est pas écoulé après l'EIH
- les mesures de contrôle permettant de mettre la centrale dans un état sûr à long terme, à la suite d'un accident

Les opérateurs de la centrale devraient pouvoir consulter la valeur de chaque paramètre d'entrée utilisé pour le fonctionnement des systèmes de sûreté, le statut de chaque fonction de déclenchement et d'actionnement dans chaque division, et le statut concernant le lancement de chaque système.

Renseignements supplémentaires

D'autres renseignements sont disponibles dans les documents suivants :

- CEI 61513, *Centrales nucléaires de puissance – Instrumentation et contrôle-commande importants pour la sûreté – Exigences générales pour les systèmes* [2011]
- CEI 60880, *Centrales nucléaires de puissance – Instrumentation et contrôle-commande importants pour la sûreté – Aspects logiciels des systèmes programmés réalisant des fonctions de catégorie A* [2006]
- CEI 60987, *Centrales nucléaires de puissance – Instrumentation et contrôle-commande importants pour la sûreté – Exigences applicables à la conception du matériel des systèmes informatisés* [2007]
- CEI 60671, *Centrales nucléaires de puissance – Instrumentation et contrôle-commande importants pour la sûreté – Essais de surveillance* [2007]
- CEI 62385, *Centrales nucléaires de puissance – Instrumentation et contrôle-commande importants pour la sûreté – Méthodes d'évaluation des performances des chaînes d'instrumentation des systèmes de sûreté* [2007]
- IEEE 603, *IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations* [2009]
- IEEE 7-4.3.2, *IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations* [2010]
- CSA N290.6-09, *Exigences relatives à la surveillance et à l'affichage des fonctions de sûreté d'une centrale nucléaire au moment d'un accident* [2009]
- CSA N290.14-07, *Qualification of pre-developed software for use in safety related instrumentation and control applications in nuclear power plants* [2007]

7.9.2 Utilisation de systèmes ou d'équipement informatisés

Les normes et codes utilisés pour les systèmes ou les équipements informatisés sont identifiés avant la conception. Le cycle chronologique d'élaboration des systèmes d'instrumentation et de contrôle, qui applique les exigences figurant dans les normes et les codes, devrait être coordonné avec le cycle chronologique d'ingénierie des facteurs humains (IFH) et le cycle chronologique de la cybersécurité étant donné qu'ils ont une grande influence sur l'élaboration des systèmes d'IC.

Les activités de vérification et de validation devraient être identifiées et utiliser une approche descendante. La relation entre la conception et les activités de vérification et de validation devrait être indiquée et les résultats des activités de vérification et de validation devraient être documentés. La relation entre le cycle chronologique et les activités de vérification et de validation devrait être signalée.

Le logiciel livré par un tiers fournisseur devrait avoir le même niveau de qualification que le logiciel écrit spécialement pour l'application. La qualification des logiciels devrait être vérifiée à l'aide des normes nationales et internationales correspondant aux activités de qualification des logiciels préconçus.

Le processus de développement des logiciels devrait comprendre la prise en considération de la cohérence, de la modularité, de la structuration, de la traçabilité, de l'intelligibilité et des possibilités de vérification :

- la cohérence devrait comprendre des notations, une terminologie, des commentaires, des symboles et des techniques de mise en œuvre uniformes
- la modularité devrait veiller à ce que les changements apportés à un composant aient des répercussions minimales sur les autres composants

- la structuration signifie que la conception devrait se faire de manière systématique et ordonnée (p. ex. une conception descendante) en réduisant le plus possible les liens entre les modules et les sous-systèmes
- la traçabilité devrait fournir un fil conducteur entre les documents précédents et les documents suivants; elle se rapporte à la possibilité de retracer l'historique des décisions prises sur le plan de la conception et la justification des modifications
- l'intelligibilité signifie qu'une tierce partie devrait clairement comprendre les processus de développement et les résultats
- les possibilités de vérification devraient mentionner dans quelle mesure les processus de développement et les résultats ont été créés pour faciliter la vérification à l'aide de méthodes statiques et en procédant à des essais

La documentation relative au développement du logiciel devrait fournir toutes les informations, tout au long du cycle de développement du logiciel.

7.9.3 Instrumentation servant à la surveillance des accidents

Des instruments sont prévus afin de s'assurer que les renseignements essentiels sont disponibles pour évaluer les conditions de la centrale, surveiller le rendement des systèmes de sûreté, prendre des décisions liées aux réponses de la centrale aux événements anormaux et prédire les rejets de matières radioactives. Des instruments sont également prévus pour enregistrer les variables et les paramètres essentiels de la centrale, y compris :

- la température à divers endroits
- la pression dans l'enceinte de confinement et dans le système de refroidissement du réacteur
- le niveau de radioactivité à divers endroits
- le niveau d'eau de la cuve du réacteur pour les réacteurs à eau ordinaire (REO) ou le niveau du modérateur pour les centrales nucléaires CANDU
- le niveau d'eau dans l'enceinte de confinement
- la concentration d'hydrogène

La conception devrait fournir le dimensionnement, les critères de conception et les critères d'affichage des paramètres de surveillance des accidents.

L'instrumentation servant à la surveillance des accidents devrait respecter les critères de rendement tels que la plage de mesure, la précision, le temps de réponse, le temps de fonctionnement et les objectifs de fiabilité. Une analyse appropriée de la conception devrait être réalisée pour confirmer le respect des critères de rendement.

L'instrumentation servant à la surveillance des accidents répond au critère de défaillance simple (version 2 du document RD-337, section 7.6.2). La conception devrait tenir compte des défaillances d'origine commune au niveau des variables.

Il faudrait dans la mesure du praticable utiliser des variables et des affichages identiques pour la surveillance de l'exploitation normale et la surveillance des accidents.

La conception devrait :

- intégrer des possibilités de mise à l'essai afin de vérifier périodiquement les exigences en matière d'exploitabilité
- faciliter l'entretien, les réparations et l'étalonnage
- permettre un contrôle d'accès administratif en vue de l'étalonnage et de la mise à l'essai des chaînes d'instrumentation

Il faut démontrer que l'instrumentation servant à la surveillance des accidents est qualifiée pour remplir ses fonctions pendant toute la durée requise en cas d'accident.

Renseignements supplémentaires :

D'autres renseignements sont disponibles dans les documents suivants :

- IEEE 497-2010, *IEEE Standard Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating Stations* [2010]
- CSA N290.6-09, *Exigences relatives à la surveillance et à l'affichage des fonctions de sûreté d'une centrale nucléaire au moment d'un accident* [2009]

7.10 Systèmes de support en matière de sûreté

Le dimensionnement des systèmes d'air comprimé desservant un élément important pour la sûreté de la centrale nucléaire devrait préciser la qualité, le débit et le degré de propreté de l'air à fournir.

Il faudrait prévoir des systèmes de climatisation de l'air, de chauffage de l'air, de refroidissement d'air et de ventilation (s'il y a lieu) dans les locaux auxiliaires ou dans d'autres zones de la centrale nucléaire de manière à maintenir les conditions environnementales requises par les systèmes et les composants importants pour la sûreté, pour tous les états de la centrale.

Tel qu'indiqué dans la version 2 du document RD-337, « *les systèmes de support d'urgence doivent appuyer la continuité des fonctions de sûreté fondamentales jusqu'à ce que le service à long terme (normal ou de relève) soit rétabli,*

- *sans que l'opérateur ait besoin d'intervenir pour connecter les services temporaires sur le site pendant au moins 8 heures*
- *sans qu'il soit nécessaire d'utiliser les services et le soutien hors site pendant au moins 72 heures ».*

L'équipement préinstallé peut être appelé à intervenir au bout de 30 minutes lorsque les mesures à prendre se limitent à la salle de commande, ou après une heure si les mesures doivent être prises sur le terrain. Ces mesures devraient se limiter à la commande de vannes, au démarrage de pompes, etc. La section 8.10.4 fournit des indications concernant la justification de telles mesures.

Si l'équipement n'est pas préinstallé mais qu'il est entreposé sur le site, il peut normalement être appelé à intervenir au bout de 8 heures. Toutefois, cela doit être justifié en se fondant sur une évaluation des mesures requises et de la présence de procédures et de formations à l'appui des ces mesures. Certaines mesures complexes peuvent éventuellement nécessiter des délais plus longs. L'équipement ou les fournitures entreposés à l'extérieur du site ou les équipes de soutien se trouvant hors du site ne devraient normalement pas intervenir avant 72 heures. Encore une fois, la valeur utilisée devrait être justifiée et peut être plus longue.

De l'orientation concernant les points de connexion redondants pour les services temporaires est décrite à la section 7.3.4.

7.11 État d'arrêt garanti

Un état d'arrêt garanti (EAG) est un état pour lequel le réacteur demeurera dans un état sous-critique stable, indépendant des variations de la réactivité découlant d'un changement de la configuration du cœur, des propriétés du cœur ou de la défaillance d'un système fonctionnel..

La conception devrait décrire les EAG que l'on prévoit d'utiliser tout au long du cycle de vie de l'installation, y compris les mesures relatives à l'établissement d'un état d'arrêt garanti, à la levée de l'état d'arrêt garanti et au redémarrage, ainsi que les essais à effectuer.

7.12 Sûreté contre les incendies

7.12.1 Dispositions générales

Une protection efficace contre les incendies est obtenue par :

- des dispositifs de protection contre l'incendie tels que des programmes et des procédures, les mesures liées à la prévention et à la détection des incendies, aux alarmes d'incendie, aux communications d'urgence, à la gestion des produits accessoires, à l'extinction et au confinement des incendies, à la construction en matériaux incombustibles, et à la qualification sismique et environnementale des équipements de protection contre l'incendie
- l'utilisation de barrières pour séparer les SSC redondants importants pour la sûreté

La conception devrait aborder la protection-incendie en démontrant qu'une méthode de défense en profondeur a été mise en œuvre. Les documents justificatifs devraient comprendre un rapport de conception détaillé, une vérification de la conformité aux codes, une évaluation des risques d'incendie, une analyse des arrêts sûrs en cas d'incendie et un programme de protection contre l'incendie.

Une tierce partie indépendante devrait réaliser un examen de la conception pour évaluer si celle-ci est conforme aux codes et aux normes de prévention des incendies applicables en ce qui concerne la protection contre les incendies et les explosions. L'examen devrait formellement déclarer que la conception est conforme aux codes et normes identifiés, qu'elle est conforme aux règles de l'art et qu'elle répond aux objectifs de protection contre l'incendie.

La conception devrait respecter les exigences des normes et codes suivants :

- Commission des codes du bâtiment et de prévention des incendies, *Code national du bâtiment du Canada* (CNBC) [2010]
- Norme CSA N293-F07, *Protection contre l'incendie dans les centrales nucléaires CANDU* [2007]
- Conseil national de recherches Canada, *Code national de prévention des incendies – Canada* (CNPI) [2010]

Bien que la norme CSA N293-F07 soit considérée comme acceptable pour fournir des critères de conception neutres sur le plan technologique, elle n'aborde pas entièrement certains aspects de la protection contre l'incendie, tels que :

- les interventions manuelles effectuées par l'opérateur
- l'analyse du circuit d'arrêts sûrs en cas d'incendie
- les manœuvres intempestives multiples

Des orientations concernant les aspects de protection contre l'incendie mentionnés ci-dessus sont données dans les documents suivants :

- U.S. NRC NUREG 1852, *Demonstrating the Feasibility and Reliability of Operator Manual Actions in Response to Fire* [2007]

- Nuclear Energy Institute NEI 00-01, *Guidance for Post-Fire Safe Shutdown Circuit Analysis* [2005]
- U.S. NRC SECY-08-0093, *Resolution of Issues Related to Fire-Induced Circuit Failures* [2008]

Renseignements supplémentaires

D'autres renseignements sont disponibles dans les documents suivants :

- NEI 04-02, Revision 1, *Guidance for Implementing a Risk-Informed, Performance-Based Fire Protection Program under 10 CFR 50.48(c)* [2005]
- National Fire Protection Association (NFPA) NFPA 804, *Standard for Fire Protection for Advanced Light Water Reactor Electric Generating Plants* [2010]
- NFPA 805, *Performance-Based Standard for Fire Protection for Light Water Reactor Electric Generating Plants* [2010]
- NFPA, *Fire Protection Handbook* [2008]
- Society of Fire Protection Engineers, *SFPE Handbook of Fire Protection Engineering* [2008]
- AIEA, NS-G-1.7, *Protection Against Internal Fires and Explosions in the Design of Nuclear Power Plants* [2004]
- AIEA, NS-G-2.1, *Protection contre l'incendie des centrales nucléaires en exploitation* [2000]
- AIEA, collection *Rapports de sûreté* n° 8, *Safe Preparation of Fire Hazard Analysis for Nuclear Power Plants* [1998]
- U.S. NRC NUREG/CR-6850, EPRI 1011989 *Fire Probabilistic Risk Assessment Methods Enhancements* [2010]
- U.S. NRC NUREG-0800, *Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR edition - Fire Protection Program*, section 9.5.1.1 [2009]
- U.S. NRC Regulatory Guide 1.189, *Fire Protection for Operating Nuclear Power Plants* [2001]

7.12.2 Sûreté des personnes

Le *Code national du bâtiment du Canada* (CNBC) est un code modèle national axé sur les objectifs. Les dispositions du CNBC sont considérées comme les mesures minimales acceptables pour répondre aux objectifs liés à la sûreté, à la santé, à la protection structurale et à la protection des bâtiments contre l'incendie. En soi, des mesures de protection contre l'incendie supplémentaires peuvent s'avérer nécessaires pour répondre aux exigences réglementaires précisées dans la version 2 du document RD-337. Les mesures supplémentaires de protection contre l'incendie sont habituellement évaluées et documentées dans le rapport de vérification de la conformité au code et l'évaluation des risques d'incendie, comme l'exige la norme CSA N293-F07, *Protection contre l'incendie dans les centrales nucléaires CANDU*.

7.12.3 Protection environnementale et sûreté nucléaire

Tel qu'indiqué à la section 7.12.2, le *Code national du bâtiment du Canada* et le *Code national de prévention des incendies – Canada* (CNPI) traitent des mesures minimales de protection contre l'incendie qui doivent être incorporées au moment de la conception et de la construction des bâtiments. D'autres mesures de protection contre l'incendie peuvent s'avérer nécessaires pour répondre aux exigences réglementaires précisées à la section 7.12.3 de la version 2 du document RD-337. Les mesures supplémentaires de protection contre l'incendie sont habituellement évaluées et documentées dans le rapport de vérification de la conformité au code, dans l'évaluation des risques d'incendie et dans l'analyse des arrêts sûrs en cas d'incendie, comme l'exige la norme CSA N293-F07.

7.13 Qualification sismique

7.13.1 Conception et classification sismiques

La conception sismique d'une centrale nucléaire devrait tenir compte des points suivants :

- les objectifs de sûreté techniques et les catégories de charges correspondantes
- le mouvement dû à un apport sismique
- la classification sismique
- les critères d'aménagement structural
- l'analyse sismique et la conception des systèmes, sous-systèmes et équipements structuraux
- les essais sismiques et l'instrumentation

Les catégories de charge nominale et hors dimensionnement sont définies pour démontrer le rendement structural dans les états de fonctionnement et les conditions d'accident. Les charges sismiques ne font pas partie de la catégorie des charges normales correspondant à une exploitation normale. La charge sismique nominale du site, selon la série de normes CSA N289 sur la conception et la qualification sismiques, est définie dans la catégorie des charges sévères correspondant à un IFP. Le séisme de référence est défini comme faisant partie de la catégorie de charge anormale/extrême correspondant à un accident de dimensionnement (AD). Les charges sismiques hors dimensionnement doivent être prises en compte dans le cadre des CAD.

Le mouvement dû à un apport sismique, dérivé du séisme de référence, devrait être basé sur la sismicité et les conditions géologiques du site et être exprimé d'une manière applicable à la qualification des SSC. Le spectre de réponse au séisme de référence devrait être défini en tenant compte d'un facteur de conception appliqué à un spectre de risque uniforme moyen (avec une probabilité d'occurrence de 10^{-4} /an selon la définition donnée dans la norme ASCE 43-05, *Seismic Design Criteria for Structures, Systems and Components in Nuclear Facilities*). Un mouvement minimal dû à un apport sismique, conforme aux normes nationales ou internationales, devrait être pris en compte dans la phase de conception pour le séisme de référence. Le mouvement minimal dû à un apport sismique devrait prendre en compte les fréquences d'intérêt pour les SSC.

Les critères d'aménagement structural, y compris la séparation structurale, devraient suivre les meilleures pratiques d'ingénierie et les enseignements tirés des séismes passés.

La modélisation des interactions sol-structure (ISS) devrait être fondée sur une étude géotechnique et tenir compte du caractère aléatoire des propriétés des matériaux du sol et des incertitudes inhérentes incorporées dans les modèles de constitution des sols utilisés dans l'analyse. Afin de tenir compte des incertitudes dans les propriétés des sols, on devrait employer une plage qui comprend au moins trois valeurs (limite supérieure, meilleure estimation et limite inférieure) dans l'analyse selon la norme CSA N289.3-10, *Design procedures for seismic qualification of nuclear power plants*, clause 5.2.2.

Dans l'analyse des ISS, on devrait prendre en compte tous les effets dus à l'interaction cinématique (effet du mouvement sismique du sol sur une structure de masse nulle) et à l'interaction inertielle (forces d'inertie développées dans la structure due au mouvement sismique du sol). Le degré de détail et de sophistication des modèles sol-structure devrait correspondre aux fins des analyses. La plage de fréquence d'intérêt détermine les aspects du modèle structure et les paramètres du modèle des ISS.

La plage des fréquences d'intérêt devrait être basée sur la combinaison de divers facteurs : la plage des fréquences de l'apport sismique, les propriétés du sol, la plage des fréquences de réponse du

bâtiment (y compris la réponse des sous-systèmes dans le modèle de la structure ou du bâtiment principal) et la plage des fréquences du paramètre de réponse d'intérêt. Des modèles raffinés d'éléments finis et une rigueur analytique accrue sont requis pour répercuter les fréquences élevées tout au long des modèles analytiques.

Des rapports d'amortissement s'appliquant aux systèmes et sous-systèmes structuraux devraient être pris en compte conformément à la norme ASCE 43-05. Pour générer les spectres de réponse dans la structure qui seront utilisés comme intrants pour les composants et les systèmes montés sur les structures, l'amortissement du niveau de réponse 1 est plus approprié, sauf si la réponse de la structure est généralement supérieure au facteur de demande par rapport à la capacité selon la norme ASCE 43-05.

La conception sismique des systèmes structuraux devrait être réalisée selon la catégorie de conception sismique (CCS – en anglais SDC pour *seismic design category*) 1 à 5 de la norme ASCE 43-05.

Les systèmes structuraux des niveaux CCS 1 et 2 devraient être conformes au *Code national du bâtiment du Canada*, Division B, partie 4. Selon le Code, la CCS 1 devrait être considérée comme le niveau normal et la CCS 2 comme le niveau de protection civile.

Toutes les structures importantes pour la sûreté sont classées au niveau CCS 5. Cependant, le concepteur peut classer certaines structures aux niveaux CCS 3, 4 et 5, à condition de justifier adéquatement ce classement. Les lignes directrices pour les systèmes structuraux des niveaux CCS 3, 4 et 5 (si on emploie les niveaux CCS 3 et 4) sont présentées comme suit :

- pour les enceintes de confinement en béton, la conception devrait être fondée sur la norme ASCE 43-05 de l'American Society of Civil Engineers (CCS 5, état limite D) et la norme CSA N287.3-93, *Design Requirements for Concrete Containment Structures for CANDU Nuclear Power Plants*
- pour les enceintes de confinement en acier, la conception devrait être fondée sur la norme ASCE 43-05 (SDC 5), 2010 *ASME Boiler and Pressure Vessel Code*, Section III: Rules for Construction of Nuclear Power Plant Components, Division 1, Subsection NE: Class MC Components et sur le document U.S. NRC Regulatory Guide 1.57, *Design Limits and Loading Combinations for Metal Primary Reactor Containment System Components*
- pour les structures en béton et en acier liées à la sûreté, la conception devrait être fondée sur la norme ASCE 43-05 (CCS 5, état limite D) et CSA N291-F08, *Exigences relatives aux enceintes reliées à la sûreté des centrales nucléaires CANDU*

Pour toutes les catégories de conception de sûreté dans une centrale nucléaire, les exigences de ductilité devraient être conformes aux normes CSA-A23.3-F04 (C2010), *Calcul des ouvrages en béton*, pour les structures en béton et CSA S16-F09, *Règles de calcul des charpentes en acier*, pour les structures en acier en supposant que les structures sont ductiles ou de type D. Ces exigences de ductilité devraient fournir des marges de sûreté pour les séismes hors dimensionnement.

L'analyse des sous-systèmes devrait suivre les directives présentées pour les systèmes structuraux avec les critères suivants spécifiques aux supports des sous-systèmes :

- spectres de réponse dans la structure
- historiques des réponses dans le temps dans la structure

Les méthodes de définition des spectres de réponse dans la structure ou des historiques des réponses dans le temps dans la structure, ainsi que l'application de cet apport sismique à des

sous-systèmes et composants devraient être conformes à la norme ASCE 04, *Seismic Analysis for Safety-Related Nuclear Structures*.

L'intrant sismique pour les supports multiples des sous-systèmes et composants devrait tenir compte de leurs composantes inertielles et cinématiques. L'analyse devrait suivre les normes ASCE 04 ou CSA N289.3-10, *Design procedures for seismic qualification of nuclear power plants*.

La détermination du nombre de cycles sismiques pour l'analyse des sous-systèmes devrait être conforme au document U.S. NRC NUREG-0800, Standard Review Plan, section 3.7.3, *Seismic Subsystem Analysis*, ainsi qu'à l'analyse sismique des réservoirs hors-sol.

La conception sismique des sous-systèmes et des composants devrait être conforme à la norme ASCE 43-05, section 8.2.3, qui suit le code de l'ASME.

Pour les équipements qualifiés par des essais, les essais multiaxes et multifréquences sont acceptables pour le séisme de référence conformément aux exigences de la norme IEEE 344-2004 – *IEEE Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations*, et le spectre de réponse obtenu par les essais doit être un facteur d'au moins 1,4 fois le spectre de réponse requis pour toute la plage des fréquences. Tout écart par rapport à ce critère devrait être justifié selon une approche prudente, au cas par cas.

Toute évaluation pour un séisme hors dimensionnement devrait utiliser la méthode décrite dans le document de l'Electrical Power Research Institute, (EPRI) TR-103959, *Methodology for Developing Seismic Fragilities*, pour déterminer si on satisfait au critère de faible probabilité de défaillance avec un degré de confiance élevé (HCLPF, de l'anglais *high confidence low probability of failure*).

La conception des instruments de mesures sismiques devrait respecter la norme CSA-N289.5-M91 (R2008) *Seismic, Instrumentation Requirements for CANDU Nuclear Power Plants*, qui énumère les exigences relatives à l'instrumentation sismique pour les centrales à une ou plusieurs tranches.

La marge hors dimensionnement devrait être telle que les probabilités de défaillances des SSC induites par des séismes ne contribuent pas à la fréquence d'endommagement total du cœur et à la fréquence des petits et grands rejets au point où ils ne répondent pas aux objectifs de sûreté. Les critères d'acceptation pour les séismes hors dimensionnement devraient:

- avoir une valeur HCLPF au niveau de la centrale égale à au moins 1,67 fois la valeur pour le séisme de référence
- assurer l'intégrité des enceintes de confinement dans le cas d'un séisme hors dimensionnement

L'évaluation et la validation des marges pour un séisme hors dimensionnement devraient être prises en considération, y compris le critère HCLPF.

L'isolation sismique des SSC est une approche de conception acceptable pour limiter la demande sismique. Les dispositifs d'isolation sismique devraient être conçus, fabriqués et installés pour résister à une action sismique définie par un séisme de référence sans aucune défaillance, tout en préservant leur résistance mécanique et leur pleine force portante pendant et après le séisme. En outre, les dispositifs et l'ensemble du système structural devraient être conçus pour résister au séisme hors dimensionnement jusqu'à deux fois les accélérations spectrales du séisme de référence sans dommages majeurs tout en préservant leur fonction (sans manifester d'effet falaise). Ils comprennent des dispositions permettant les déplacements structuraux jusqu'à deux fois les déplacements correspondant aux conditions de séisme de référence.

Renseignements supplémentaires

D'autres renseignements sont disponibles dans les documents suivants :

- CSA N289, collection de normes consacrées à la conception et à la qualification parasismique des centrales nucléaires CANDU
- *Code national du bâtiment du Canada (CNBC)* [2010]
- CSA A23.3-F04 (2010), *Calcul des ouvrages en béton* [2010]
- CSA S16-F09, *Règles de calcul des charpentes en acier* [2009]
- CSA N287, collection de normes consacrées aux exigences relatives aux enceintes de confinement en béton des centrales nucléaires CANDU
- CSA N291-08, *Exigences relatives aux enceintes reliées à la sûreté des centrales nucléaires CANDU* [mai 2009]
- American Society of Civil Engineers (ASCE)/SEI 43-05, *Seismic Design Criteria for Structures, Systems and Components in Nuclear Facilities* [2005]
- American National Standards Institute (ANSI)/American Nuclear Society (ANS) Standard 2.26, *Categorization of Nuclear Facility Structures, Systems, and Components for Seismic Design* [confirmée en 2010]
- ASCE 04-98, *Seismic Analysis of Safety-Related Nuclear Structures* [2000]
- American Society of Mechanical Engineers (ASME) BPV Code Section III, Division 1-Subsection NE *Rules for Construction of Nuclear Facility Components* [2010]
- U.S. NRC, Regulatory Guide 1.57, *Design Limits and Loading Combinations for Metal Primary Reactor Containment System Components* [2007]
- U.S. NRC Regulatory Guide 1.91, *Evaluations of Explosions Postulated to Occur on Transportation Routes Near Nuclear Power Plants* [1978]
- U.S. NRC, NUREG-0800, section 3.7.3, *Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR edition- Seismic Subsystem Analysis* [2007]
- Institute of Electrical and Electronics Engineers, *IEEE Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations*, IEEE 344-2004
- Electric Power Research Institute, *Methodology for Developing Seismic Fragilities*, TR-103959 [1994]
- Norme européenne NF EN 1337-3, *Appareils d'appui structuraux – Partie 3 : Appareils d'appui en élastomère* [septembre 2005]
- Norme européenne NF EN 1337-1, *Appareils d'appui structuraux – Partie 3 : Indications générales* [décembre 2000]
- Norme européenne NF EN 15129, *Dispositifs antisismiques* [janvier 2010]

7.14 Essais, entretien, réparations, inspection et surveillance en cours d'exploitation

Même si les essais, l'entretien, les réparations, l'inspection et la surveillance en cours d'exploitation interviennent principalement pendant la phase d'exploitation du cycle de vie de la centrale, la centrale nucléaire est conçue pour permettre la réalisation efficace de ces activités durant l'exploitation. En particulier, le cœur du réacteur devrait être conçu pour permettre la mise en œuvre d'un programme de surveillance des matériaux afin de surveiller les effets des conditions opérationnelles sur les propriétés des matériaux tout au long de la durée de vie utile du réacteur.

La conception devrait établir un fondement technique pour les SSC qui doivent être mis à l'essai, entretenus, réparés, inspectés et surveillés en cours d'exploitation.

L'élaboration de stratégies et de programmes tenant compte des essais, de l'entretien, des réparations, de l'inspection et de la surveillance en cours d'exploitation est un aspect nécessaire de la phase de conception de la centrale. Les stratégies et les programmes qui seront mis en œuvre

pour ces activités en cours d'exploitation devraient être élaborés afin de garantir que les SSC de la centrale demeureront aptes et disponibles pour exécuter leurs fonctions de sûreté. La conception devrait incorporer des dispositions reconnaissant le besoin d'essais, d'entretien, de réparations, d'inspection et de surveillance en cours d'exploitation, ainsi que des dispositions permettant de réparer, de remplacer et de modifier les SSC susceptibles de nécessiter de telles mesures en raison des conditions opérationnelles prévues. En outre, les activités qui doivent être exécutées durant les phases de construction et de mise en service devraient être identifiées afin de fournir des données de référence significatives de la centrale, dès le début de sa durée de vie utile.

Les stratégies devraient comprendre des programmes efficaces et bien planifiés pour l'évaluation et l'établissement de tendances relativement au rendement des SSC, associés à un programme d'entretien préventif optimisé.

Les stratégies et les programmes devraient démontrer la prise en considération des éléments suivants :

- la durée de vie nominale, les conditions de charge nominale, les exigences opérationnelles et l'importance des SSC pour la sûreté
- les exigences relatives aux codes, aux normes et aux règlements applicables
- les responsabilités du concepteur, du fournisseur, du constructeur, de l'organisme exploitant et des sous-traitants
- l'interdépendance des SSC importants pour la sûreté et les effets possibles de la défaillance des SSC d'une classe de sûreté moins élevée sur les SSC d'une classe de sûreté supérieure
- la conception, l'agencement et l'accessibilité des SSC durant la construction, la mise en service et la durée de vie prévue de la centrale
- les programmes de surveillance, d'inspection et d'essais utilisés durant la construction, la mise en service et l'exploitation de centrales nucléaires présentant une conception et un agencement similaires ou identiques
- les techniques et les méthodes disponibles pour la surveillance, l'inspection et les essais, ainsi que pour la réparation, le remplacement ou la modification des SSC
- les activités de recherche et de développement
- l'expérience en exploitation
- les facteurs humains
- la formation et la qualification du personnel
- la disponibilité d'une main-d'œuvre suffisamment formée et qualifiée
- la disponibilité des services de laboratoire ou des installations et équipements d'essai nécessaires

En cas d'utilisation de méthodes d'inspection en cours d'exploitation tenant compte des risques lors de la définition de la portée d'un programme d'inspection, la méthode devrait être clairement documentée.

Les SSC importants pour la sûreté devraient être conçus et disposés afin de faciliter la surveillance et l'entretien, de permettre d'y accéder rapidement, de poser un diagnostic et d'effectuer des réparations en cas de défaillance, et de réduire au minimum les risques posés au personnel d'entretien.

Les moyens prévus pour l'entretien des SSC importants pour la sûreté devraient être conçus de manière à ce que les effets sur la sûreté de la centrale soient acceptables.

Renseignements supplémentaires

D'autres renseignements sont disponibles dans les documents suivants :

- CSA, N285.4-F09, *Inspection périodique des composants des centrales nucléaires CANDU* [2009]
- CSA, N285.4-08, *Inspection périodique des composants de confinement des centrales nucléaires CANDU* [2008]
- CSA, N287.7-F08, *Exigences relatives à la mise à l'essai et à la vérification, en cours d'exploitation, des enceintes de confinement en béton des centrales nucléaires CANDU* [2008]
- CSA N291-08, *Exigences relatives aux enceintes reliées à la sûreté des centrales nucléaires CANDU* [mai 2009]
- CCSN, S-210, *Programmes d'entretien des centrales nucléaires* [2007]
- CCSN, RD-334, *Gestion du vieillissement des centrales nucléaires* [2011]
- ASME *Boiler and Pressure Vessel Code-2010*, Section XI, *Rules for Inservice Inspection of Nuclear Power Plants* [2010]
- AIEA, Guide de sûreté n° NS-G-2.6, *Maintenance, Surveillance and In-Service Inspection in Nuclear Power Plants* [2002]

7.15 Structures de génie civil

Les présentes lignes directrices traitent de la conception de toutes les structures liées à la sûreté, y compris les enceintes de confinement de la centrale nucléaire.

7.15.1 Conception

L'autorité responsable de la conception devrait fournir les principes de conception, les exigences et les critères relatifs au dimensionnement, les codes et normes applicables, les procédures de conception et d'analyse, les conditions limitatives supposées et les programmes informatiques utilisés dans les analyses et lors de la conception.

Toutes les charges liées aux risques internes et externes et les critères de celles-ci sont spécifiés à la section 7.4. Les charges dues aux mouvements sismiques d'un séisme de référence et les répercussions des actes malveillants, y compris les écrasements d'avions, se trouvent respectivement à la section 7.13 et à la section 7.22.

L'autorité responsable de la conception devrait démontrer que les objectifs de sûreté ont été atteints en effectuant une analyse détaillée des dangers dans les divers états de fonctionnement et les conditions d'accident.

Les catégories de charges correspondant aux états de la centrale sont définies dans cette section de manière à démontrer le rendement structural de la façon suivante :

- les charges liées aux conditions normales attendues au cours de la durée de vie nominale de la centrale nucléaire
- les charges en cas d'IFP (ou les charges environnementales sévères)
- les charges en cas d'AD (ou les charges environnementales anormales ou extrêmes)
- les charges liées aux CAD (ou charges hors dimensionnement)

La conception devrait identifier toutes les charges liées aux CAD prises en considération dans la conception des structures et fournir la méthode d'évaluation et les critères d'acceptation.

La conception des structures devrait tenir compte de l'influence du vieillissement sur la structure et ses matériaux.

La conception devrait démontrer l'existence de marges de sûreté suffisantes pour les bâtiments et les structures ayant une importance sur le plan de la sûreté.

La description des caractéristiques physiques et matérielles de chaque structure de génie civil et de sa dalle-support devrait comprendre :

- le type de structure et ses caractéristiques structurales et fonctionnelles
- la géométrie des structures, y compris des schémas montrant la vue en plan à des hauteurs et des sections différentes (au moins deux plans orthogonaux)
- la relation entre les structures adjacentes, y compris les séparations ou liens structuraux éventuels
- le type de dalle-support et son ordonnance avec les méthodes de transfert des forces de cisaillement horizontal (comme celles induites par les séismes) aux fondations

Structure de confinement

La conception devrait spécifier les exigences relatives à la sûreté du bâtiment ou du système de confinement, y compris, par exemple, sa résistance structurale, son étanchéité et sa résistance aux charges permanentes et transitoires (comme celles générées par la pression, la température, le rayonnement et les chocs mécaniques) susceptibles d'être engendrées par des événements hypothétiques internes et externes. De plus, la conception devrait spécifier les exigences de sûreté et les caractéristiques de la conception concernant les structures internes de confinement, telles que la structure de la voûte du réacteur, les portes de blindage, les sas, le contrôle de l'accès et les installations.

La conception de la structure de confinement devrait comprendre les éléments suivants :

- la dalle-support et la couche de fondation
- la conception des parois et du dôme de confinement
- les ouvertures et les percées dans les murs de confinement
- le système de précontrainte
- le revêtement du confinement et sa méthode de fixation

La pression nominale du bâtiment de confinement devrait être déterminée en augmentant d'au moins 10 % le pic de pression qui serait engendré par l'AD (consulter la clause 4.49 du Guide de sûreté de l'AIEA NS-G-1.10, *Design of Reactor Containment Systems for Nuclear Power Plants*).

La capacité maximale de pression interne devrait être fournie pour les structures de l'enceinte de confinement, y compris les percées dans le confinement.

Si la fondation de l'enceinte de confinement est constituée de la dalle-support commune et qu'elle n'est pas séparée de la fondation des autres bâtiments, il faudrait évaluer les répercussions.

Les structures de confinement en béton devraient être conçues et construites conformément à la collection de normes CSA N287, le cas échéant :

- la norme N287.1 pour les exigences générales relatives à la documentation des spécifications de conception et des rapports sur la conception
- la norme N287.2 pour les matériaux
- la norme N287.3 pour la conception
- les normes N287.4 et N287.5 pour la construction et l'inspection des enceintes de confinement
- la norme N287.6 pour les essais de pressurisation effectués avant la mise en service

Les structures de confinement en acier devraient être conçues conformément à la publication de l'ASME intitulée *Boiler and Pressure Vessel Code* (Section III, Division 1, Subsection NE, Class MC Components or equivalency). La stabilité de la cuve de confinement et des dépendances devrait

être évaluée en utilisant les méthodes de conception du gauchissement des enceintes de confinement métalliques du Code de l'ASME (Cas N-284-1, Classe MC, Section III, Division 1).

En ce qui concerne les autres exigences relatives à la conception des structures de confinement, consulter la section 8.6.2 de la version 2 du document RD-337.

Structures liées à la sûreté

Les structures liées à la sûreté autres que le confinement devraient être conçues et construites conformément à la norme CSA N291-08, *Exigences relatives aux enceintes reliées à la sûreté des centrales nucléaires CANDU*.

La conception des autres structures liées à la sûreté devrait comprendre les éléments suivants :

- les structures internes du bâtiment du réacteur
- le bâtiment de service (auxiliaire)
- le bâtiment de stockage du combustible
- le bâtiment de contrôle
- les structures des génératrices diesel
- le bâtiment de l'enceinte de confinement blindée, le cas échéant
- les autres structures liées à la sûreté définies par la conception
- le bâtiment des turbines (pour le réacteur à eau bouillante)

Renseignements supplémentaires

D'autres renseignements sont disponibles dans les documents suivants :

- ACI 349-06, *Code Requirements for Nuclear Safety-Related Concrete Structures & Commentary*, American Concrete Institute [2007]
- AIEA, Guide de sûreté n° NS-G-1.10, *Design of Reactor Containment Systems for Nuclear Power Plants* [2004]
- ASME BPVC Section III, Division 2, Section 3, *Code for Concrete Containments* [2010]
- U.S. NRC NUREG-0800, *Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition - Concrete Containment*, Section 3.8.1 [2007]
- U.S. NRC Regulatory Guide 1.76, *Design Basis Tornado and Tornado Missiles for Nuclear Power Plants* [2007]
- U.S. NRC Regulatory Guide 1.91, *Evaluations of Explosions Postulated to occur on Transportation Routes near Nuclear Power Plants* [1978]
- U.S. NRC NUREG/CR-6486, *Assessment of Modular Construction for Safety-Related Structures at Advanced Nuclear Power Plants* [1997]

7.15.2 Surveillance

En ce qui concerne les enceintes de confinement en béton, il est important de tenir compte de l'inspection de l'intégrité structurale et des essais de pression pour la phase préalable à l'exploitation et la phase en cours d'exploitation. Les programmes d'inspection et d'essais de pression devraient être fournis et satisfaire aux exigences applicables énumérées par la norme CSA N287.6-11, *Pre-operational proof and leakage rate testing requirements for concrete containment structures for nuclear power plants*, et la norme CSA N287.7-F08, *Exigences relatives à la mise à l'essai et à la vérification, en cours d'exploitation, des enceintes de confinement en béton des centrales nucléaires CANDU*.

La conception devrait prévoir des dispositions particulières pour tenir compte de l'inspection et des essais de pression des enceintes de confinement en béton en cours d'exploitation (p. ex. en assurant un accès physique suffisant, en prévoyant d'autres moyens d'identification des conditions dans les

zones inaccessibles pouvant conduire à une dégradation, ou en permettant une surveillance visuelle à distance des zones à haut niveau de rayonnement). Il faudrait mettre en place des programmes permettant d'examiner les zones inaccessibles, de surveiller les propriétés chimiques des eaux souterraines et de surveiller les affaissements et les déplacements différentiels. La conception devrait également prévoir des équipements et des instruments, par exemple une jauge de contrainte, pour surveiller les contraintes, les tensions et la déformation éventuelle des structures.

7.15.3 Levage de charges lourdes

Cette section est traitée de manière suffisante par la version 2 du document RD-337, *Conception des nouvelles centrales nucléaires*. Il n'est donc pas nécessaire de fournir de l'orientation supplémentaire à ce sujet.

7.16 Construction et mise en service

Il faudrait tenir dûment compte de l'expérience pertinente qui a été acquise dans la construction et la mise en service d'autres centrales similaires et de leurs SSC connexes. En cas d'adoption des pratiques exemplaires d'autres industries pertinentes, il faudrait montrer que ces pratiques conviennent à l'application nucléaire envisagée.

La conception devrait comprendre des exigences préliminaires relatives à la mise en service de la centrale pour les essais préalables à l'exploitation et les essais liés au démarrage initial :

- Les essais préalables à l'exploitation sont les essais réalisés après l'achèvement des activités de construction et des inspections et essais liés à la construction, mais avant le chargement du combustible. De tels essais démontrent, dans la mesure du praticable, que les SSC sont capables de répondre aux exigences de rendement et aux critères d'acceptation.
- Les essais liés au démarrage initial comprennent les activités d'essai que l'on prévoit de réaliser durant et suivant le chargement du combustible. Les activités d'essai comprennent le chargement du combustible, les essais préalables à la criticité, les essais réalisés à l'étape de criticité initiale à faible puissance et les essais de montée en puissance, qui devraient confirmer les mécanismes de dimensionnement et démontrer, dans la mesure du praticable, que la centrale fonctionnera conformément à sa conception et qu'elle est capable, telle que conçue, de répondre aux IFP et aux conditions d'accident.

L'autorité responsable de la conception devrait fournir une orientation générale sur le contrôle des activités de mise en service, y compris les contrôles administratifs qui seront utilisés pour élaborer, examiner et approuver les différentes procédures d'essai, la coordination avec les organisations participant au programme d'essai, la participation du personnel technique et du personnel chargé de l'exploitation de la centrale, ainsi que l'examen, l'évaluation et l'approbation des résultats des essais.

La conception devrait comprendre une orientation générale sur la façon dont le programme d'essai va utiliser et mettre à l'épreuve les procédures d'exploitation, de surveillance et d'urgence de la centrale, et dans quelle mesure il va le faire.

La conception devrait inclure des résumés des essais des SSC et des caractéristiques de conception particulières qui seront mis à l'épreuve pour vérifier que le rendement des SSC est conforme aux exigences de la conception. Ces résumés des essais devraient comprendre les objectifs, les exigences préalables, les méthodes d'essai et les critères d'acceptation qui feront partie des procédures d'essai.

La conception devrait inclure les critères d'acceptation des activités de mise en service nécessaires et suffisantes pour fournir des assurances raisonnables quant au fait que l'installation « telle que

construite » sera conforme à la conception approuvée de la centrale et aux règlements applicables si ces activités de mise en service sont effectuées et que les critères d'acceptation sont respectés.

La portée des critères d'acceptation devrait correspondre aux SSC qui figurent dans les descriptions de la conception. En général, chaque système devrait avoir des critères d'acceptation suffisants pour vérifier l'information figurant dans les descriptions de la conception. Le niveau de détail spécifié dans les critères d'acceptation devrait être proportionnel à l'importance sur le plan de la sûreté des fonctions et des fondements de ces SSC.

Les critères d'acceptation devraient être objectifs et non ambigus, correspondre aux engagements de la conception et pouvoir être vérifiés par des inspections, des analyses et des essais adéquats durant les étapes de la construction et de la mise en service.

Renseignements supplémentaires

D'autres renseignements sont disponibles dans les documents suivants :

- AIEA, SSR 2/2, *Sûreté des centrales nucléaires : mise en service et exploitation* [2012]
- AIEA, collection Normes de sûreté n° NS-G-2.9, *Commissioning for Nuclear Power Plants* [2003]
- U.S. NRC NUREG-0800, *Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition – Initial Test Program and ITAAC – Design Certification*, chapitre 14 [2007]

7.17 Vieillessement et usure

Outre celles présentées dans la version 2 du document RD-337, des exigences supplémentaires concernant le vieillissement et l'usure sont fournies dans le document d'application de la réglementation RD-334, *Gestion du vieillissement des centrales nucléaires*.

La conception devrait également prendre en considération les éléments suivants :

- l'identification de tous les SSC faisant l'objet d'une gestion du vieillissement
- l'utilisation de nouveaux matériaux présentant de meilleures propriétés de résistance au vieillissement
- le besoin de programmes d'essai des matériaux pour surveiller le vieillissement et la dégradation
- le besoin d'incorporer une surveillance en ligne, en particulier lorsque cette technologie permet de fournir un avertissement rapide d'une dégradation entraînant la défaillance des SSC et que cette défaillance pourrait avoir des conséquences importantes sur le plan de la sûreté

7.18 Contrôle des corps étrangers

Cette section est traitée de manière suffisante par la version 2 du document RD-337, *Conception des nouvelles centrales nucléaires*. Il n'est donc pas nécessaire de fournir de l'orientation supplémentaire à ce sujet.

7.19 Transport et emballage de combustible et de déchets radioactifs

Cette section est traitée de manière suffisante par la version 2 du document RD-337, *Conception des nouvelles centrales nucléaires*. Il n'est donc pas nécessaire de fournir de l'orientation supplémentaire à ce sujet.

7.20 Voies d'évacuation d'urgence et moyens de communications

Renseignements supplémentaires

D'autres renseignements sont disponibles dans les documents suivants :

- Commission des codes du bâtiment et de prévention des incendies, *Code national du bâtiment du Canada*, Ottawa [2010]
- Norme CSA N293-F07, *Protection contre l'incendie dans les centrales nucléaires CANDU* [2007]
- Conseil national de recherches Canada, *Code national de prévention des incendies – Canada (CNPI)* [2010]
- AIEA, GS-R-2 – *Préparation et intervention en cas de situation d'urgence nucléaire ou radiologique – Prescriptions* [2002]

7.21 Facteurs humains

La présente section s'applique à la conception de tous les systèmes de la centrale présentant des considérations relatives aux facteurs humains (FH). Selon la définition du document de la CCSN P-119, *Politique sur les facteurs humains*, les facteurs humains sont « des facteurs qui influencent le rendement humain ». En pratique, on s'attend à ce que la plupart des systèmes de la centrale nécessiteront une certaine prise en compte des FH.

Les processus et les approches systématiques adoptés pour les FH dans la conception devraient répondre aux exigences des normes internationales et des pratiques exemplaires. Les normes et codes liés aux FH utilisés par l'autorité responsable de la conception pour la conception de la centrale devraient être identifiés et évalués en fonction de leur applicabilité, de leur exhaustivité et de leur pertinence.

Il devrait y avoir une autorité suffisante pour la gestion des FH dans la conception afin d'assurer une prise en compte adéquate des considérations relatives aux FH qui influent sur la sûreté. Les exigences de conception liées aux FH qui compléteront les codes (p. ex. en ce qui concerne la facilité d'utilisation et le rendement humain) devraient également être identifiées et spécifiées tout au début du processus de conception.

Les domaines suivants devraient avoir des interfaces avec les FH dans la conception :

- la conception technique de certains SSC
- l'élaboration de procédures
- l'élaboration de formations
- la prise en considération des interventions humaines dans les analyses de sûreté
- les spécifications relatives à la dotation en personnel et à l'effectif minimal par quart

Les attentes relatives à la conception sont présentées ci-dessous en vue de leur utilisation à différentes étapes de la conception.

Planification

Un plan de programme d'ingénierie des facteurs humains (PPIFH) démontre la façon dont les considérations relatives aux FH sont intégrées dans les activités de conception. Des indications complémentaires sur la façon d'élaborer un tel plan sont fournies dans le guide d'application de la

réglementation de la CCSN G-276, *Plan de programme d'ingénierie des facteurs humains*, et dans la publication de la Nuclear Regulatory Commission (NRC) des États-Unis NUREG-0711 (Révision 2), *Human Factors Engineering Program Review Model*. Les éléments techniques décrits dans le plan devraient être appuyés par des activités de vérification et de validation subséquentes de la conception qui en résulte, de la façon décrite dans le guide d'application de la réglementation de la CCSN G-278, *Plan de vérification et de validation des facteurs humains*.

Les activités de conception liées aux FH sont intégrées de manière efficace dans le processus général de conception technique et incorporées suffisamment tôt pour contribuer efficacement à la sûreté. Les activités de conception liées aux FH devraient être réalisées par un nombre suffisant de spécialistes formés, qualifiés et expérimentés dans le domaine des FH.

Analyse

Des méthodes d'analyse systématiques sont utilisées pour établir les données d'entrée relatives aux FH. De telles analyses devraient être réalisées au tout début de la conception, afin de fournir des fondations solides sur lesquelles reposent les solutions de conception. Chaque analyse des FH devrait :

- être adaptée aux activités abordées en tenant compte du risque posé par les activités et la nouveauté de la conception
- être réalisée tout au long de l'élaboration de la conception
- utiliser des méthodes, des techniques et des pratiques exemplaires considérées comme acceptables par des spécialistes des facteurs humains formés et expérimentés
- partager l'information produite avec les différents groupes participant à la conception

Les analyses des FH pourraient inclure :

- l'analyse des fonctions
- l'analyse des tâches
- l'analyse de la fiabilité humaine
- l'analyse des dangers
- l'analyse des liens
- l'analyse des exigences en matière d'information
- l'analyse de la dotation en personnel
- l'analyse de la facilité d'utilisation
- l'analyse de la facilité d'exploitation et d'entretien

La conception devrait également fournir des rapports sur les recherches ou les études menées sur les travaux réalisés dans le cadre du processus de mise au point et de mise à l'essai de nouvelles techniques d'interface homme-système (p. ex. affichages et commandes) nouvellement appliquées aux centrales nucléaires et susceptibles d'influer sur la sûreté.

La conception devrait démontrer que des mesures ont été prises lors de l'élaboration de la conception afin de réduire ou d'éliminer dans la mesure du praticable les risques d'erreurs humaines, qu'il existe des moyens acceptables permettant d'identifier les erreurs, que l'on a prévu des méthodes de rétablissement en cas d'erreur et qu'il est possible d'atténuer les conséquences des erreurs.

Conception

Il faudrait établir qu'il existe un processus systématique pour la conception des zones de travail, des milieux de travail et des interfaces homme-système pour les SSC dans toute la centrale. La conception devrait démontrer la prise en considération des questions liées aux FH pour tous les aspects de la centrale et pas seulement dans les zones de commande. Les aspects liés aux FH devraient être pris en considération lors de la spécification et de l'acquisition de SSC disponibles dans le commerce. En ce qui concerne les questions liées aux FH, la conception devrait tenir compte de l'expérience en exploitation acquise dans le cadre de systèmes existants ou de systèmes similaires.

Un aspect important de ce processus systématique est l'utilisation des pratiques exemplaires, des normes et des codes les plus récents dans le domaine des facteurs humains, lors de l'élaboration de la conception. Des orientations sont fournies dans la publication de la Nuclear Regulatory Commission (NRC) des États-Unis NUREG-0700 (révision 2), *Human-System Interface Design Review Guidelines*.

La conception devrait démontrer que les opérateurs (et tout autre utilisateur potentiel) se trouvant dans la salle de commande principale, la salle de commande auxiliaire, le centre de soutien d'urgence et la centrale disposent des renseignements nécessaires et appropriés, dans un format compatible avec les décisions à prendre et les délais d'intervention. Le même type de considérations devrait s'appliquer aux autres utilisateurs d'équipements (p. ex. les techniciens et le personnel chargé de l'entretien) ailleurs dans la centrale.

Personnel d'exploitation

Le personnel disposant d'une expérience opérationnelle acquise dans des centrales similaires devrait participer activement au processus de conception afin de tenir compte le plus tôt possible des considérations relatives à l'exploitation et à l'entretien futurs des SSC.

Il faudrait définir des interfaces formelles entre le(s) groupe(s) chargé(s) des FH dans la conception et les divers groupes chargés de la conception technique participant au processus de conception. Cela facilite les interactions et le partage d'information permettant d'obtenir une bonne intégration des considérations liées aux FH dans la conception.

Vérification et validation

Les évaluations sont un élément essentiel des FH dans le processus de conception et comprennent des activités de vérification et des activités de validation. Les critères d'évaluation (p. ex. les exigences et les normes en matière de conception) devraient être établis avant de procéder à ces évaluations.

Des activités de vérification des FH devraient être réalisées (généralement par le fournisseur et le titulaire de permis) pour confirmer que la conception est conforme aux normes de conception des FH et qu'elle a été mise en œuvre comme prévu dans la centrale.

Des activités de validation devraient être réalisées en mode itératif à différentes étapes du processus de conception, en veillant à ce que la fidélité des tâches soit appropriée. Les données fournies par les activités de validation devraient être analysées et les résultats devraient servir à améliorer la conception. La validation devrait confirmer que le système, y compris les composantes humaines et les procédures visant à appuyer les tâches, répond aux exigences spécifiées pour le système et la

facilité d'utilisation. Les activités de validation devraient également démontrer que le personnel chargé de l'exploitation et de l'entretien est capable d'accomplir ses tâches de manière sécuritaire.

De l'orientation sur les évaluations est fournie dans le guide d'application de la réglementation de la CCSN G-278, *Plan de vérification et de validation des facteurs humains*, et dans la publication de la Nuclear Regulatory Commission (NRC) des États-Unis NUREG-6393, *Integrated System Validation: Methodology and Review Criteria*.

Renseignements supplémentaires

D'autres renseignements sont disponibles dans les documents suivants :

- CCSN, P-119, *Politique sur les facteurs humains* [2000]
- CCSN, G-276, *Plan de programme d'ingénierie des facteurs humains* [2003]
- CCSN, G-278, *Plan de vérification et validation des facteurs humains* [2003]
- CCSN, G-323, *Assurer la présence d'un nombre suffisant de travailleurs qualifiés aux installations nucléaires de catégorie I – Effectif minimal* [2007]
- CSA N290.6-09, *Exigences relatives à la surveillance et à l'affichage des fonctions de sûreté d'une centrale nucléaire au moment d'un accident* [2009]
- CSA N290.4-11, *Requirements for Reactor Control Systems of Nuclear Power Plants* [2011]
- CEI 61839, *Centrales nucléaires de puissance – Conception des salles de commande – Analyse fonctionnelle et affectation des fonctions* [2000]
- CEI 60964, *Centrales nucléaires de puissance – Salles de commande – Conception* [2009]
- ANSI/ANS-58.8, *Time Response Design Criteria for Safety-Related Operator Actions* [1994]
- IEEE 1023, *IEEE Guide for the Application of Human Factors Engineering to Systems, Equipment, and Facilities of Nuclear Power Generating Stations* [2004]
- IEEE 1289, *IEEE Guide for the Application of Human Factors Engineering in the Design of Computer-Based Monitoring and Control Displays for Nuclear Power Generating Stations* [1998]
- U.S. NRC NUREG/CR-1278, *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications- Final Report* [2011]
- U.S. NRC NUREG-0711, *Human Factors Engineering Program Review Model* [2002]
- U.S. NRC NUREG-0700, *Human System Interface Design Review Guidelines* [2002]
- U.S. NRC NUREG-6393, *Integrated System Validation: Methodology and Review Criteria* [1997]
- U.S. NRC NUREG/CR-6633, *Advanced Information Systems Design: Technical Basis and Human Factors Review Guidelines* [2000]
- U.S. NRC NUREG-6684, *Advanced Alarm Systems: Revision of Guidance and Its Technical Basis* [2000]

7.22 Robustesse contre des actes malveillants

Les aspects de sûreté technique liés à la robustesse et à la protection contre les actes malveillants devraient tenir compte des éléments suivants :

- l'approche adoptée pour la conception de base
- les objectifs en matière de rendement des structures
- la caractérisation des menaces
- le développement des charges
- les propriétés des matériaux

- les principes d'analyse et de conception
- les critères d'acceptation structureaux
- la conception des SSC

L'identification des actes malveillants pris en considération dans la conception repose sur le risque d'entraîner un rejet de radioactivité dans la population et l'environnement.

7.22.1 Principes de conception

L'identification des zones vitales implique d'identifier et de localiser les SSC qui doivent être protégés afin d'éviter toute conséquence radiologique inacceptable. La conception comprend le bâtiment du réacteur et la piscine de stockage du combustible usé, y compris la structure abritant la piscine de stockage du combustible usé. Les mesures de protection de ces zones vitales identifiées devraient être évaluées.

En fonction des menaces identifiées, il faudrait sélectionner, définir et élaborer des ensembles de cas de charges pour les menaces de référence (MR) et les menaces improbables (MI). Chaque cas de charge devrait être sélectionné comme le scénario du cas le plus défavorable pour une menace donnée.

7.22.2 Méthodes de conception

Les zones vitales sont conçues conformément à l'approche par paliers liée au niveau de la menace. En ce qui concerne les charges induites par des MR, la méthode de conception des structures applique des mesures de conception prudentes et de saines méthodes d'ingénierie qui répondent aux exigences des codes et des normes.

En ce qui concerne les événements plus graves (MI de premier niveau), une intégrité suffisante des structures permet de protéger les systèmes importants. Les critères relatifs au code de conception peuvent être assouplis, mais la méthode de conception est respectée.

En ce qui concerne les événements extrêmes (MI de deuxième niveau), une dégradation de la barrière de confinement peut être acceptée mais la dégradation est limitée. Les structures des zones vitales sont conçues pour des MI de deuxième niveau qui peuvent dépasser les limites des codes de conception mais demeurent dans les limites documentées pour les matériaux et les structures.

Les fonctions de chargement dues aux écrasements d'avions, liées aux MR et aux MI, sont « classifiées » et peuvent être obtenues par les demandeurs et les titulaires de permis sur demande auprès de la CCSN.

Il est acceptable de modéliser tout l'avion comme une charge qui heurte la structure. Toutefois, la conception devrait faire en sorte que les fonctions de chargement dues à l'écrasement de l'avion modélisé sur une enveloppe cible rigide soient acceptables.

Deux types distincts de modes de défaillance structurale doivent être examinés : la défaillance locale (rupture par poinçonnement, rupture fragile) et la défaillance globale (déformation plastique, rupture par flexion). Les caractéristiques de chargement et le comportement structural de ces deux modes de défaillance sont différents et devraient être examinés séparément. Toutefois, il convient de noter que, dans certains cas, ces deux modes de défaillance (p. ex. un écrasement d'avion) peuvent intervenir simultanément ou de façon quasi simultanée.

Le comportement des structures locales en cas de charges induites par un acte malveillant devrait être évalué. Les dommages locaux causés à la cible peuvent être définis à l'aide des descriptions suivantes :

- pénétration – la profondeur du cratère dû à l'impact du missile
- effritement – l'éjection de matières de la cible provenant de la face avant de la cible (face heurtée)
- écaillage – l'éjection de matières provenant de la face arrière de la cible
- perforation uniquement – le missile ne fait que pénétrer la cible, avec une vitesse résiduelle nulle

En cas d'écrasement d'avion, la plupart des références techniques considèrent les moteurs comme les missiles déterminants. En général, de tels modes de dégradation locale ne devraient pas entraîner l'écroulement des structures, mais ils peuvent endommager des systèmes ou des composants liés à la sûreté. L'application de formules empiriques pour la perforation et la formation d'éclats est une méthode acceptable pour évaluer le comportement des structures soumises à des charges locales et concentrées.

Les effets globaux de la réponse structurale désignent le comportement global du bâtiment en réponse aux charges appliquées par l'impact. La réponse globale peut être caractérisée par des dommages structuraux importants tels qu'une perforation importante ou l'effondrement de parties importantes des murs, des planchers et des structures portantes du bâtiment. L'impact est également susceptible d'induire des vibrations importantes ou des « charges par à-coups » dans tout le bâtiment.

En cas d'écrasement d'avion, les dommages locaux liés à l'impact d'un missile dans la paroi peuvent entraîner l'écaillage du béton de la face arrière. En fin de compte, ils peuvent entraîner une rupture locale des barres d'armature, permettant la perforation de la paroi par la masse résiduelle du moteur écrasé et la partie restante de l'arbre. Toutefois, le dommage structural global est généralement lié à la déformation de l'ensemble du système structural.

La conception du système de protection physique de l'installation devrait tenir compte des changements survenant au niveau des menaces, d'une meilleure compréhension des vulnérabilités potentielles de l'installation, de ses systèmes et de ses structures, ainsi que des avancées dans les méthodes, les systèmes et les techniques de protection physique.

7.22.3 Critères d'acceptation

Les critères d'acceptation pour le comportement local et le comportement global devraient être satisfaits simultanément.

Les critères d'acceptation structuraux pour le comportement local devraient comporter les éléments suivants :

- MR – pas d'écaillage de la face arrière des éléments structuraux, possiblement avec un effritement superficiel et limité du béton, facilement réparable
- MI graves – pas d'écaillage de la face arrière des éléments structuraux, ou un effritement limité possible (enrobage de béton) lorsqu'il est confiné au chemisage en acier. Le chemisage en acier devrait rester étanche
- MI extrêmes – pas de perforation, conformément à la formule applicable avec un facteur d'augmentation correspondant de 1,2 appliqué à l'épaisseur calculée

Les analyses structurales détaillées des enceintes de confinement représentatives indiquent qu'il faudrait s'attendre à de grands déplacements de l'enceinte de confinement ainsi qu'à des vibrations induites. Les critères d'acceptation structuraux pour le comportement global sont liés à la limitation des fléchissements structuraux (MR et MI graves) ou des dommages globaux (MI extrêmes). Par conséquent, il convient d'accorder une attention particulière aux aspects suivants :

- les dommages occasionnés aux structures internes et à l'enceinte de confinement en raison des déformations importantes subies par le bâtiment de confinement
- les dommages causés par les chocs aux composants fragiles directement fixés au mur de confinement
- les vibrations induites
- l'intégrité structurale du réservoir d'eau de réserve (p. ex. conception des réacteurs CANDU)
- l'intégrité structurale du pont polaire de manutention

Les critères d'acceptation structuraux pour les éléments en béton armé sont présentés au tableau 1.

Les critères d'acceptation pour les éléments en acier sont présentés au tableau 2.

Tableau 1 : Critères d'acceptation structuraux pour les éléments en béton armé adaptés de la publication ACI 349-06 de l'American Concrete Institute, *Code Requirements for Nuclear Safety-related Concrete Structures and Commentary* et de la publication TM 5-1300 du Département de l'Armée des États-Unis, *Structures to Resist the Effects of Accidental Explosions* [1990] (remplacée par la publication UFC 3-340-02, 2008).

Type d'élément	Contrôle des contraintes	Ductilité, μ_a	Rotation du support en degrés ^(3,4) , θ_a		
			MR	MI de premier niveau	MI de deuxième niveau
Poutres	Flexion	(2)	comportement essentiellement élastique ⁽⁶⁾	2	4
	Cisaillement : ⁽¹⁾				
	béton uniquement	1,3			
	béton + étriers	1,6			
	étriers uniquement	3,0			
	compression	1,3			
Dalles-support	Flexion	(2)	comportement essentiellement élastique ⁽⁶⁾	4	8
	Cisaillement : ⁽¹⁾				
	béton uniquement	1,3			
	béton + étriers	1,6			
	étriers uniquement	3,0			
	compression	1,3			
Poutres-colonnes, murs et dalles-support en compression	Flexion	1,3 ⁽⁵⁾	comportement essentiellement élastique ⁽⁶⁾	2	4
	Compression	1,3			
Cisaillement des murs, diaphragmes	Flexion	3	comportement essentiellement élastique ⁽⁶⁾	1,5	2
	Cisaillement – dans le plan	1,5			

Légende

- (1) contrôles du cisaillement lorsque la résistance au cisaillement est inférieure à 120 % de la résistance à la flexion, d'après la publication ACI-349
- (2) lors des contrôles de la flexion, le rapport de ductilité admissible = $0,05/(\rho - \rho') < 10$ ou la capacité de rotation en radians est limitée à $0,0065(d/c) < 0,07$ radians = 4 degrés
- (3) des étriers sont requis pour supporter des rotations supérieures à 2 degrés
- (4) ces critères de rotation (en degrés) correspondent généralement à ceux indiqués dans le manuel technique de l'ACE, qui ne spécifie pas de déformation inélastique admissible en ce qui concerne les critères du rapport de ductilité pour la flexion
- (5) pour d'autres critères détaillés, consulter la section F.3.8 du document ACI-349
- (6) un comportement essentiellement élastique signifie une analyse de l'élasticité structurale utilisant des critères d'acceptation des déformations de conception de 1 % pour les armatures tendues et de 0,35 % pour le béton en compression

Tableau 2 : Critères d'acceptation structuraux - déformations admissibles pour l'acier

Matériau	Mesure des déformations	Valeur admissible pour les MR	Valeur admissible pour les MI de premier niveau
Tôle d'acier au carbone	Déformation principale de la membrane (déformation due à la traction)	0,01	0,050
	Déformation locale effective par déchirement ductile	non disponible	0,140/FT
Tôle d'acier inoxydable 304	Déformation principale de la membrane (déformation due à la traction)	0,01	0,067
	Déformation locale effective par déchirement ductile	non disponible	0,275/FT
Acier d'armature de nuance 60	Déformation due à la traction	0,01	0,050
Acier de précontrainte (tendons non injectés)	Déformation due à la traction	0,010	0,030
Acier de précontrainte (tendons injectés)	Déformation due à la traction	0,010	0,020

Par mesure de prudence, on peut prendre une valeur de FT (facteur triaxial) égale à 2.

$$TF = \frac{\sigma_1 + \sigma_2 + \sigma_3}{\sigma_e}$$

Où σ_1 , σ_2 et σ_3 sont les contraintes principales et σ_e est la contrainte effective ou contrainte équivalente.

Les valeurs des tableaux 1 et 2 sont des valeurs maximales en condition de chargement. Pour le béton armé et précontraint, la déformation maximale en compression pour les MR est de 0,0035. Pour les MI de premier niveau, cette déformation est de 0,005. Les déformations des MI de deuxième niveau peuvent être déduites des rotations du support données au tableau 2. Il convient de noter que les critères d'acceptation présentés aux tableaux 1 et 2 s'appliquent aux parties importantes des structures subissant des forces impulsives importantes.

D'autres renseignements concernant la conception et la construction des enceintes de confinement et des autres structures liées à la sûreté figurent respectivement dans la collection de normes CSA N287 et dans la norme CSA N291-08, *Exigences relatives aux enceintes reliées à la sûreté des centrales nucléaires CANDU*.

Renseignements supplémentaires

D'autres renseignements sont disponibles dans les documents suivants :

- CCSN, G-274, *Les programmes de sécurité pour les matières nucléaires de catégorie I ou II, ou pour certaines installations nucléaires* [2003]
- CCSN, G-208, *Les plans de sécurité pour le transport des matières nucléaires de catégorie I, II ou III* [2003]
- CCSN, RD-363, *Aptitudes psychologiques, médicales et physiques des agents de sécurité nucléaire* [2008]
- AIEA, TECDOC-967 (Rev.1)/F, *Orientations et considérations concernant l'application du document INFCIRC/225/Rev.4, La protection physique des matières et installations nucléaires* [mai 2002]
- AIEA, *Recommandations de sûreté nucléaire sur la protection physique des matières nucléaires et des installations nucléaires (INFCIRC/225/Révision 5)* [2011]
- AIEA, TECDOC-1276, *Handbook on the physical protection of nuclear materials and facilities* [2002]
- Centre de la sécurité des télécommunications, TRA-1, *Méthodologie harmonisée d'évaluation des menaces et des risques (EMR)* [2007]
- CSA N291-08, *Exigences relatives aux enceintes reliées à la sûreté des centrales nucléaires CANDU* [mai 2009]
- American Society of Civil Engineers (ASCE), *Design of Blast-Resistant Buildings in Petrochemical Facilities* [2010]
- Norme ACI 349, *Code Requirements for Nuclear Safety-Related Concrete Structures & Commentary* [2007]
- U.S. Department of the Army, TM 5-1300, *Structures to Resist the Effects of Accidental Explosions* [1990]. Remplacée par la publication UFC 3-340-02, 2008.
- American Society of Civil Engineers (ASCE), *Structural Analysis and Design of Nuclear Plant Facilities: 58 (ASCE Manual and Reports on Engineering Practice)* [1980]
- United Kingdom Atomic Energy Authority, (UK AEA), *Guidelines for the design and assessment of concrete structures subjected to impact* [1990]
- Nuclear Energy Institute, NEI 07-13, *Methodology for Performing Aircraft Impact Assessments for New Plant Designs* [2011]

7.22.4 Cybersécurité

La sécurité des systèmes d'IC informatisés est conçue pour assurer un environnement de développement sécurisé doté d'éléments défensifs et de protéger contre les attaques informatiques. Il faudrait utiliser les codes et les normes applicables et consulter les pratiques d'excellence de l'industrie.

La conception d'un programme de cybersécurité devrait prendre en considération :

- la documentation sur la façon dont l'autorité responsable de la conception établit, met en œuvre et maintient le programme pour fournir un niveau d'assurance élevé quant à la protection des systèmes faisant l'objet des mesures de sécurité;

- l'application de stratégies de défense en profondeur pour fournir un niveau d'assurance élevé quant à la pertinence des capacités du programme en matière de cybersécurité;
- la prise en compte des vulnérabilités potentielles sur le plan de la sécurité à chaque phase du cycle de vie des systèmes d'IC informatisés pour les systèmes informatisés importants pour la sûreté;
- l'inclusion de contrôles de sécurité permettant d'assurer un environnement de développement sécurisé durant les phases de développement;
- le programme propre au site devrait comprendre, sans toutefois s'y limiter, les éléments suivants :
 - une stratégie défensive
 - l'identification des biens et des contrôles de sécurité
 - les rôles et les responsabilités
 - les politiques et les procédures
 - la sensibilisation et la formation
 - la gestion de la configuration
 - la protection de l'information
 - la coordination avec d'autres programmes de sécurité
 - le signalement des incidents et un plan de rétablissement
 - la maintenance des programmes

La version 2 du document RD-337 indique que « *la conception de systèmes d'instrumentation et de contrôle informatisés qui sont importants pour la sûreté doit comprendre une architecture de défense de la cybersécurité* ». L'architecture de défense devrait présenter des niveaux de défense de la cybersécurité séparés par des périmètres de sécurité. Les systèmes nécessitant le degré de sécurité le plus important devraient être situés dans les périmètres les plus sécurisés.

L'autorité responsable de la conception devrait identifier les caractéristiques de conception qui assurent un environnement sécuritaire d'exploitation des systèmes importants pour la sûreté.

Les exigences liées à la conception de la sécurité des systèmes d'IC informatisés devraient s'appuyer sur les données des analyses des vulnérabilités. Les vulnérabilités prises en compte par la conception devraient comprendre les éléments suivants :

- les lacunes présentées par la conception, susceptibles de permettre d'accéder aux systèmes (matériel informatique et logiciels) par inadvertance, de manière non intentionnelle ou sans autorisation, ou d'y apporter des modifications pouvant dégrader la fiabilité, l'intégrité ou la fonctionnalité des systèmes durant l'exploitation
- la non-exécution des fonctions de sûreté des systèmes en cas de comportement indésirable des systèmes connectés

En ce qui concerne la protection des systèmes d'instrumentation et de contrôle ainsi que des composants informatisés importants pour les fonctions de sûreté, il faudrait tenir compte des aspects suivants :

- il faudrait protéger les systèmes d'instrumentation et de contrôle ainsi que les composants informatisés qui sont importants pour la sûreté, de même que les systèmes de support et les composants qui, s'ils sont compromis, pourraient avoir une incidence négative sur les fonctions de sûreté
- les attaques informatiques comprennent des menaces physiques ou des menaces logiques (malveillantes ou sans mauvaise intention) provenant de sources situées à l'intérieur ou à l'extérieur du périmètre de l'installation du système

- les systèmes et composants informatisés comprennent le matériel informatique, les logiciels, les micrologiciels et les interfaces
- tous les systèmes informatisés, qu'ils soient autonomes ou non autonomes, devraient être protégés
- les systèmes et composants informatisés destinés aux fonctions du système de préparation aux situations d'urgence, à la sécurité et aux garanties devraient être protégés, si leur conception le permet

Les systèmes d'instrumentation et de contrôle informatisés importants pour la sûreté devraient être protégés des attaques physiques et des accès physiques ou logiques non autorisés, de sorte que :

- tous les systèmes, composants et câblages de réseau importants pour la sûreté devraient être installés à un endroit de la centrale assurant une protection physique de l'équipement
- il faudrait utiliser des méthodes efficaces, notamment des combinaisons appropriées de contrôles par programmation et de mesures de sécurité physiques (p. ex. des enceintes et des pièces fermées à clé, des alarmes sur les portes des enceintes)
- il faudrait limiter l'accès inutile ou non autorisé aux réglages des valeurs de consigne et des valeurs de calage, à cause de leur importance pour éviter une dégradation du rendement des systèmes due aux erreurs éventuelles commises durant l'exploitation ou l'entretien
- les raccords nécessaires pour une utilisation temporaire devraient être désactivés lorsqu'ils ne sont pas utilisés (p. ex. raccordement d'ordinateurs d'entretien et de développement)
- les raccords de transfert des données non utilisés devraient être désactivés
- tous les raccords de transfert des données des systèmes et des composants devraient être placés dans des enceintes
- il faudrait limiter tout accès à distance au système de sûreté à partir d'un ordinateur situé dans une zone présentant une sécurité physique moindre que le système de sûreté
- l'accès aux systèmes de sûreté devrait être noté dans un journal et les journaux de sécurité devraient être vérifiés périodiquement
- la communication sans fil ne devrait pas être appliquée aux systèmes de sûreté
- les systèmes de sûreté devraient être conçus de manière à ne pas nécessiter de logiciels antivirus
- la communication des données de la centrale entre la centrale et la salle de commande d'urgence (située sur place ou hors site) devrait se faire par liaisons unidirectionnelles

La version 2 du document RD-337 indique que « *les caractéristiques de la cybersécurité ne doivent pas compromettre les fonctions ni le rendement des SSC importants pour la sûreté* ». Les fonctions de sécurité et les fonctions de support de la sécurité des systèmes d'IC ne devraient pas avoir d'incidence négative sur les fonctions des systèmes et des composants importants pour la sûreté. La conception devrait assurer que ni l'exécution ni la défaillance des mesures de sécurité mises en œuvre n'auront d'incidence négative sur les capacités des systèmes importants pour la sûreté.

En cas de mise en œuvre de fonctions ou de contrôles de sécurité particuliers, ou encore d'un ensemble complet de contrôles appliqués aux systèmes de sûreté, il faudrait tenir compte des éléments suivants :

- la mise en œuvre ne devrait pas avoir de répercussions sur le rendement, y compris le temps de réponse, l'efficacité ou l'exécution des fonctions de sûreté
- dans la mesure du possible, il faudrait éviter de procéder à la mise en œuvre directement dans le système de sûreté
- en cas d'application aux affichages et aux contrôles du système de sûreté, le contrôle de sécurité ne devrait pas avoir d'incidence négative sur la capacité de l'opérateur à maintenir la sûreté de la centrale

- en cas de mise en œuvre au sein du système de sûreté, des mesures adéquates devraient être prises pour s'assurer que les contrôles de sûreté n'aient pas d'incidence négative sur la capacité du système à remplir ses fonctions de sûreté
- les contrôles de sécurité au sein d'un système de sûreté devraient être développés et qualifiés pour avoir le même niveau de qualification que le système qui abrite le contrôle

Il faudrait prendre des dispositions en matière de vérifications périodiques et de vérifications à la suite d'un entretien, afin de vérifier la configuration et le fonctionnement corrects des caractéristiques de sécurité.

Renseignements supplémentaires :

D'autres renseignements sont disponibles dans les documents suivants :

- AIEA, collection Sécurité nucléaire n° 17, *Computer Security at Nuclear Facilities* [2011]
- IEEE 7-4.3.2, *IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations* [2010]
- CEI 61513, *Centrales nucléaires de puissance – Instrumentation et contrôle-commande importants pour la sûreté – Exigences générales pour les systèmes* [2011]
- NEI 08-09 Rev.6, *Cyber Security Plan for Nuclear Power Reactors* [2010]
- U.S. NRC, Regulatory Guide 5.71, *Cyber Security Programs for Nuclear Facilities* [2010]

7.23 Garanties

Dans le cadre du présent document, le terme « garanties » désigne un système d'inspections et autres activités de vérification entreprises par l'AIEA afin d'évaluer la conformité d'un pays à ses obligations conformément à l'accord de garanties qu'il a conclu avec l'AIEA dans le cadre du *Traité sur la non-prolifération des armes nucléaires*. L'accord de garanties conclu entre le Canada et l'AIEA vise à permettre à l'AIEA de fournir, sur une base annuelle, l'assurance au Canada et à la communauté internationale que toutes les matières nucléaires déclarées servent à des fins pacifiques et non explosives et qu'il n'y a aucun signe d'activités ou de matières nucléaires non déclarées. La CCSN est l'autorité gouvernementale chargée de la mise en œuvre de l'accord de garanties conclu entre le Canada et l'AIEA.

L'intégration de considérations relatives aux garanties au cours de la première phase de la conception d'une nouvelle centrale nucléaire est une pratique bien établie dans le secteur nucléaire canadien. Cette approche permet d'éviter la mise en conformité des équipements de contrôle des garanties lorsque la conception est achevée, laquelle pourrait autrement entraîner une augmentation importante des coûts liés aux activités de modification de la conception, à la prolongation des délais et aux demandes supplémentaires en ressources humaines. En cas d'exigence relative à l'installation d'équipement de contrôle des garanties de l'AIEA pour surveiller les flux et les stocks de matières nucléaires, il faudrait identifier de façon précise les exigences liées à l'aménagement de la centrale dès le début du processus afin de s'assurer qu'un « espace de conception » approprié est alloué aux diverses installations critiques en matière de garanties.

La CCSN exige des titulaires de permis qu'ils mettent en place un programme et des procédures appropriées pour assurer une mise en œuvre efficace des garanties, conformément aux obligations du Canada.

Renseignements supplémentaires :

D'autres renseignements sont disponibles dans les documents suivants :

- CCSN, RD-336, *Comptabilisation et déclaration des matières nucléaires* [2010]

- CCSN, GD-336, *Document d'orientation pour la comptabilisation et la déclaration des matières nucléaires* [2010]

7.24 Déclassement

Tel qu'indiqué dans la version 2 du document RD-337, « *la conception doit tenir compte des activités futures de déclassement et de démantèlement de la centrale* ». Cela devrait inclure des considérations sur l'expérience acquise lors du déclassement de centrales existantes, ainsi que de centrales en état de stockage sûr à long terme. L'expérience suggère que le déclassement de centrales nucléaires pourrait être facilité s'il jouissait d'une plus grande attention à l'étape de la conception. La prise en considération du déclassement à l'étape de la conception devrait entraîner une diminution des doses reçues par les travailleurs et une réduction des répercussions environnementales.

Renseignements supplémentaires

D'autres renseignements sont disponibles dans les documents suivants :

- CCSN, G-219, *Les plans de déclassement des activités autorisées* [2000]
- Agence pour l'énergie nucléaire (AEN), NEA n° 6833, *Decommissioning Considerations for New Nuclear Power Plants*, OCDE [2010]
- Agence pour l'énergie nucléaire (AEN), NEA n° 6946, *Intégration du retour d'expérience du démantèlement à la conception et l'exploitation des futures centrales nucléaires*, OCDE [2010]
- AIEA, TECDOC-1657, *Design Lessons Drawn from the Decommissioning of Nuclear Facilities* [2011]
- CSA N294-09, *Decommissioning of Facilities Containing Nuclear Substances* [2009]
- AIEA, collection Normes de sûreté n° WS-G-2.1, *Déclassement des centrales nucléaires et des réacteurs de recherche – Guide de sûreté* [novembre 2004]

8.0 Exigences relatives aux systèmes

8.1 Cœur du réacteur

La conception du cœur du réacteur devrait donner l'assurance que les limites de conception admises dans les divers états de fonctionnement et en conditions d'accident ne sont pas dépassées, en tenant compte des tolérances techniques et des incertitudes liées aux calculs.

8.1.0.1 Conception nucléaire

La conception nucléaire prend en compte les flux et la distribution d'énergie à l'intérieur du cœur du réacteur, la conception et l'utilisation des systèmes de contrôle de la réactivité lors de l'exploitation normale et lors de la mise à l'arrêt du réacteur, la stabilité du cœur, les différentes caractéristiques de contre-réaction de réactivité et la physique du combustible.

Attentes générales

La conception du cœur du réacteur devrait tenir compte de tous les moyens pratiques de sorte que, pour l'ensemble des régimes d'exploitation, l'effet net de la contre-réaction nucléaire instantanée compense l'augmentation rapide de la réactivité et de la puissance. Les conséquences des accidents pouvant être aggravés par une contre-réaction de réactivité positive devraient être acceptables ou être atténuées de manière satisfaisante par d'autres caractéristiques de conception.

La conception devrait tenir compte des mesures relevées dans des réacteurs précédents et dans des expériences sur la criticité, de leur utilisation dans les analyses des incertitudes, ainsi que des mesures à relever, y compris les essais de confirmation réalisés lors du démarrage et les mesures régulièrement requises.

La conception devrait prévoir des systèmes d'instrumentation et de contrôle pour :

- maintenir les variables et les systèmes dans les plages d'exploitation prescrites
- surveiller les variables et les systèmes pouvant influencer sur le procédé de fission pour les gammes d'états de fonctionnement et de conditions d'accident prévues

L'efficacité de ces systèmes d'instrumentation et de contrôle devrait être démontrée.

Défense en profondeur

La conception nucléaire devrait incorporer des caractéristiques de sûreté inhérentes pour réduire la dépendance aux dispositifs spécifiquement conçus de sûreté ou aux procédures d'exploitation. La défense en profondeur et les principes connexes devraient être appliqués à la conception de la fonction de sûreté du système de contrôle de la réactivité de manière à contrôler la réaction de fission en chaîne dans les divers états de fonctionnement et d'y mettre fin, au besoin, en conditions d'accident.

La conception nucléaire devrait prévoir des moyens efficaces pour assurer le succès des fonctions de sûreté suivantes :

- prévenir les transitoires de réactivité inacceptables
- arrêter au besoin le réacteur pour éviter la progression des IFP en AD, ou des AD en CAD
- maintenir et surveiller le réacteur en état d'arrêt sûr

Densités et distributions de la puissance du cœur

Les limites de conception des densités et des distributions de puissance devraient être déterminées à partir d'un examen intégré des limites de conception du combustible, des limites thermiques, des limites de la chaleur de désintégration et des analyses des IFP et des accidents. En ce qui concerne la distribution de puissance, la conception du cœur du réacteur devrait démontrer les éléments suivants :

a) Il y a haut niveau de confiance quant à la possibilité de respecter les limites de conception proposées pour l'ensemble des conditions d'exploitation prévues du réacteur, compte tenu :

- des méthodes d'analyse et des données destinées aux calculs de conception
- des analyses des incertitudes et des comparaisons expérimentales présentées pour les calculs de conception
- de la suffisance des durées calculées des cas de conception pour le cycle de rechargement du combustible ou lors du chargement du combustible en marche (en fonction de la conception du réacteur, de la configuration des dispositifs de réglage de la réactivité et des transitoires après chargement)
- des problèmes particuliers (comme les impulsions de puissance neutronique), des asymétries éventuelles et des dispositifs de contrôle de la réactivité mal alignés

b) Il y a haut niveau de confiance quant au fait que, en mode d'exploitation normale, les limites de conception ne seront pas dépassées en se fondant sur la prise en considération des renseignements fournis par les instruments de surveillance des distributions de puissance. Le traitement de ces renseignements devrait comprendre :

- les calculs (corrélations entre les instruments et les calculs) impliqués dans le traitement
- les procédures d'exploitation utilisées
- les exigences relatives aux mesures de vérification périodiques
- l'exactitude des calculs de conception utilisés pour établir des corrélations lorsque les variables primaires ne sont pas mesurées
- les analyses des incertitudes pour l'information et le système de traitement
- les exigences relatives aux instruments, à l'étalonnage et aux calculs impliqués dans leur utilisation, et les incertitudes impliquées lors de la conversion des indications des instruments en distribution de puissance
- les limites et les points de consigne pour les mesures de contrôle, les alarmes ou le déclenchement automatique des systèmes d'instruments et la démonstration du fait que ces systèmes peuvent maintenir le réacteur à l'intérieur des limites nominales de distribution de puissance (y compris les alarmes des instruments) pour les limites des conditions d'exploitation normale (p. ex. déviations maximales permises, limites du banc de contrôle) et pour les situations anormales (p. ex. alarmes de basculement du flux)
- les mesures réalisées dans des réacteurs précédents et des expériences sur la criticité, y compris leur utilisation dans les analyses des incertitudes
- les mesures nécessaires pour les essais de confirmation réalisés lors du démarrage et les mesures périodiques requises

Les limites des distributions de puissance devraient être déterminées de manière à pouvoir maintenir les limites imposées aux densités de puissance et aux facteurs de surpuissance durant l'exploitation. Ces limites des distributions de puissance pourraient être maintenues (c.-à-d. non dépassées) administrativement (c.-à-d. pas par mise à l'arrêt automatique) pour autant qu'il soit convenablement démontré que les instruments du réacteur fournissent des renseignements et des alarmes correctement traduites pour garder l'opérateur au courant.

La conception devrait établir la corrélation entre les distributions de puissance nominales et les distributions de puissance en exploitation, y compris les corrélations entre les instruments et les calculs, les procédures d'exploitation utilisées et les mesures qui seront prises. Il faudrait établir les limites nécessaires imposées à ces opérations.

Il faudrait établir la répartition des distributions de puissance nominales entre les composants suivants :

- la puissance générée dans le combustible
- la puissance générée directement dans le caloporteur et le modérateur
- la puissance générée directement dans les internes du cœur

Il faudrait établir les distributions de référence des puissances nominales du cœur (distributions axiale, radiale et locale et facteurs de surpuissance) utilisées dans les analyses des IFP et des accidents. En outre, il faudrait établir les distributions de puissance dans les aiguilles de combustible.

Les limites de conception des densités de puissance (et donc des facteurs de surpuissance) en mode d'exploitation normale devraient faire en sorte que les limites de conception acceptables du combustible ne soient pas dépassées en cas d'IFP et que les autres limites ne soient pas dépassées en conditions d'accident. Les limites de conception, de même que les incertitudes, les limites d'exploitation, les exigences relatives aux instruments et les points de consigne connexes devraient être intégrés dans les LCE.

Coefficients de réactivité

La conception devrait établir et caractériser les valeurs de référence limitatives (prudentes) des coefficients de réactivité.

La gamme des états de la centrale à couvrir devrait comprendre l'ensemble de conditions d'exploitation (de l'état d'arrêt à froid à la pleine puissance) et les conditions extrêmes atteintes en cas d'IFP et en conditions d'accident. Elle devrait inclure toute la gamme du cycle de chargement en combustible et la gamme appropriée de configurations des dispositifs de réglage de la réactivité.

Les calculs de conception des coefficients de réactivité devraient couvrir toute la gamme des variables et des approximations de modélisation applicables dans les analyses des IFP et des accidents, y compris les approximations liées à la modélisation et à la nodalisation du système de refroidissement du réacteur. Le cas échéant, il faut établir la différence entre les coefficients du modérateur à l'intérieur des assemblages et entre ceux-ci.

Le niveau de prudence devrait être pris en considération en se fondant sur :

- l'utilisation d'un coefficient (c.-à-d. les analyses dans lesquelles il est important)
- le fait de savoir si des outils de pointe ont servi à calculer le coefficient
- l'incertitude liée à des tels calculs, les vérifications expérimentales du coefficient dans les réacteurs en exploitation
- toute vérification du coefficient requise par le programme de démarrage à la suite d'un changement important de configuration du cœur

Le calcul de conception devrait couvrir et être appuyé par les éléments suivants :

- les valeurs nominales calculées pour les coefficients de réactivité, comme les coefficients du caloporteur et du modérateur (coefficients de température, de vide ou de densité), le coefficient Doppler et les coefficients de puissance
- les analyses de l'incertitude des valeurs nominales, y compris l'ampleur de l'incertitude et la justification de l'ampleur (en examinant la précision des méthodes utilisées dans les calculs), ainsi que la comparaison, dans la mesure du praticable, avec les expériences réalisées dans les réacteurs. En ce qui concerne les comparaisons avec les expériences, il importe de démontrer que les expériences sont applicables et pertinentes, et que les conditions expérimentales coïncident avec les conditions en mode d'exploitation normale et en cas d'accident prévu

- une combinaison de valeurs nominales et d'incertitudes fournissant des valeurs suffisamment prudentes à utiliser dans l'analyse de l'état stationnaire du réacteur (principalement les exigences relatives au contrôle), les analyses de la stabilité et les analyses des IFP et des accidents

Le coefficient de puissance de la réactivité devrait être négatif, ou l'autorité responsable de la conception devrait démontrer que l'exploitation avec un coefficient de puissance positif est acceptable pour certains états de fonctionnement rares, en montrant que :

- une valeur limite du coefficient de puissance de la réactivité a été calculée pour tous les états de fonctionnement autorisés et qu'elle est utilisée dans les analyses du contrôle, de la stabilité et de la sûreté
- des mesures du coefficient de puissance de la réactivité sont effectuées au démarrage et de façon périodique pour certaines conditions limitatives d'exploitation du cœur afin de démontrer que les valeurs mesurées sont délimitées par les valeurs calculées avec une marge appropriée
- le système de contrôle du réacteur est conçu avec une fiabilité adéquate et a la capacité de répondre automatiquement à un coefficient de puissance de la réactivité positif pour une vaste gamme d'IFP

La conception devrait assurer que la probabilité de dépassement des critères spécifiés pour les IFP sans mise à l'arrêt est suffisamment faible en démontrant que les critères sont respectés ou qu'un moyen d'arrêt différent est installé, ce qui réduit considérablement la probabilité d'une incapacité de mise à l'arrêt.

Criticité

La conception nucléaire devrait garantir que la criticité du réacteur est contrôlée durant le rechargement en combustible. En cas d'utilisation du rechargement en combustible en marche pour compenser l'épuisement de la réactivité du cœur, la conception nucléaire devrait établir les valeurs relatives à l'excédent de réactivité du cœur, les puissances locales maximales, la quantité de combustible chargé par opération de rechargement en combustible et la fréquence des opérations de rechargement. La conception devrait également assurer que l'excédent maximal de réactivité du cœur et les pointes de puissance locales prévues ne dépasseront pas la capacité de contrôle du système et les limites thermiques du combustible.

Stabilité du cœur

Les fluctuations de puissance susceptibles d'entraîner des conditions dépassant certaines limites de conception acceptables du combustible devraient être impossibles, ou devraient être détectées et supprimées de façon rapide et fiable.

L'évaluation de la stabilité du cœur du réacteur devrait comprendre :

- les phénomènes et les aspects du réacteur qui influencent la stabilité du cœur du réacteur nucléaire
- les calculs et les considérations accordées aux oscillations spatiales induites par le xénon
- les problèmes de stabilité potentiels, dus à d'autres phénomènes ou conditions
- la vérification des méthodes d'analyse pour la comparaison avec les données mesurées

Méthodes d'analyse

Les méthodes d'analyse et la base de données utilisées pour les analyses de la conception nucléaire et de la physique du réacteur devraient être conformes aux pratiques exemplaires les plus récentes.

En outre, les expériences utilisées pour valider les méthodes d'analyse devraient être des représentations adéquates de la conception du combustible dans le réacteur et les gammes des principaux paramètres de la base de données de validation devraient coïncider avec celles prévues par la conception et l'analyse de la sûreté.

La conception devrait faire en sorte que les méthodes d'analyse utilisées dans la conception nucléaire (y compris celles destinées à prévoir la criticité, les coefficients de réactivité, la combustion nucléaire et la stabilité) ainsi que la base de données et les bibliothèques de données nucléaires utilisées pour les données relatives aux sections de capture des neutrons et les autres paramètres nucléaires (y compris les données concernant les neutrons retardés et les photoneutrons et les autres données pertinentes) sont pertinentes et conviennent aux applications, en se fondant sur une qualification adéquate. La qualification devrait s'appuyer sur des pratiques de validation et de vérification éprouvées, faisant appel à des codes et des normes acceptables.

Internes et cuve du cœur

La conception nucléaire devrait établir :

- le spectre du flux neutronique au-dessus d'un million d'électron-volts (MeV) dans le cœur, à la périphérie du cœur et à l'intérieur de la paroi de la cuve, le cas échéant
- les hypothèses utilisées dans les calculs, comprenant le niveau de puissance, le facteur d'utilisation, le type de cycle du combustible considéré, et la durée de vie nominale de la cuve
- les programmes informatiques utilisés dans les analyses
- la base de données concernant les sections efficaces d'absorption des neutrons rapides
- la modélisation géométrique du cœur du réacteur, des internes et de la cuve (ou des cuves)
- les incertitudes figurant dans les calculs

Renseignements supplémentaires

D'autres renseignements sont disponibles dans les documents suivants :

- CSA N290.4-11, *Requirements for the Reactor Control Systems of Nuclear Power Plants* [2011]
- CSA CAN3-N290.1-80, *Requirements for the Shutdown Systems of CANDU Nuclear Power Plants* [confirmée en 2011]
- CSA N286.7-F99, *Assurance de la qualité des programmes informatiques scientifiques, d'analyse et de conception des centrales nucléaires* [confirmée en 2007]
- CSA N286.7.1-09, *Guideline for the application of N286.7-99, Quality assurance of analytical, scientific, and design computer programs for nuclear power plants* [2009]
- AIEA NS-G-1.12, *Design of the Reactor Core for Nuclear Power Plants* [2005]
- AIEA NS-G-2.5, *Core Management and Fuel Handling for Nuclear Power Plants* [2002]
- U.S. NRC Regulatory Guide 1.77, *Assumptions Used for Evaluating a Control Rod Ejection Accident for Pressurized Water Reactors* [1974]
- U.S. NRC Regulatory Guide 1.203, *Transient and Accident Analysis Methods* [2005]

8.1.0.2 Gestion du cœur et manutention du combustible

La conception du réacteur devrait faire en sorte que la centrale puisse fonctionner dans les limites de fonctionnement prescrites pour toute la durée de vie utile du réacteur (y compris les états intermédiaires du cœur du réacteur).

La conception devrait prévoir des essais à effectuer périodiquement pour surveiller le bon état des composants du réacteur.

La conception devrait prévoir la capacité de surveiller en ligne les paramètres importants du cœur afin de s'assurer que le fonctionnement du réacteur ne sorte pas des limites acceptables en mode d'exploitation normale. Il faudrait décrire les types de détecteurs et autres dispositifs utilisés pour surveiller les paramètres du cœur.

La stratégie de contrôle du réacteur devrait être définie pour assurer que le réacteur soit remis dans un état sûr acceptable si un paramètre du réacteur s'écarte de la plage de valeurs admises. La stratégie de contrôle devrait permettre de maintenir l'intégrité du combustible pour tous les IFP.

Le schéma de rechargement en combustible devrait être établi pour s'assurer que les configurations intermédiaires de rechargement en combustible ne présentent pas une réactivité supérieure à la configuration la plus réactive approuvée par la conception. Les paramètres du cœur pour les configurations intermédiaires devraient respecter les limites approuvées.

La conception devrait permettre l'acquisition de données durant l'exploitation du réacteur et la tenue de dossiers pour les extraire et les analyser ultérieurement.

La conception devrait tenir compte des détails de la stratégie de gestion du combustible, y compris le chargement de combustible dans un cœur neuf, ainsi que des critères permettant de déterminer l'emplacement des assemblages de combustible à décharger du réacteur et charger celui-ci de combustible neuf.

En ce qui concerne les conceptions de réacteurs comportant un chargement de combustible par lots, la conception devrait prévoir des tests de diagnostic réalisés au début du cycle du combustible, de manière à vérifier si les paramètres du cœur ne dépassent pas les limites autorisées.

Il faudrait montrer que les coefficients de réactivité et les paramètres physiques importants restent dans des limites sûres, décrites dans l'analyse de la sûreté.

Internes de réacteur

Les composants internes du réacteur, qualifiés de structures participant au support du cœur par la section III du code de l'ASME, *Core Support Structures*, devraient être conçus, fabriqués et examinés conformément aux dispositions de la section III, sous-section NG du code de l'ASME.

Les composants internes du réacteur, non qualifiés de structures de support du cœur par la section III du code de l'ASME, *Core Support Structures*, devraient être appelés structures internes conformément à la section III, sous-section NG-1122 du code de l'ASME. Les critères de conception, les conditions de chargement et les analyses qui servent de fondement à la conception des internes du réacteur (autres que les structures de support du cœur) devraient satisfaire aux lignes directrices de la section III, sous-section NG-3000 du code de l'ASME, et être construits de façon à ne pas nuire à l'intégrité des structures de support du cœur. Si les critères de contrainte, de déformation et de fatigue se fondent sur d'autres lignes directrices (p. ex. les normes du fabricant ou des méthodes empiriques s'appuyant sur l'expérience acquise et testée sur le terrain), ces lignes directrices devraient être identifiées et leur utilisation justifiée dans la conception.

En ce qui concerne les structures et composants non visés par le code de l'ASME, les marges de conception présentées pour la contrainte, la déformation et la fatigue admissibles devraient être égales ou supérieures aux marges utilisées pour d'autres centrales de conception similaire, disposant d'une expérience en exploitation fructueuse. Toute diminution des marges de conception devrait être justifiée.

Certains composants internes du réacteur désignés comme faisant partie de la classe 1, de la classe 2 ou de la classe 3, devraient être conçus, fabriqués et examinés conformément aux codes et normes applicables, tels que la section III de l'ASME pour les réacteurs à eau ordinaire (REO) et la

norme CSA N285.0, *Exigences générales relatives aux systèmes et aux composants sous pression des centrales nucléaires CANDU*, pour les centrales nucléaires CANDU.

8.1.1 Éléments et assemblages de combustible

La conception et la qualification du combustible devraient garantir le respect des exigences relatives à la conception du cœur du réacteur indiquées à la section 8.2 de la version 2 du document RD-337.

8.1.1.1 Conception du combustible

Il faudrait établir des critères d'acceptation pour les dommages causés au combustible, la défaillance des barres de combustible et les possibilités de refroidissement du combustible. Ces critères devraient provenir d'expériences qui identifient les limites des propriétés des matériaux du combustible et des assemblages de combustible. Les critères de conception du combustible et d'autres considérations relatives à la conception sont présentés ci-dessous.

Domage causés au combustible

Les critères relatifs aux dommages causés au combustible devraient être inclus pour tous les mécanismes de dégradation du combustible connus en conditions d'exploitation normale. Les critères relatifs aux dommages devraient veiller à ce que les dimensions du combustible respectent les limites de tolérance opérationnelle et à ce que les capacités fonctionnelles ne soient pas réduites en deçà de celles présumées dans l'analyse de la sûreté. Le cas échéant, les critères relatifs aux dommages causés au combustible devraient tenir compte des effets d'une combustion nucléaire importante en se fondant sur les données concernant les propriétés des matériaux irradiés. Les critères devraient comprendre les contraintes, les déformations ou les limites de chargement, le nombre cumulatif de cycles de contrainte, l'usure par frottement, l'oxydation, l'hydruration (la deutération dans les réacteurs CANDU), l'accumulation de produits de corrosion, les variations dimensionnelles, les pressions des gaz à l'intérieur des barres, les charges hydrauliques les plus défavorables, et la réactivité et les possibilités d'insertion des barres de commande des REO.

Défaillance des barres de combustible

La défaillance des barres de combustible s'applique aux divers états de fonctionnement et aux conditions d'accident. Les critères de défaillance des barres de combustible devraient être fournis pour tous les mécanismes de défaillance des barres de combustible connus. La conception devrait veiller à ce que le combustible ne subisse pas de défaillance en raison d'une cause particulière dans les états de fonctionnement. Des défaillances des barres de combustible peuvent survenir en conditions d'accident et sont prises en compte dans l'analyse de la sûreté.

Il faudrait indiquer les méthodes utilisées pour évaluer les mécanismes de défaillance du combustible, les limitations relatives au chargement du combustible et aux manœuvres de puissance, ainsi que le service du combustible ayant conduit à une probabilité de défaillance suffisamment faible. Le cas échéant, les critères relatifs aux défaillances des barres de combustible devraient tenir compte des effets d'une combustion nucléaire importante en se fondant sur les données concernant les propriétés des matériaux irradiés. Les critères devraient comprendre :

- l'hydruration
- l'effondrement des gaines
- la surchauffe des gaines
- la surchauffe des pastilles de combustible
- l'enthalpie excessive du combustible

- l'interaction entre les gaines et les pastilles
- la fissuration par corrosion sous tension
- l'éclatement des gaines
- la rupture mécanique

Possibilités de refroidissement du combustible

Les possibilités de refroidissement du combustible s'appliquent aux AD et, dans la mesure du praticable, aux CAD. Les critères relatifs aux possibilités de refroidissement du combustible et les critères relatifs aux possibilités d'insertion des barres de commande des REO devraient être prévus pour tous les mécanismes de dégradation en conditions d'accident. Le combustible devrait être conçu pour assurer que les dommages causés aux barres de combustible ne gêneront pas l'efficacité du système de refroidissement d'urgence du cœur. Les gaines ne devraient pas atteindre des températures suffisamment élevées pour permettre l'apparition d'une réaction importante entre le métal et l'eau, réduisant ainsi la possibilité de rejet de produits de fission hors du site. Les critères devraient inclure la fragilisation des gaines, l'expulsion violente de combustible, la fusion généralisée des gaines, le gonflement des barres de combustible, la déformation des structures et, dans les réacteurs CANDU, la pénétration de brasure au béryllium.

Autres considérations relatives à la conception

La conception devrait également comprendre :

- toutes les activités de manutention du combustible prévues
- les effets de la manutention des assemblages de combustible après irradiation
- le courant de refroidissement des autres composants des assemblages de combustible des REO (tels que les barres de commande, les barres de poison, les instruments ou les sources de neutrons)

Programmes d'essais, d'inspection et de surveillance du combustible

Il faudrait établir des programmes pour l'essai et l'inspection du nouveau combustible de même que pour la surveillance du combustible en marche et la surveillance du combustible irradié après l'irradiation.

Spécifications relatives au combustible

La conception devrait établir les spécifications relatives aux barres et aux assemblages de combustible (y compris les barres de commande des REO) afin de réduire au maximum les écarts de conception et de déterminer si tous les fondements de conception (tels que les limites et les tolérances) sont respectés.

Renseignements supplémentaires

D'autres renseignements sont disponibles dans les documents suivants :

- CCSN, G-144, *Critères d'acceptation des paramètres de déclenchement aux fins de l'analyse de sûreté des centrales nucléaires CANDU* [2006]
- U.S. NRC NUREG-0800, *Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition - Fuel System Design, Section 4.2* [2007]
- ANSI/ANS-57.5-1996, *Light Water Reactor Fuel Assembly Mechanical Design and Evaluation* [1996]

8.1.1.2 Conception thermohydraulique du cœur du réacteur

La conception thermohydraulique devrait prévoir des marges suffisantes permettant d'assurer un transfert de chaleur adéquat entre le combustible et le système de refroidissement du réacteur, de manière à prévenir la surchauffe de la gaine. Les exigences de conception peuvent être démontrées en respectant un ensemble de critères d'acceptation dérivés, comme l'exige le document RD-310, *Analyses de la sûreté pour les centrales nucléaires*.

Le flux thermique critique (FTC) est défini comme le flux thermique se produisant au commencement de l'ébullition nucléée (CEN), habituellement utilisée dans les réacteurs à eau sous pression, ou lors de l'assèchement, habituellement utilisé dans les conceptions de réacteurs CANDU.

Il convient de noter que, bien qu'un critère de marge thermique ne suffise pas à démontrer qu'il est possible d'éviter la surchauffe d'un mécanisme de refroidissement défectueux, d'autres méthodes mécaniques peuvent être acceptables dans la mesure où le FTC n'est pas considéré comme un mécanisme de rupture. Dans certaines conceptions, les conditions de FTC durant les transitoires peuvent être tolérées si l'on peut démontrer par d'autres méthodes que la température de la gaine ne dépasse pas des limites acceptables bien définies. Toutefois, d'autres critères que le critère de FTC devraient tenir compte de la température de la gaine, de la pression, de la durée, de l'oxydation, de la fragilisation, etc., et ces nouveaux critères devraient être appuyés par des preuves expérimentales et des données analytiques suffisantes. En l'absence de telles preuves, la conception thermohydraulique du cœur devrait démontrer une marge thermique par rapport au FTC.

La démonstration de la marge thermique devrait être présentée de manière à tenir compte de l'ensemble des états et conditions de fonctionnement possibles du réacteur, tels que déterminés par les schémas d'exploitation, y compris tous les IFP. La démonstration devrait également inclure les effets à long terme du vieillissement de la centrale et des autres changements prévus dans la configuration du cœur tout au long de la durée de vie utile de la centrale.

La démonstration de la marge thermique devrait soigneusement tenir compte des incertitudes liées aux divers paramètres touchant à la marge thermique. La conception devrait identifier toutes les sources d'incertitude importantes qui contribuent à l'incertitude de la marge thermique. L'incertitude liée à chaque source devrait être quantifiée avec des preuves convaincantes.

En plus de la démonstration de la marge thermique, la conception thermohydraulique du cœur devrait également tenir compte des fluctuations éventuelles de la puissance et du flux du cœur et des instabilités thermohydrauliques. La conception devrait rendre impossible les fluctuations de puissance et de flux susceptibles d'entraîner des conditions dépassant certaines limites de conception acceptables du combustible, ou permettre de les détecter et de les supprimer de façon rapide et fiable.

8.1.2 Système de contrôle du cœur du réacteur

Tel qu'indiqué dans la version 2 du document RD-337, « *le système de contrôle du cœur du réacteur doit détecter et intercepter les déviations par rapport aux états normaux de fonctionnement dans le but d'empêcher les IFP de se transformer en accidents* ».

Contrôle de la réactivité

Le contrôle de la réactivité devrait veiller à ce que :

- les limites de conception acceptables du combustible ne soient pas dépassées en raison d'une vaste gamme d'IFP

- la fonction de contrôle de la réactivité ne puisse présenter le moindre dysfonctionnement susceptible d'entraîner un dépassement des limites de conception acceptables du combustible

Les exigences de la conception nucléaire en matière de contrôle de la réactivité et les dispositions relatives au contrôle devraient :

- compenser les variations de réactivité à long terme du cœur. Ceci comprend les variations de la réactivité dues à l'épuisement des matières fissiles dans le combustible, l'épuisement du poison consommable dans certaines barres de combustible (le cas échéant), ainsi que l'accumulation de produits de fission et d'isotopes transuraniens
- compenser la variation de réactivité causée par le changement de température du réacteur de l'état chaud à puissance nulle à l'état d'arrêt à froid
- compenser les effets sur la réactivité causés par le changement du niveau de puissance du réacteur de la pleine puissance à la puissance nulle
- assurer la gestion de la réactivité au cours du cycle de chargement du combustible et les périodes intermédiaires du cycle du combustible
- compenser les effets sur la distribution et la stabilité de la puissance dus à la forte capacité d'absorption des neutrons du produit de fission xénon-135
- couvrir les incertitudes liées aux barres de commande, y compris :
 - les tolérances de fabrication
 - les erreurs de méthode
 - les modes d'exploitation non prévus
 - l'épuisement des absorbeurs des éléments de commande
 - la mesure des incertitudes dans la démonstration de la marge d'arrêt

Configurations et valeur de réactivité des dispositifs de réactivité

En ce qui concerne les configurations des dispositifs de réactivité, y compris (le cas échéant) les profils des barres de commande ainsi que la valeur de réactivité, la conception nucléaire devrait établir les éléments suivants :

- les configurations des dispositifs de réactivité prévues tout au long du cycle de rechargement du combustible, les manœuvres de puissance et le suivi de charge (le cas échéant). Ceci comprend la manœuvre de barres simples, ou de groupes ou bancs de barres, l'ordre de retrait des barres et les limites d'insertion en fonction de la puissance et de la durée de vie du cœur
- la valeur prévue des dispositifs de réactivité et les taux d'insertion de la réactivité. Ils devraient être raisonnablement liés aux valeurs susceptibles de se présenter dans le réacteur. Remarque : Ces valeurs sont habituellement utilisées dans l'analyse de la sûreté, et les jugements relatifs à la pertinence des tolérances liées aux incertitudes sont réalisés lors de l'examen de l'analyse de la sûreté
- les écarts admissibles par rapport aux profils indiqués ci-dessus, tels que ceux correspondant à des barres décalées, des barres coincées, ou des positions de barres utilisées pour la mise en forme spatiale de la puissance
- la valeur de réactivité maximale des barres individuelles ou des bancs de barres en fonction de la position pour la puissance et les conditions du cycle de vie, appropriée au retrait des barres, aux accidents entraînant l'éjection (ou la chute) de barres, et à d'autres défaillances imaginables des composants de contrôle de la réactivité entraînant des insertions de réactivité positive
- les taux maximum d'augmentation de la réactivité liés aux retraits des dispositifs de réactivité et à toute autre modification imaginable de la configuration des dispositifs de réactivité, dus aux défaillances du système de contrôle de la réactivité. Ils devraient également comporter la confirmation expérimentale de la valeur de réactivité des barres et d'autres facteurs justifiant les taux d'augmentation de la réactivité utilisés dans les analyses des accidents liés aux barres

- de commande, ainsi que les équipements, les procédures administratives et les alarmes qui peuvent être employés pour limiter la valeur potentielle de réactivité des barres
- la réactivité dégressive suite au déclenchement (ou à l'arrêt automatique) en fonction du temps après le déclenchement (ou l'arrêt automatique) et d'autres paramètres pertinents, y compris les méthodes de calcul de la réactivité dégressive
 - l'équipement, les limites d'exploitation et les procédures administratives nécessaires pour limiter la valeur potentielle de réactivité des barres ou les taux d'insertion de la réactivité

8.2 Système de refroidissement du réacteur

Afin de répondre aux exigences en matière de sûreté du système de refroidissement du réacteur (SRR), la conception devrait présenter des dispositions adéquates en ce qui concerne le système de refroidissement du réacteur et les systèmes auxiliaires du réacteur. La conception devrait respecter les limites de conception relatives aux conditions les plus défavorables rencontrées en mode d'exploitation normale, en cas d'IFP et en cas d'AD, y compris les charges dues aux chocs thermiques pressurisés et aux coups de bélier. Le système de refroidissement du réacteur et les systèmes auxiliaires du réacteur devraient remplir (ou contribuer à remplir) les fonctions suivantes :

- maintenir des réserves de caloporteur suffisantes pour assurer le refroidissement du cœur durant et après tous les événements initiateurs hypothétiques envisagés dans le dimensionnement
- évacuer la chaleur du cœur du réacteur à la suite d'une défaillance de l'enveloppe sous pression du système de refroidissement du réacteur afin de limiter les dommages au combustible
- évacuer la chaleur du cœur du réacteur dans les états de fonctionnement appropriés et en conditions d'accident avec l'enveloppe sous pression du système de refroidissement du réacteur intacte
- transférer la chaleur des autres systèmes de sûreté vers la source froide ultime

La conception de chaque système auxiliaire du réacteur devrait s'assurer que le mécanisme automatique déclenché par le système ne puisse nuire à une fonction de sûreté.

L'autorité responsable de la conception devrait démontrer la pertinence des éléments suivants :

- le débit et les chutes de pression dans les principaux composants
- les principaux paramètres thermohydrauliques, tels que la pression d'exploitation et les plages de température
- le rendement des vannes (débit, chute de pression, durées d'ouverture et de fermeture, stabilité, coups de bélier)
- le rendement des pompes (charge, débit, écoulement diphasique, rendement des joints d'étanchéité)
- les vibrations des composants et des conduites
- le contrôle des accumulations de gaz (en particulier la prévention de l'accumulation de gaz combustibles)
- les vitesses d'échauffement et de refroidissement maximales admises
- la prise en considération des chocs thermiques pressurisés causés par le fonctionnement (y compris la manœuvre accidentelle) des systèmes auxiliaires
- la stabilité des flux, y compris la stabilité d'un circuit à l'autre et les fluctuations vide-enthalpie (réacteurs CANDU)
- la conception des robinets d'instrumentation

Le texte qui suit présente quelques exemples d'attentes relatives à la conception du système de refroidissement du réacteur et du système auxiliaire du réacteur :

Pressuriseur

Pour les conceptions comportant un pressuriseur, l'autorité responsable de la conception devrait démontrer la pertinence des éléments suivants :

- le volume et la capacité d'absorption des variations de charge
- la capacité à résister au choc thermique, en particulier dans les buses de pulvérisation et les raccords au circuit du SRR principal
- le contrôle des pressions à l'aide d'appareils de chauffage, de pulvérisateurs ou de refroidisseurs

Dépressurisation du circuit primaire

L'autorité responsable de la conception devrait démontrer la pertinence des éléments suivants :

- le débit en écoulement monophasique et en écoulement diphasique
- l'examen de la corrosion des surfaces de la vanne
- les dispositions permettant d'assurer que la dépressurisation n'entraîne pas un environnement trop hostile dans l'enceinte de confinement
- la stabilité de la vanne de décharge

Pompes du système de refroidissement du réacteur

Pour les conceptions comportant un circuit primaire à circulation forcée, l'autorité responsable de la conception devrait démontrer la pertinence des éléments suivants :

- les caractéristiques de rendement des pompes du circuit primaire, y compris les caractéristiques de la charge et du débit, la vitesse d'écoulement vers l'aval, le rendement des pompes monophasées et biphasées
- les paramètres de fonctionnement des pompes (p. ex. vitesse, débit, charge)
- la charge nette absolue à l'aspiration des pompes pour éviter la cavitation
- la conception et le rendement des joints d'étanchéité des pompes (y compris les limites de température des joints d'étanchéité, le cas échéant)
- les dispositions relatives à la surveillance des vibrations

Renseignements supplémentaires

D'autres renseignements sont disponibles dans le document suivant :

- AIEA, NS-G-1.9, *Design of the Reactor Coolant System and Associated Systems in Nuclear Power Plants Safety Guide* [2004]

8.2.1 Inspection de l'enveloppe sous pression en cours d'exploitation

Cette section est traitée de manière suffisante par la version 2 du document RD-337, *Conception des nouvelles centrales nucléaires*. Il n'est donc pas nécessaire de fournir de l'orientation supplémentaire à ce sujet.

8.2.2 Inventaire

Tel qu'indiqué dans la version 2 du document RD-337, « *en tenant compte des variations volumétriques et des fuites, la conception doit prévoir le contrôle de l'inventaire et de la pression du caloporteur afin de ne pas dépasser les limites spécifiées pour les divers états de fonctionnement* ». En répondant à cette exigence, la conception devrait tenir compte de la présence

d'une capacité adéquate, des variations volumétriques, des fuites, du débit et des volumes de stockage dans les systèmes qui remplissent cette fonction.

8.2.3 Nettoyage

Cette section est traitée de manière suffisante par la version 2 du document RD-337, *Conception des nouvelles centrales nucléaires*. Il n'est donc pas nécessaire de fournir de l'orientation supplémentaire à ce sujet.

8.2.4 Évacuation de la chaleur résiduelle du cœur du réacteur

Cette section est traitée de manière suffisante par la version 2 du document RD-337, *Conception des nouvelles centrales nucléaires*. Il n'est donc pas nécessaire de fournir de l'orientation supplémentaire à ce sujet.

8.3 Système d'alimentation en vapeur d'eau

Des lignes directrices relatives au système d'alimentation en vapeur d'eau figurent au chapitre 10 de la publication de la Nuclear Regulatory Commission (NRC) des États-Unis NUREG-0800, *Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition - Steam and Power Conversion System*.

8.3.1 Conduites de vapeur

Cette section est traitée de manière suffisante par la version 2 du document RD-337, *Conception des nouvelles centrales nucléaires*. Il n'est donc pas nécessaire de fournir de l'orientation supplémentaire à ce sujet.

8.3.2 Tuyauterie et cuves des systèmes de vapeur et d'eau d'alimentation

Cette section est traitée de manière suffisante par la version 2 du document RD-337, *Conception des nouvelles centrales nucléaires*. Il n'est donc pas nécessaire de fournir de l'orientation supplémentaire à ce sujet.

8.3.3 Turbo-alternateurs

La conception des turbo-alternateurs devrait répondre aux attentes suivantes :

- un système de commande et de protection contre la survitesse de la turbine devrait contrôler le fonctionnement de la turbine dans toutes les conditions d'exploitation normale ou anormale et devrait s'assurer qu'un déclenchement de la turbine à pleine charge n'entraîne pas une survitesse de la turbine au-delà des limites acceptables
- le système de protection contre la survitesse devrait répondre au critère de défaillance simple et devrait pouvoir être mis à l'essai lorsque la turbine est en fonctionnement
- les vannes d'arrêt principales de vapeur et les vannes de commande de la turbine ainsi que les vannes d'arrêt de réchauffage et d'interception de la vapeur devraient empêcher la turbine de dépasser les vitesses prédéfinies et devraient protéger le système du réacteur contre les augmentations anormales
- le groupe turbo-alternateur devrait être en mesure de permettre des essais périodiques des composants importants pour la sûreté alors que le groupe fonctionne à charge nominale
- il faudrait établir un programme d'inspection et d'essais en cours d'exploitation pour les principales vannes de vapeur et de réchauffage
- la disposition des joints de raccordement entre l'échappement de la turbine basse pression et le condenseur principal devrait prévenir les effets nuisibles sur les équipements liés à la sûreté

situés dans la salle de la turbine en cas de rupture (il est préférable de ne pas placer d'équipement lié à la sûreté dans la salle de la turbine)

8.4 Systèmes d'arrêt d'urgence

Tel qu'indiqué dans la version 2 du document RD-337, « *la conception doit prévoir deux méthodes distinctes, indépendantes et différentes pour arrêter le réacteur* ».

Pour que les deux méthodes soient indépendantes l'une de l'autre, elles ne doivent pas partager de composants. Si les deux méthodes interviennent à l'intérieur du cœur et qu'une séparation complète est impossible, une séparation adéquate des composants situés à l'extérieur du cœur devrait être démontrée.

La conception utilise diverses méthodes pour tous les aspects des systèmes d'arrêt d'urgence, telles que :

- l'insertion de barres de commande solides et l'injection d'une solution de matières absorbant les neutrons sont les différentes méthodes habituellement utilisées dans les réacteurs refroidis à l'eau
- différentes méthodes devraient être envisagées dans la conception des capteurs, des moyens logiques et des moyens de déclenchement du système d'arrêt

Tel qu'indiqué dans la version 2 du document RD-337, « *il doit y avoir redondance des moyens rapides d'arrêt d'urgence du réacteur* » à moins que l'analyse de la sûreté ne démontre que les critères d'acceptation peuvent être respectés pour tout IFP ou AD coïncidant avec la défaillance d'un seul dispositif d'arrêt d'urgence du cœur du réacteur.

En ce qui concerne les méthodes fondées sur l'injection d'une solution absorbant les neutrons, il faudrait tenir compte des problèmes liés aux réactions chimiques (comme le fait d'éviter les précipitations).

L'autorité responsable de la conception devrait spécifier les exigences relatives à l'inspection, aux essais et à l'entretien, y compris les essais de mise en service réalisés pour vérifier la vitesse et la capacité de mise à l'arrêt de chaque système d'arrêt.

En ce qui concerne les conceptions de REO, le flambage des barres de combustible peut entraîner des charges sur les tubes de guidage des barres de commande susceptibles de nuire aux systèmes d'arrêt fondés sur les barres. La conception du combustible devrait veiller à ce que ce phénomène ne se produise pas dans les états fonctionnement et en cas d'AD.

Tel qu'indiqué dans la version 2 du document RD-337, « *au moins un dispositif d'arrêt d'urgence du réacteur doit permettre, de façon indépendante, de faire passer rapidement le réacteur nucléaire dans un état sous-critique en mode d'exploitation, d'IFP et d'AD et de le maintenir dans cet état avec une marge appropriée et avec un degré de fiabilité élevé même en présence des conditions les plus réactives du cœur du réacteur* ». Cela comprend habituellement un cœur avec un excédent de réactivité admissible maximum (par exemple, à la suite d'un rechargement de combustible par lots) et les conditions les plus réactives pour la température et la densité du caloporteur et du modérateur (par exemple, en conditions d'état d'arrêt à froid pour un réacteur présentant un coefficient de température de réactivité négatif).

En ce qui concerne les réacteurs CANDU, un accident de perte de réfrigérant primaire (APRP) pourrait se produire dans le cœur, ce qui pose un problème particulier aux systèmes de contrôle de

la réactivité. En particulier, les charges hydrauliques d'un APRP dans le cœur peuvent endommager les guides des barres d'arrêt et éventuellement endommager les buses d'injection du poison. Si un APRP dans le cœur exige une intervention de mise à l'arrêt, la spécification de conception devrait identifier le nombre de dispositifs de réactivité susceptibles d'être endommagés par l'APRP dans le cœur. Ceci devrait correspondre aux hypothèses de l'analyse de sûreté. Il faudrait fournir les résultats de l'analyse de l'ampleur des dégâts et des expériences justificatives.

L'autorité responsable de la conception devrait également fournir les critères de rendement relatifs à la vitesse et à la profondeur des moyens rapides d'arrêt d'urgence du réacteur. Un moyen d'arrêt d'urgence est considéré comme efficace lorsque les critères d'acceptation de l'analyse de la sûreté sont satisfaits. L'autorité responsable de la conception devrait fournir les critères de rendement pour une marge de sous-criticité appropriée du moyen d'arrêt d'urgence.

En ce qui concerne les REO, en particulier les réacteurs à eau sous pression (REP), un APRP grave peut entraîner des charges hydrauliques importantes sur les internes du cœur, comme les guides des barres de commande se trouvant dans le plénum supérieur. Une déformation du cloisonnement du cœur peut entraîner des mauvais alignements. Si l'insertion des barres de commande est validée dans l'analyse de sûreté pour les APRP graves (la plupart des REO ne valident pas le mouvement des barres), la conception devrait démontrer que l'insertion des barres de commande ne sera pas entravée.

8.4.1 Paramètres de déclenchement des systèmes d'arrêt d'urgence

L'efficacité des paramètres de déclenchement est évaluée grâce aux analyses de la sûreté réalisées conformément aux indications du document RD-310, *Analyses de la sûreté pour les centrales nucléaires*. Des indications complémentaires sont fournies dans le guide d'application de la réglementation GD-310, *Document d'orientation sur les analyses de la sûreté des centrales nucléaires*.

Il faudrait démontrer la couverture de déclenchement pour l'ensemble des états d'exploitation, pour tous les moyens d'arrêt d'urgence validés et pour tous les paramètres de déclenchement validés. Il convient de noter que le nombre de moyens d'arrêt d'urgence crédités et que le nombre de paramètres de déclenchement crédités peuvent varier en fonction de l'événement, de la conception du réacteur et de la disponibilité d'un déclenchement direct.

Il appartient à l'autorité responsable de la conception de définir les critères d'acceptation dérivés qui conviennent à une conception particulière. Le document RD-310, *Analyses de la sûreté pour les centrales nucléaires*, fournit des exigences à ce sujet.

Les critères d'acceptation dérivés devraient être définis séparément pour les IFP et les AD. Les critères d'acceptation dérivés devraient être établis pour fournir un niveau de confiance approprié quant au fait qu'une fonction de sûreté fondamentale soit remplie et qu'une barrière contre le rejet de produits de fission ne subira pas de défaillance. Les critères d'acceptation dérivés devraient :

- être quantifiables et bien compris
- tenir compte du fait que l'analyse de la sûreté est stylisée, et que l'état de la centrale au moment de l'accident peut être très différent de l'état analysé
- couvrir les incertitudes dans l'analyse, les paramètres d'entrée de la centrale et de l'analyse, ainsi que la validation des programmes informatiques

Les déclenchements directs sont les méthodes préférées d'actionnement des systèmes d'arrêt d'urgence en raison de leur robustesse et de leur faible dépendance par rapport aux modèles de calcul.

Des paramètres de déclenchement différents mesurent différentes variables physiques du réacteur, assurant par conséquent une protection supplémentaire contre les défaillances de mode commun. Lorsqu'il est pratiquement impossible de fournir toute la diversité des paramètres de déclenchement, il faudrait prévoir différents endroits de mesure, différents types d'instruments et différents ordinateurs de traitement. Le déclenchement manuel est considéré comme un paramètre de déclenchement acceptable si l'opérateur dispose d'un temps suffisant pour amorcer l'action de mise à l'arrêt à la suite d'une indication non-ambiguë de la nécessité d'effectuer l'intervention (conformément à la section 8.10.4 de la version 2 du document RD-337).

Il appartient à l'autorité responsable de la conception d'identifier et de justifier les paramètres de déclenchement qui peuvent être considérés comme « directs ». L'autorité responsable de la conception devrait également démontrer que tout paramètre de déclenchement qui est une mesure de l'événement mais qui n'est pas une mesure d'un enjeu à l'égard des critères d'acceptation, ne peut pas être « masqué » ou « aveuglé » par le fonctionnement du système de contrôle ou par d'autres moyens.

Les déclenchements qui dépendent d'un nombre de variables mesurées, comme les déclenchements à la suite d'un rapport de flux thermique critique (RFTC) faible dans les REO, seront uniquement considérés comme directs si toutes les variables sont directes.

La version 2 du document RD-337 indique que « *pour chaque dispositif d'arrêt d'urgence crédité, la conception doit prévoir un paramètre de déclenchement direct des systèmes d'arrêt d'urgence amorcé en temps opportun pour tous les IFP et les AD satisfaisant aux critères d'acceptation dérivés. Lorsqu'un paramètre de déclenchement direct n'existe pas pour un dispositif crédité donné, il doit y avoir deux paramètres différents de déclenchement indiqués pour ce dispositif.*

Pour tous les IFP et les AD, il doit y avoir au moins deux paramètres de déclenchement différents à moins que l'on puisse démontrer que l'incapacité de déclencher les systèmes d'arrêt d'urgence n'entraînera pas de conséquences inacceptables ».

Le premier paragraphe est interprété comme s'appliquant à chaque dispositif d'arrêt d'urgence crédité dans le dossier de sûreté de la centrale, pour tous les IFP et AD. Il n'exige qu'un seul paramètre de déclenchement, pour autant qu'il soit « direct » par nature. Lorsqu'un paramètre direct n'est pas disponible, ce dispositif crédité doit présenter deux paramètres différents.

Le deuxième paragraphe est interprété pour faire la distinction entre les conceptions de réacteurs :

- les réacteurs à sûreté inhérente : conceptions qui démontrent qu'un IFP ou un AD avec défaillance du moyen rapide d'arrêt d'urgence (IFP sans analyse du déclenchement du réacteur) n'entraînera pas de dommages graves au cœur du réacteur et d'une mise à l'épreuve importante et rapide de l'enveloppe de confinement
- les réacteurs à sûreté spécifiquement conçue : conceptions incapables de démontrer qu'un IFP ou un AD avec défaillance du moyen rapide d'arrêt d'urgence n'entraînera pas de dommages graves au cœur du réacteur et une mise à l'épreuve importante et rapide de l'enveloppe de confinement

Le tableau 3 du guide d'application de la réglementation GD-310, *Document d'orientation sur les analyses de la sûreté des centrales nucléaires*, présente les attentes minimales relatives au nombre de paramètres de déclenchement.

Un déclenchement manuel du réacteur peut être considéré comme équivalent à un paramètre de déclenchement si les exigences relatives à la validation de l'intervention des opérateurs de la salle de commande principale sont respectées (voir la sous-section 8.10.4) et si la fiabilité de la mise à l'arrêt manuelle répond aux exigences en matière de fiabilité d'un déclenchement automatique.

8.4.2 Fiabilité

Tel qu'indiqué à la section 7.6 de la version 2 du document RD-337, « *les systèmes de sûreté et leurs systèmes de support doivent être conçus de manière à ce que la probabilité qu'un système en demande fasse défaut, pour toutes les causes, soit inférieure à 10^{-3}* ».

Les calculs de fiabilité devraient inclure la détection du besoin d'arrêter le réacteur, le déclenchement de la mise à l'arrêt et l'insertion de réactivité négative. Tous les éléments nécessaires pour accomplir la fonction de mise à l'arrêt doivent être inclus.

L'évaluation de la fiabilité devrait faire en sorte que la fonction de mise à l'arrêt présente une fiabilité montrant que la fréquence cumulative de l'échec des demandes de mise à l'arrêt est inférieure à 10^{-5} et que la contribution de toutes les séquences comportant un échec de mise à l'arrêt à la fréquence des grandes émissions radioactives des objectifs de sûreté est inférieure à 10^{-7} /année.

La section 7.6.2 de la version 2 du document RD-337 exige que la fonction de mise à l'arrêt soit exécutée, même en présence d'une défaillance simple et même durant la configuration la plus défavorable attribuable aux essais et à l'entretien. Par exemple, en cas de système reposant sur des barres pour satisfaire au critère de défaillance simple (CDS), l'analyse de la sûreté peut supposer que les deux barres de commande présentant la valeur de réactivité maximale sont indisponibles (l'une en raison des essais et l'autre supposée faire défaut à la demande, conformément au CDS). Dans ce cas, aucun autre essai des barres ne sera permis tant que la barre en cours d'essai ne sera pas disponible.

8.4.3 Surveillance et interventions de l'opérateur

Cette section est traitée de manière suffisante par la version 2 du document RD-337, *Conception des nouvelles centrales nucléaires*. Il n'est donc pas nécessaire de fournir de l'orientation supplémentaire à ce sujet.

8.5 Système de refroidissement d'urgence du cœur du réacteur

Tel qu'indiqué dans la version 2 du document RD-337, « *la conception doit tenir compte des effets sur la réactivité du cœur qu'exerce le mélange de l'eau du RUC avec l'eau de refroidissement du réacteur, y compris le mélange possible attribuable à une fuite interne* ». Par exemple, les REP prévoient souvent du bore soluble dans les accumulateurs et les réservoirs de stockage du système de refroidissement d'urgence du cœur (SRUC) afin de compléter l'insertion des barres de commande pour le contrôle à long terme de la réactivité. L'autorité responsable de la conception devrait décrire toute fonction de contrôle de la réactivité remplie par le SRUC, ainsi que les limites et conditions nécessaires.

Les conceptions du SRUC devraient être éprouvées par des programmes expérimentaux et une modélisation informatique appropriés. Il faudrait démontrer qu'il existe des preuves expérimentales suffisantes de l'efficacité du SRUC.

Les exemples d'éléments pouvant présenter de l'importance pour la conception du SRUC comprennent :

- les mécanismes de contournement du cœur (p. ex. le contournement des conduites de descente en cas de purge dans les REP, ou le contournement du cœur par les générateurs de vapeur dans les réacteurs CANDU)
- les effets des gaz non condensables sur le rendement du SRUC

- les phénomènes pouvant nuire au remplissage et au remouillage du cœur (comme les périodes de stagnation, la formation de bouchons de vapeur dans les générateurs de vapeur des REP, les effets des canaux parallèles dans les réacteurs CANDU)
- l'effet du flux multidimensionnel dans les collecteurs du système de transport de la chaleur des réacteurs CANDU
- l'effet de la résistance non uniforme à l'écoulement dans les canaux dans le cœur des réacteurs CANDU (p. ex. les canaux périphériques à faible écoulement et à faible puissance présentent une résistance plus importante à l'écoulement pour le remplissage du SRUC)
- l'effet sur le pressuriseur

La section 8.5 de la version 2 du document RD-337 exige que le SRUC soit capable d'évacuer la chaleur résiduelle sur une longue période. Cela implique habituellement l'évacuation de l'eau ayant débordé à la suite de la rupture, son refroidissement et son retour dans le réacteur. Il faudrait également démontrer que :

- la conception est capable de faire recirculer l'eau de refroidissement même en présence de la quantité maximale de débris susceptibles d'être présents après un APRP
- les effets chimiques éventuels dans le puisard de récupération du bâtiment du réacteur ont été pris en considération et les précipités et autres espèces chimiques (gels, colloïdes, etc.) éventuels ne peuvent altérer de façon importante le circuit de recirculation du SRUC (par exemple, au niveau des crépines ou des échangeurs de chaleur)
- les interventions de récupération (telles que le transport vers l'injection de la branche chaude du SRUC ou le transport vers le système habituel d'évacuation de la chaleur résiduelle) sont décrites et il est montré qu'elles sont réalisables. L'évacuation à long terme de la chaleur par ébullition dans le cœur pourrait éventuellement provoquer des dépôts ou un encrassement (par exemple la précipitation de cristaux d'acide borique) diminuant l'écoulement et le transfert de chaleur
- l'usure des roulements et des joints d'étanchéité a été prise en considération, y compris l'abrasion causée par de petites particules et la corrosion chimique
- l'écoulement naturel, lorsqu'il est crédité, est capable de fournir une circulation suffisante et ne peut être diminué par des effets tels que l'accumulation de gaz non condensables ou les distributions de température défavorables

Les sections 7.14 et 7.16 de la version 2 du document RD-337 décrivent les exigences relatives aux activités d'inspection, d'essai et d'entretien qui devraient comprendre :

- les essais de mise en service destinés à vérifier le débit, la chute de pression et (le cas échéant) l'isolation des réservoirs après injection pour les accumulateurs et les autres réservoirs d'appoint
- les essais de mise en service destinés à vérifier la charge des pompes, l'écoulement et la chute de pression du système pour l'injection par pompage

Tel qu'indiqué dans la version 2 du document RD-337, « *advenant un accident nécessitant l'injection de liquide de refroidissement d'urgence, l'opérateur ne doit pas pouvoir empêcher la procédure d'injection* ». Ceci peut être réalisé par différentes méthodes pour s'assurer que l'intervention de blocage est intentionnelle (en exigeant par exemple plusieurs interventions, des interventions séquentielles, des interventions séparées dans le temps, ou des interventions qui doivent être exécutées par des personnes différentes).

Les procédures d'exploitation d'urgence devraient interdire le blocage de l'injection du SRUC, à moins d'une indication claire et non ambiguë qu'elle n'est pas nécessaire (par exemple, en cas

d'indication claire de la présence de réserves suffisantes pour assurer le refroidissement du cœur et que les réserves ne sont pas en train de diminuer).

L'injection d'un volume important d'eau froide peut provoquer un choc thermique pressurisé dans l'enveloppe sous pression du système de refroidissement du réacteur, ou une déformation des internes du réacteur. L'autorité responsable de la conception devrait démontrer que le choc thermique a été pris en considération de manière adéquate dans la conception en ce qui concerne le calcul des conditions transitoires des fluides aux endroits clés ainsi que la température des métaux qui en résulte et les contraintes correspondantes.

Les charges dues aux coups de bélier peuvent être produites par l'actionnement de vannes ou par la condensation en cas d'injection d'eau froide dans des systèmes remplis de vapeur. L'autorité responsable de la conception devrait démontrer qu'une évaluation des coups de bélier a été effectuée.

8.6 Confinement

8.6.1 Orientation relative aux exigences générales

La conception devrait établir les critères d'acceptation pour les mesures d'inspection, d'essais et d'entretien, y compris, le cas échéant :

- les durées d'isolation contre les pénétrations du confinement
- le rendement des gicleurs de l'enceinte de confinement
- la capacité des événements à filtre
- l'activation du bâtiment sous vide
- la capacité du système d'atténuation des risques liés à l'hydrogène (p. ex. les recombineurs)
- les systèmes et équipements servant à évacuer la chaleur de l'enceinte de confinement
- l'état du béton et la dégradation éventuelle de celui-ci

Les effets du rejet d'air comprimé dans l'enceinte de confinement après isolation (provenant par exemple de vannes à commande pneumatique) devraient être pris en considération lors du calcul des charges de pression de l'enceinte de confinement.

Renseignements supplémentaires :

D'autres renseignements sont disponibles dans les documents suivants :

- CSA N287.3-93 (2009), *Design Requirements for Concrete Containment Structures for CANDU Nuclear Power Plants* [confirmée en 2009]
- CSA N290.0-11/N290.3-11 COLLECTION – Contient les *General requirements for safety systems of nuclear power plants* et la norme N290.3-11, *Requirements for the containment system of nuclear power plants* [2011]

8.6.2 Résistance de la structure de confinement

La section 8.6.12 de la version 2 du document RD-337 indique que, en plus des exigences particulières relatives aux AD, il convient de tenir compte des conditions liées aux accidents graves afin de fournir une garantie raisonnable quant au fait que l'enceinte de confinement assurera les fonctions créditées dans l'analyse des CAD.

Pour de l'orientation supplémentaire concernant la conception des structures de confinement, consulter la section 7.15.

8.6.3 Capacité relative aux essais de pressurisation

Cette section est traitée de manière suffisante par la version 2 du document RD-337, *Conception des nouvelles centrales nucléaires*. Il n'est donc pas nécessaire de fournir de l'orientation supplémentaire à ce sujet.

8.6.4 Fuites

Limites de débit de fuite

Une enceinte de confinement moderne devrait être à même d'atteindre un débit de fuite inférieur à 0,5 % de la masse d'air de l'enceinte de confinement par jour à la pression maximale de l'enceinte de confinement pour tout AD. Par exemple, les conceptions les plus récentes obtiennent un débit de fuite de 0,1 à 0,5 % de la masse d'air de l'enceinte de confinement par jour à la pression nominale.

La limite nominale de débit de fuite est le débit de fuite maximal permettant de respecter les critères d'acceptation des doses pour tout IFP ou AD. L'enceinte de confinement devrait être conçue avec un débit de fuite nettement plus faible. Des essais de vérification de la conformité réalisés tout au long de la durée de vie du réacteur assurent que le débit de fuite nominal ne sera pas dépassé.

Limites de débit de fuite acceptable en cours d'essai

Cette section est traitée de manière suffisante par la version 2 du document RD-337, *Conception des nouvelles centrales nucléaires*. Il n'est donc pas nécessaire de fournir de l'orientation supplémentaire à ce sujet.

Essai de débit de fuite

Cette section est traitée de manière suffisante par la version 2 du document RD-337, *Conception des nouvelles centrales nucléaires*. Il n'est donc pas nécessaire de fournir de l'orientation supplémentaire à ce sujet.

Renseignements supplémentaires

D'autres renseignements sont disponibles dans les documents suivants :

- CAS N287.6-11, *Pre-operational Proof and Leakage Rate Testing Requirements for Concrete Containment Structures for Nuclear Power Plants* [2011]
- CSA, N287.7-F08, *Exigences relatives à la mise à l'essai et à la vérification, en cours d'exploitation, des enceintes de confinement en béton des centrales nucléaires CANDU* [2008]

8.6.5 Pénétrations de l'enceinte de confinement

Tel qu'indiqué dans la version 2 du document RD-337, « le nombre de pénétrations dans l'enceinte de confinement doit être maintenu à un niveau minimal ». Le respect de cette exigence devrait envisager le besoin de séparation et de redondance et être conforme aux conceptions les plus récentes.

8.6.6 Isolation du confinement

Cette section est traitée de manière suffisante par la version 2 du document RD-337, *Conception des nouvelles centrales nucléaires*. Il n'est donc pas nécessaire de fournir de l'orientation supplémentaire à ce sujet.

8.6.7 Sas du confinement

Les ouvertures de l'enceinte de confinement destinées à faire passer des équipements ou des matières devraient être conçues afin d'être fermées de façon rapide et fiable en cas de besoin d'isoler l'enceinte de confinement.

Le besoin d'accès à l'enceinte de confinement par le personnel devrait être réduit le plus possible. À la suite d'un accident, il ne devrait pas être nécessaire d'accéder à l'enceinte de confinement pour assurer la sûreté de l'installation (à court ou à long terme).

8.6.8 Structures internes du confinement

Il faudrait utiliser des méthodes acceptables pour calculer les différences de pression et démontrer que les structures porteuses et les systèmes de sûreté ne subiront pas de perte des fonctions de sûreté en cas d'IFP et en conditions d'accident (y compris les considérations relatives à l'hydrogène). En particulier, les analyses d'un APRP grave, de la rupture de la canalisation de vapeur principale et du séisme de référence devraient aboutir à des conditions difficiles. Les hypothèses des analyses devraient assurer qu'elles sont prudentes en ce qui concerne la pression de l'enceinte de confinement, les différences de pression entre les compartiments et la distribution de l'hydrogène, ainsi que les fonctions de sûreté des SSC.

Il faudrait prévoir des ouvertures suffisantes entre les compartiments de manière à éviter l'accumulation potentielle d'hydrogène dans les impasses. Le cas échéant, il faudrait tenir compte de phénomènes tels que l'accélération de flamme et les flammes fixes.

Les structures internes devraient fournir des moyens adéquats de renvoi du liquide de refroidissement dans le circuit de recirculation (p. ex. vers le puisard de l'enceinte de confinement en cas de rupture de conduite) lorsqu'ils sont validés dans l'analyse de la sûreté. Il faudrait tenir compte de l'obstruction éventuelle des voies d'écoulement par des débris.

Pour de l'orientation supplémentaires concernant la conception des structures internes, consulter la section 7.15.

Renseignements supplémentaires

D'autres renseignements sont disponibles dans le document suivant :

- CSA N291-08, *Exigences relatives aux enceintes reliées à la sûreté des centrales nucléaires CANDU* [mai 2009]

8.6.9 Pression de l'enceinte de confinement et gestion de l'énergie

Les moyens permettant d'évacuer la chaleur et de réduire la pression dans l'enceinte de confinement peuvent varier considérablement d'une conception à l'autre et peuvent faire appel à des systèmes tels que :

- les piscines de suppression de pression, les condenseurs à glace, les chambres à vide
- les refroidisseurs et les ventilateurs de l'enceinte de confinement
- les systèmes de refroidissement de l'eau des puisards ou de l'enceinte de confinement utilisés dans le cadre de la recirculation après un APRP
- le refroidissement passif de l'enceinte de confinement
- les systèmes de pulvérisation ou d'aspersion de l'enceinte de confinement
- le volume libre à l'intérieur du bâtiment du réacteur

- mise à l'air de l'enceinte de confinement au travers de filtres ou de laveurs

L'équipement crédité dans les AD est traité dans le cadre du système de confinement. Par exemple, lorsqu'ils sont crédités, les moteurs de ventilateurs devraient être conçus pour fonctionner en conditions post-accidentelles présentant des gaz combustibles.

Pour les AD, toutes les sources de chaleur devraient être prises en considération, y compris la combustion des gaz, les réactions métal-eau et la formation de solutions solides (y compris les eutectiques). La conception devrait s'assurer que la capacité d'évacuation de la chaleur correspond à l'analyse des conditions de l'enceinte de confinement.

Les systèmes d'alimentation en air (destinés par exemple à l'air d'instrumentation et à l'air respirable) devraient être isolés de façon fiable après un événement initiateur hypothétique nécessitant l'isolation de l'enceinte de confinement afin d'éviter la surpression de l'enceinte de confinement et de réduire les effets de la combustion et des explosions.

8.6.10 Contrôle et nettoyage de l'atmosphère de l'enceinte de confinement

Cette section est traitée de manière suffisante par la version 2 du document RD-337, *Conception des nouvelles centrales nucléaires*. Il n'est donc pas nécessaire de fournir de l'orientation supplémentaire à ce sujet.

8.6.11 Revêtements et matériaux

L'autorité responsable de la conception devrait s'assurer que les revêtements et les matériaux interfèrent le moins possible avec les fonctions de sûreté et les autres systèmes de sûreté. En voici des exemples :

- les matériaux d'isolation, les produits de corrosion, le délaminage des peintures et des revêtements susceptibles d'encrasser les circuits de recirculation du RUC ou d'empêcher le fonctionnement de l'équipement
- l'utilisation de matériaux d'étanchéité caoutchoutés pouvant fondre ou présenter d'autres défaillances et provoquer des fuites supplémentaires au niveau de l'enceinte de confinement ou la défaillance d'un composant ou d'un système lié à la sûreté
- les matériaux pouvant réagir en conditions post-accidentelles et produire des gaz combustibles, corrosifs ou toxiques

Quand des structures de grande taille situées dans l'enceinte de confinement sont créditées en tant que sources froides lors du calcul des pressions et des températures post-accidentelles dans l'enceinte de confinement, les calculs devraient utiliser des renseignements fiables sur les produits de revêtement et leurs propriétés thermiques.

8.6.12 Conditions additionnelles de dimensionnement

Les dispositions relatives aux conditions additionnelles de dimensionnement (CAD) varient considérablement d'une conception à l'autre. La fonctionnalité et l'analyse revendiquées devraient être appuyées par des preuves suffisantes.

Le débit de fuite de l'enceinte de confinement en CAD ne dépasse pas le débit de fuite nominal pendant une période suffisante pour permettre la mise en œuvre des mesures d'urgence hors site. Il faudrait démontrer avec une certitude raisonnable que cette période sera d'au moins 24 heures.

La conception de la mise à l'air de l'enclume de confinement devrait tenir compte de facteurs tels que :

- l'inflammation de gaz inflammables
- l'incidence sur les filtres des conditions environnementales de l'enclume de confinement, telles que les matières radioactives, des températures élevées et un degré d'humidité élevé

Il faudrait fournir des preuves expérimentales et des données analytiques pour démontrer que la mise à l'air n'entraînera pas de rejets non filtrés et incontrôlés de matières radioactives dans l'environnement.

8.7 Transfert de chaleur vers une source froide ultime

Les exigences de fiabilité et d'importance sur le plan de la sûreté en ce qui a trait au transfert de chaleur vers une source froide ultime devraient être traitées en tenant compte de toute déclaration formulée dans le dossier de sûreté quant à leur disponibilité pour assurer le refroidissement dans les états de fonctionnement et en conditions d'accident.

8.8 Système d'évacuation d'urgence de la chaleur

Le système d'évacuation d'urgence de la chaleur est destiné à fournir un mode de transfert vers la source froide ultime en cas d'indisponibilité des capacités normales d'évacuation de la chaleur. Ce système a pour but d'empêcher l'escalade des conditions d'accident et d'atténuer les conséquences de celles-ci.

L'évacuation d'urgence de la chaleur concerne l'évacuation de la chaleur à la suite d'un accident et peut être assurée par un certain nombre de systèmes, en fonction des circonstances :

- l'évacuation de la chaleur à la suite d'un APRP peut être assurée par le SRUC (consulter la section 8.5)
- en ce qui concerne les événements non liés à un APRP, l'évacuation d'urgence de la chaleur peut se faire par le truchement des systèmes de refroidissement primaires ou secondaires

Pour tous les moyens d'évacuation d'urgence de la chaleur, la conception devrait faire en sorte que tout l'équipement est conçu de manière adéquate pour fonctionner dans la classe d'accidents pour lesquels il est validé.

Si le système validé joue un autre rôle en mode d'exploitation normale, alors la conception devrait faire en sorte que le système respectera les exigences relatives à un système de sûreté lorsque celui-ci est utilisé en conditions d'accident. Le dimensionnement du système dans ce rôle devrait être fourni.

De nombreuses actions liées au fonctionnement des systèmes validés pour l'évacuation d'urgence de la chaleur peuvent ne pas être enclenchées automatiquement. En cas de dépendance par rapport au fonctionnement manuel, il faudrait accorder beaucoup d'importance à l'examen des facteurs humains.

L'évacuation d'urgence de la chaleur du côté primaire pourrait se faire à l'aide des moyens normaux de refroidissement à l'arrêt. La conception devrait faire en sorte que :

- un moyen de dépressurisation du système primaire est prévu et le moyen de dépressurisation répond aux exigences relatives aux systèmes de sûreté; ou

- le système de refroidissement à l'arrêt est capable de fonctionner aux niveaux de pression et de température du circuit primaire

Il est possible d'utiliser des moyens d'évacuation de la chaleur passifs ou actifs (p. ex. circulation naturelle ou circulation par pompe). Les systèmes actifs exigent une alimentation électrique d'urgence. Il faudrait démontrer que les systèmes à circulation naturelle sont capables de fonctionner dans toutes les conditions d'exploitation applicables.

L'évacuation d'urgence de la chaleur du côté secondaire qui dépend de l'eau fournie au côté secondaire des générateurs de vapeur peut se faire à l'aide d'une alimentation par pompage séparée ou à l'aide d'une dépressurisation secondaire et d'une alimentation par gravité. L'alimentation en eau répond aux exigences relatives aux systèmes de sûreté.

8.9 Systèmes d'alimentation électrique

Conception des systèmes d'alimentation électrique

Il faudrait adopter une approche systématique pour identifier les systèmes d'alimentation électrique permettant d'assurer que les SSC nécessaires à l'exécution des fonctions de sûreté sont alimentés par des sources d'électricité présentant une classification de sûreté et une fiabilité adéquates.

Il faudrait spécifier les fondements de conception, les critères de conception, les documents d'application de la réglementation, les normes et les autres documents qui seront utilisés pour concevoir les systèmes d'alimentation électrique.

Les fondements de conception de chaque système d'alimentation électrique devraient inclure :

- la prise en considération de tous les modes d'exploitation, des états de la centrale jusqu'aux CAD, et de tous les événements crédibles qui pourraient avoir une incidence sur les systèmes d'alimentation électrique
- la fiabilité et les objectifs de disponibilité des systèmes et des principaux équipements
- les exigences en matière de capacité et de rendement
- l'identification de toutes les charges (c.-à-d. les systèmes et équipements qui ont besoin d'électricité pour remplir leurs fonctions de sûreté), y compris les caractéristiques électriques, les conditions de demande maximale et la classification de sûreté
- les dispositifs de protection et la coordination de la protection
- la spécification des gammes de tensions et de fréquences acceptables pour le fonctionnement continu des charges connectées pour chaque système d'alimentation électrique
- l'identification des gammes acceptables de perturbations temporaires survenant sur le site et hors du site, susceptibles d'avoir une incidence sur les systèmes d'alimentation électrique

La conception devrait spécifier les exigences relatives à l'alimentation électrique préférée (AEP) (c.-à-d. les sources normales de courant alternatif des circuits électriques de la centrale importants pour la sûreté) et à l'interface de la centrale avec le réseau de distribution afin de réduire les risques de perte des sources normales d'alimentation en courant alternatif.

Il faudrait entreprendre des études du réseau de transport concernant les conditions et perturbations raisonnablement prévisibles du réseau électrique afin de démontrer que les sources normales d'alimentation en courant alternatif ne seront pas détériorées à un niveau posant des difficultés inutiles aux systèmes de sûreté et aux systèmes d'alimentation électrique de relève et d'urgence. Il faudrait établir les critères de rendement des éléments suivants :

- le rendement des génératrices durant des excursions de fréquence et de tension définies afin d'assurer que les génératrices restent reliées au réseau électrique
- des mesures de conception contre la foudre et les surtensions afin de protéger les systèmes de distribution électrique de la centrale contre les conditions de surtension temporaire comme celles causées par la foudre ou les commutations

Les systèmes d'alimentation électrique normale en CA devraient avoir la capacité d'alimenter toutes les charges électriques de la centrale dans les états de fonctionnement et en conditions d'accident.

Les alimentations électriques normales en CA devraient être conçues pour :

- empêcher les écarts par rapport à l'exploitation normale
- éviter que des défaillances simples ne touchent plus d'une division redondante d'alimentation électrique
- éviter de poser des difficultés évitables aux systèmes d'alimentation électrique de relève et d'urgence en raison d'une perturbation du système électrique, d'une condition temporaire ou d'une excursion de puissance (p. ex. déclenchement du groupe turbo-alternateur)

L'alimentation électrique en provenance de l'extérieur et alimentant le circuit électrique sur le site devrait être assurée par au moins deux lignes de transport d'électricité physiquement indépendantes, conçues et situées afin de minimiser la probabilité de leur défaillance simultanée. L'analyse de la sûreté devrait fournir des renseignements sur les circuits de puissance hors site venant du réseau de transport vers le poste de manœuvre de la centrale. Un poste de manœuvre commun aux deux circuits est acceptable, mais il faudrait utiliser des pylônes de lignes de transport séparés. Pour certaines conceptions de réacteurs, il est possible de justifier qu'un seul raccordement électrique hors site est suffisant.

Chacune des lignes de transport hors site de la centrale devrait avoir la capacité d'alimenter toutes les charges électriques de la centrale pour tous les états de la centrale.

La conception devrait prévoir au moins une ligne de transport hors site et l'AEP connexe automatiquement disponibles pour fournir de l'électricité aux divisions de sûreté correspondantes dans les secondes qui suivent un IFP ou un AD.

Un deuxième circuit d'AEP devrait être conçu pour être disponible dans un laps de temps correspondant à l'exigence d'appuyer les fonctions de sûreté de la centrale durant les IFP ou les AD.

Pour les centrales conçues pour fonctionner en îlotage, le système d'alimentation électrique normale en courant alternatif devrait être conçu pour répondre aux excursions de fréquence et de tension de la génératrice liées au passage du mode d'exploitation normale au mode d'exploitation en îlotage.

Renseignements supplémentaires

D'autres renseignements sont disponibles dans les documents suivants :

- Norme CSA N290.5-F06 (R2011), *Exigences relatives aux systèmes d'alimentation électrique et en air d'instrumentation des centrales nucléaires CANDU* (confirmée en 2011) (Remarque : la norme CSA N290.5 est un document propre aux centrales CANDU qui traite particulièrement de la philosophie de conception des « deux groupes »)
- IEEE 308-2001, *IEEE Standard Criteria for Class 1E Power Systems for Nuclear Power Generating Stations* [2001]
- IEEE 387-1995, *IEEE Standard Criteria for Diesel-Generator Units Applied as Standby Power Supplies for Nuclear Power Generating Stations* [1995]
- IEEE 141-1993, *IEEE Recommended Practice for Electric Power Distribution for Industrial Plants*, (Red Book) [1993]
- IEEE 242-2001, *IEEE Recommended Practice for Protection and Coordination of Industrial and Commercial Power Systems*, (IEEE Buff Book) [2001]
- IEEE 279-1971, *IEEE Standard: Criteria for Protection Systems for Nuclear Power Generating Stations* [1971]
- IEEE 665-1995, *IEEE Standard for Generating Station Grounding* [confirmée en 2010]
- IEEE 1050-1996, *Guide for Instrumentation and Control Equipment Grounding in Generating Stations* [1996]
- IEEE C62.23-1995, *IEEE Application Guide for Surge Protection of Electric Generating Plants*

8.9.1 Systèmes d'alimentation électrique de relève et d'urgence

Les sources d'alimentation électrique de relève et d'urgence devraient être constituées de groupes électrogènes complets comprenant tous les auxiliaires de soutien, une source d'énergie emmagasinée pour le démarrage et un circuit d'alimentation en carburant dédié et indépendant avec stockage sur le site.

La source d'énergie emmagasinée destinée au démarrage des sources d'alimentation de relève et d'urgence devrait avoir suffisamment d'énergie emmagasinée pour cinq tentatives de démarrage successives.

Systèmes d'alimentation en courant continu (CC)

Les systèmes d'alimentation en courant continu (CC) importants pour la sûreté devraient être conçus pour être indépendants des effets des AD auxquels ils doivent répondre et être parfaitement fonctionnels pendant et après des accidents.

Chacun des groupes de charge redondants devrait avoir une division d'alimentation en CC constituée d'une ou de plusieurs batteries, un ou plusieurs chargeurs de batteries, un système de distribution, et des dispositifs de protection et d'isolation.

Chaque division d'alimentation en CC devrait être indépendante et séparée physiquement des autres divisions d'alimentation en CC.

Chaque ensemble de batteries devrait être capable, sans l'aide d'un chargeur de batterie, de répondre à toutes les demandes et conditions de charge requises pour un temps de mission déterminé (y compris les cycles de fonctionnement et les transitoires électriques) durant les états de

la centrale spécifiés dans le dimensionnement, en tenant compte de facteurs tels que les marges de conception, les effets de la température, les décharges récentes éventuelles et le vieillissement.

Chaque chargeur de batteries devraient avoir une capacité suffisante pour :

- maintenir la batterie à pleine charge durant l'exploitation normale
- remettre une batterie entièrement déchargée (c.-à-d. la limite inférieure de tension du cycle de décharge de la batterie) à pleine charge dans un laps de temps prédéfini tout en fournissant la demande de charge maximale en CC

Les chargeurs de batteries devraient être conçus pour éviter que les transitoires sur l'alimentation en courant alternatif ne nuisent au fonctionnement du système en CC, et que les transitoires en CC ne nuisent à l'alimentation en courant alternatif.

Tel qu'indiqué dans la version 2 du document RD-337, « *les systèmes d'alimentation électrique doivent comprendre des installations appropriées de protection, de contrôle, de surveillance et d'essais* » pour effectuer des essais périodiques de capacité pour les temps de mission requis.

Systèmes d'alimentation sans coupure en CA

Les systèmes d'alimentation en courant alternatif sans coupure importants pour la sûreté devraient être conçus pour être indépendants des effets des accidents de dimensionnement auxquels ils doivent répondre et être parfaitement fonctionnels pendant et après de tels accidents.

Chaque division des systèmes d'alimentation sans coupure en CA devrait comporter :

- une alimentation en CA et une alimentation en CC vers un onduleur
- une alimentation en CA venant de la même division
- un dispositif assurant la commutation automatique entre la sortie de l'onduleur et l'alimentation en CA séparée

Les caractéristiques électriques et les exigences relatives aux charges connectées devraient être prises en considération dans la conception afin que les interactions avec le système d'alimentation en CA sans coupure ne dégradent pas les fonctions de support de la sûreté des charges fournies.

Les systèmes d'alimentation en CA sans coupure devraient être conçus pour éviter que les transitoires sur l'alimentation en CA ne nuisent au chargeur de batteries ou que les transitoires sur l'alimentation en CC vers l'onduleur ne nuisent au fonctionnement de l'onduleur.

8.9.2 Source d'alimentation de remplacement en CA

La capacité de la centrale à maintenir les paramètres critiques (réserves de fluide caloporteur du réacteur, température et pression de l'enceinte de confinement, températures des pièces abritant des équipements critiques) et à évacuer la chaleur résiduelle du combustible irradié devrait être analysée pour la période durant laquelle la centrale se trouve en situation de perte d'électricité totale (PET).

Il faudrait évaluer la pertinence de la capacité des circuits de CC requis pour surveiller les paramètres critiques et alimenter les systèmes d'éclairage et de communication en cas de PET.

8.10 Salles de commande

8.10.1 Salle de commande principale

La salle de commande principale (SCP) devrait présenter des affichages suffisants pour surveiller toutes les fonctions de sûreté.

La conception devrait empêcher les interventions manuelles dangereuses (p. ex. en utilisant un verrouillage logique en fonction de l'état de la centrale).

Lorsque des systèmes liés à la sûreté et des systèmes non liés à la sûreté sont très rapprochés les uns des autres, la conception devrait maintenir une isolation fonctionnelle et une séparation physique adéquates.

Tel qu'indiqué dans la version 2 du document RD-337, « *pour tout EIH, au moins une salle de commande doit être habitable et accessible par une voie qualifiée* ». Ceci indique qu'en situations d'urgence, des parcours adéquats permettront au personnel d'une salle de commande de quitter la zone en toute sécurité et de se rendre dans une autre salle de commande.

Des mesures appropriées sont prises (y compris la mise en place de barrières entre la salle de commande et le milieu extérieur) et des informations sont fournies pour protéger les occupants de la salle de commande contre les dangers tels que les niveaux de rayonnement élevés résultant des conditions d'accident, le rejet de matières radioactives, un incendie, ou des gaz explosifs ou toxiques.

Le déclenchement manuel d'une fonction de sûreté fournit une forme de défense en profondeur en conditions anormales (y compris la défaillance d'origine commune des systèmes automatiques de contrôle et de protection) et permet l'exploitation à long terme à la suite d'un accident. Il faudrait prévoir un déclenchement manuel au niveau du système et au niveau des composants, le cas échéant.

L'affichage et le contrôle manuel des fonctions de sûreté critiques déclenchées par l'opérateur devraient être différents de ceux des systèmes de sûreté automatiques commandés par ordinateur.

La SCP, la salle de commande auxiliaire (SCA) et le centre de soutien d'urgence (CSU) devraient avoir au moins deux liaisons différentes permettant de communiquer l'un avec l'autre, et également avec :

- les zones où des communications sont requises en cas d'IFP ou en conditions d'accident
- les services d'urgence hors site
- les installations connexes

Les différents moyens de communication comportent entre autres les téléphones standards, les téléphones alimentés par batterie et les téléphones auto-alimentés.

Les différents moyens de communication cités ci-dessus devraient être :

- installés de manière à ne pas être affectés par la même défaillance, des incendies ou un EIH
- capables de fonctionner en cas d'interruption des systèmes d'alimentation électrique de provenance intérieure et extérieure

8.10.1.1 Système d'affichage des paramètres de sûreté

La fonction primaire du système d'affichage des paramètres de sûreté (SAPS) est de servir d'aide aux opérateurs pour détecter rapidement les conditions anormales en fournissant un affichage des paramètres de la centrale permettant d'évaluer l'état de sûreté de l'exploitation dans la salle de commande. Le système d'affichage peut inclure d'autres fonctions qui aident le personnel d'exploitation à évaluer l'état de la centrale. La conception du système d'affichage devrait être souple afin de permettre l'incorporation future de concepts de diagnostic et de techniques d'évaluation perfectionnés.

Le SAPS devrait afficher un ensemble minimal de paramètres de la centrale ou de variables dérivées permettant d'évaluer l'état de sûreté de la centrale. Ces paramètres et variables comprennent :

- le contrôle de la réactivité
- le refroidissement du cœur du réacteur et du combustible irradié
- l'évacuation de la chaleur du système primaire
- l'intégrité du système de refroidissement du réacteur
- le contrôle de la radioactivité
- l'intégrité de l'enceinte de confinement

Le SAPS devrait :

- présenter une disponibilité et une fiabilité suffisantes
- ne pas afficher de données ou d'alarmes non fiables ou non valides
- être conçu pour répondre aux exigences relatives à la facilité d'utilisation et aux facteurs humains

L'affichage des conditions d'exploitation anormales importantes sur le plan de la sûreté devrait avoir un aspect nettement différent de l'affichage représentant les conditions d'exploitation normale.

L'information affichée par l'écran du SAPS devrait être présentée de manière à faciliter la lecture et la compréhension des opérateurs.

L'affichage devrait être conçu pour améliorer la reconnaissance, la compréhension et la détection des états de fonctionnement anormaux par l'opérateur.

8.10.2 Salle de commande auxiliaire

Des commandes, des indications, des alarmes et des affichages suffisants devraient être prévus dans la SCA pour placer la centrale dans un état sûr, pour fournir l'assurance qu'un état sûr a été atteint et est maintenu, et pour fournir aux opérateurs des renseignements sur l'état de la centrale et les tendances des principaux paramètres de celle-ci.

Des dispositions adéquates devraient être prises hors de la SCP pour transférer le contrôle à la SCA chaque fois que la SCP est abandonnée.

Consulter la section 8.10.1 pour les autres orientations et attentes applicables en matière de conception.

8.10.3 Centre de soutien d'urgence

La conception prévoit un centre de soutien d'urgence (CSU) pour faciliter les fonctions suivantes :

- la gestion de l'intervention globale en cas d'urgence
- la coordination des activités de surveillance radiologique et environnementale
- la détermination des mesures recommandées pour protéger le public
- la coordination des activités d'intervention d'urgence avec les organismes fédéraux, provinciaux et municipaux

Des installations devraient être prévues dans le CSU pour l'acquisition, l'affichage et l'évaluation de toutes les données radiologiques et météorologiques ainsi que des données relatives aux systèmes de la centrale permettant de déterminer les mesures de protection hors site.

Les installations utilisées pour exécuter les fonctions essentielles du CSU devraient être situées au sein du complexe du CSU. Toutefois, des calculs supplémentaires et un soutien analytique des évaluations du CSU peuvent être fournis par des installations situées à l'extérieur du CSU.

Le système de données du CSU devrait être conçu pour obtenir un niveau de fiabilité adéquat.

L'emplacement du CSU devrait veiller à assurer des caractéristiques optimales sur le plan fonctionnel et de la fiabilité pour accomplir ses fonctions.

8.10.4 Directives relatives à l'équipement en cas d'accidents

La conception devrait s'assurer qu'aucune défaillance des systèmes de surveillance et d'affichage n'influencera le fonctionnement d'autres systèmes de sûreté.

Tel qu'indiqué dans la version 2 du document RD-337, « si l'intervention de l'opérateur est requise pour actionner tout équipement d'un système de sûreté ou d'un système de support, à la suite d'une alerte indiquant la nécessité d'une intervention de l'opérateur dans les salles de commande, une période minimale de 30 minutes est accordée avant que l'intervention de l'opérateur soit requise ».

Le temps accordé pour réaliser les interventions devrait être fondé sur l'analyse de la réponse de la centrale en cas d'IFP et en conditions d'accident, en utilisant des hypothèses réalistes. Le temps requis pour l'intervention de l'opérateur devrait être fondé sur une analyse de l'ingénierie des facteurs humains (IFH) du temps de réponse de l'opérateur qui (à son tour) repose sur une séquence documentée des interventions de l'opérateur. Les incertitudes de l'analyse du temps requis sont identifiées et évaluées. Il faudrait également ajouter une marge temporelle adéquate au temps analysé.

Si l'intervention de l'opérateur est requise pour actionner une fonction de sûreté mais qu'elle ne satisfait pas aux exigences de la version 2 du document RD-337, l'analyse devrait également démontrer que :

- l'opérateur disposera de suffisamment de temps pour exécuter l'intervention manuelle requise
- l'opérateur peut exécuter les interventions de façon correcte et fiable dans le délai accordé

La séquence des interventions devrait uniquement utiliser les alarmes, les contrôles et les affichages qui seraient disponibles aux endroits où les tâches seront réalisées et devraient être disponibles dans tous les scénarios analysés. Il faudrait procéder à une validation préliminaire pour fournir une confirmation indépendante de la validité du « temps disponible » estimé et du « temps nécessaire » pour accomplir les interventions humaines. Les résultats de la validation préliminaire devraient

étayer la conclusion selon laquelle le temps nécessaire (y compris la marge) pour exécuter les étapes individuelles et la séquence globale documentée des interventions manuelles de l'opérateur est raisonnable, réaliste, reproductible et limité par l'analyse initiale.

Il faudrait également procéder à un essai du système intégré afin de valider les interventions manuelles créditées dans l'analyse de la sûreté, en utilisant un simulateur à échelle réelle. Les tâches réalisées hors de la salle de commande devraient être incorporées dans les validations du système intégré.

Renseignements supplémentaires

D'autres renseignements sont disponibles dans les documents suivants :

- CSA N290.4-11, *Requirements for Reactor Control Systems of Nuclear Power Plants* [2011]
- CEI 60964-2009, *Centrales nucléaires de puissance – Salles de commande – Conception* [2009]
- CEI 60965-2009, *Centrales nucléaires de puissance – Salles de commande – Points de commande supplémentaires pour l'arrêt des réacteurs sans accès à la salle de commande principale (salle de commande de repli)* [juillet 2009]
- U.S. NRC NUREG-0696, *Functional Criteria for Emergency Response Facilities* [1981]

8.11 Traitement et contrôle des déchets

8.11.1 Contrôle des rejets liquides dans l'environnement

Cette section est traitée de manière suffisante par la version 2 du document RD-337, *Conception des nouvelles centrales nucléaires*. Il n'est donc pas nécessaire de fournir de l'orientation supplémentaire à ce sujet.

8.11.2 Contrôle des matières présentes dans l'air à l'intérieur de la centrale

Des zones radiologiques peuvent être établies dans la conception de la centrale nucléaire, en fonction des risques de contamination potentielle dans chaque zone. Le système de ventilation devrait être conçu de manière à ce que tout mouvement d'air entre les différentes zones, causé par une différence de pression, se produise d'une zone moins contaminée vers une zone dont le niveau de contamination augmente. La recirculation de l'air à l'intérieur d'une zone ou d'une pièce peut être autorisée, mais pas la recirculation au départ du système de ventilation central.

8.11.3 Contrôle des rejets gazeux dans l'environnement

Un système de gestion des déchets gazeux est conçu pour recueillir tous les gaz, vapeurs et particules volatiles actifs ou potentiellement actifs éventuellement présents afin de surveiller et de filtrer les effluents avant de les rejeter dans l'atmosphère. Les unités de filtration devraient être placées dans une pièce complètement fermée avec des murs et des sols en béton suffisamment épais de manière à protéger le personnel de la centrale contre les rayonnements. Des appareils de surveillance sont prévus dans la cheminée pour détecter toute activité présente dans les effluents. L'activité des gaz provenant de zones telles que les piscines de stockage du combustible, les zones de service et les laboratoires actifs est également surveillée et ces gaz sont filtrés avant d'être rejetés dans l'atmosphère.

Renseignements supplémentaires

D'autres renseignements sont disponibles dans les documents suivants :

- CCSN, G-129, *Maintenir les expositions et les doses au « niveau le plus bas qu'il soit raisonnablement possible d'atteindre (ALARA) »* [2004]
- CSA N292.3-08, *Gestion des déchets radioactifs de faible et de moyenne activité* [2008]
- AIEA, collection Normes de sûreté n° GS-G-3.3, *The Management System for the Processing, Handling and Storage of Radioactive Waste Safety Guide* [2008]

8.12 Manutention et stockage du combustible

La conception prévoit le fondement des systèmes de manutention et de stockage du combustible. La conception comprend des dispositions pour la surveillance et les alarmes, pour la prévention des incidents de criticité, et pour l'écran de blindage, la manutention, le stockage, le refroidissement, le transfert et le transport du combustible nucléaire.

Des facteurs tels que l'emballage, les systèmes de comptabilisation du combustible, le stockage, la prévention des incidents de criticité, le contrôle de l'intégrité du combustible, les procédures d'exclusion des matières étrangères et la sécurité du combustible, devraient être pris en compte dans la conception.

Les exigences relatives à la sûreté-criticité sont expliquées dans le document d'application de la réglementation RD-327, *Sûreté en matière de criticité nucléaire*. Des directives détaillées et des références techniques complètes sur la sûreté-criticité sont fournies par le document d'orientation GD-327, *Directives de sûreté en matière de criticité nucléaire*.

La conception devrait comprendre des dispositions pour prévenir la contamination du combustible par des matières étrangères (graisses, « uranium baladeur », etc.) et éviter la propagation de la contamination dans le réacteur.

Renseignements supplémentaires

D'autres renseignements sont disponibles dans les documents suivants :

- AIEA NS-G-1.4, *Design of Fuel Handling and Storage Systems for Nuclear Power Plants* [2003]
- AIEA NS-G-2.5, *Core Management and Fuel Handling for Nuclear Power Plants* [2002]
- ANSI/ANS-57.1-1992, American National Standard *Design Requirements for Light Water Reactor Fuel Handling Systems* (le cas échéant applicable) [1992]

8.12.1 Manutention et stockage de combustible non irradié

Cette section est traitée de manière suffisante par la version 2 du document RD-337, *Conception des nouvelles centrales nucléaires*. Il n'est donc pas nécessaire de fournir de l'orientation supplémentaire à ce sujet.

8.12.2 Manutention et stockage de combustible irradié

L'atténuation des risques liés à l'hydrogène est particulièrement importante dans la zone des piscines de stockage du combustible irradié si l'on envisage d'utiliser éventuellement la piscine pour l'épuration des produits de fission, dans le cadre de la mise à l'air de l'enceinte de confinement.

8.12.3 Détection de combustible défectueux

Tel qu'indiqué dans la version 2 du document RD-337, « *la conception doit prévoir un moyen pour détecter de façon fiable les défauts du combustible dans le réacteur et enlever subséquemment ledit combustible si les niveaux d'intervention possibles sont dépassés* ».

La conception devrait spécifier le critère utilisé pour décider de poursuivre l'exploitation avec du combustible défectueux dans le cœur ou de décharger l'assemblage de combustible du cœur. La quantité de combustible défectueux laissée dans le cœur peut avoir une incidence sur le dossier de sûreté de la conception.

La conception devrait permettre de retirer le combustible défectueux aussi rapidement que possible. La conception devrait prévoir l'inspection et la mise en quarantaine du combustible défectueux dans les installations de manutention et de stockage du combustible.

8.13 Radioprotection

La centrale nucléaire devrait être divisée en zones fondées sur les débits de dose prévus, les niveaux de contamination radioactive, la concentration de radionucléides en suspension dans l'air, les exigences relatives à l'accès et des exigences particulières (telles que le besoin de séparer les trains de sûreté). Il faudrait fournir les critères et les justifications utilisés pour la désignation des zones de rayonnement (y compris les limites des zones prévues pour l'exploitation normale, le rechargement et en conditions d'accident). Les critères devraient servir de fondement pour la conception des blindages contre les rayonnements.

Du point de vue de la radioprotection, il faudrait soigneusement évaluer les exigences relatives à l'accès pour l'exploitation, l'inspection, l'entretien, la réparation, le remplacement et le déclassement des équipements. Ces considérations devraient être incorporées dans la conception. La conception devrait également prévoir un espace permettant de déposer les outils spéciaux et de faciliter les activités d'entretien. La conception devrait également prévoir des éléments tels que des plateformes ou des passerelles, des escaliers ou des échelles permettant un accès rapide pour l'entretien ou l'inspection des composants situés dans les zones à niveau de rayonnement plus élevé.

Il faudrait envisager et incorporer l'utilisation de techniques d'entretien et de surveillance à distance dans les zones à haut niveau de rayonnement. Il faudrait de préférence utiliser des caractéristiques de conception et des contrôles techniques appropriés plutôt que des processus ou des contrôles administratifs.

Il faudrait choisir des équipements fiables nécessitant un minimum de surveillance, d'entretien, d'essais et d'étalonnages.

Les critères et les justifications prévus par la conception devraient refléter l'expérience en exploitation.

Renseignements supplémentaires

D'autres renseignements sont disponibles dans les documents suivants :

- AIEA, collection Normes de sûreté n° NS-G-1.13, *Radiation Protection Aspects of Design for Nuclear Power Plants - Safety Guide* [2005]
- CCSN, G-129, *Maintenir les expositions et les doses au « niveau le plus bas qu'il soit raisonnablement possible d'atteindre (ALARA) »* [2004]
- AIEA, Guide de sûreté n° RS-G-1.1, *Radioprotection professionnelle* [2004]

8.13.1 Conception relative à la radioprotection

Le blindage devrait être conçu en se fondant sur la délimitation des zones décrite à la section 8.13. Il faudrait fournir les critères de conception du blindage (y compris la méthode utilisée pour les paramètres de protection et le choix des matériaux du blindage). En établissant les spécifications du blindage, il faudrait tenir compte de l'accumulation de matières radioactives au cours de la durée de vie de la centrale nucléaire.

8.13.2 Contrôle de l'accès et des déplacements

Il faudrait prendre des dispositions pour contrôler la sortie (ou les sorties) des zones de rayonnement. Il faudrait établir une surveillance du personnel et du matériel aux points d'entrée et de sortie des zones de rayonnement. L'accès aux zones à débit de dose élevé ou à niveaux de contamination radioactive élevés devrait être contrôlé par la mise en place de portes verrouillables et de dispositifs de verrouillage. Il faudrait minimiser les itinéraires empruntés par le personnel dans les zones de rayonnement et les zones contaminées afin de réduire le temps passé à traverser ces zones. Les zones de rayonnement où le personnel passe un temps considérable devraient être conçues afin de présenter des débits de doses les plus faibles possibles et de respecter le principe ALARA.

Dans les zones de rayonnement, il faudrait prévoir des vestiaires pour le personnel à des endroits choisis afin d'éviter la propagation de la contamination radioactive durant l'entretien et l'exploitation normale. Dans ces vestiaires, il faudrait tenir compte du besoin d'installations de décontamination pour le personnel, d'instruments de détection du rayonnement et de zones de stockage pour les vêtements de protection. Une barrière physique devrait clairement séparer le secteur propre de la zone potentiellement contaminée.

8.13.3 Surveillance

Cette section est traitée de manière suffisante par la version 2 du document RD-337, *Conception des nouvelles centrales nucléaires*. Il n'est donc pas nécessaire de fournir de l'orientation supplémentaire à ce sujet.

8.13.4 Sources

Cette section est traitée de manière suffisante par la version 2 du document RD-337, *Conception des nouvelles centrales nucléaires*. Il n'est donc pas nécessaire de fournir de l'orientation supplémentaire à ce sujet.

8.13.5 Surveillance de l'incidence environnementale

Cette section est traitée de manière suffisante par la version 2 du document RD-337, *Conception des nouvelles centrales nucléaires*. Il n'est donc pas nécessaire de fournir de l'orientation supplémentaire à ce sujet.

On trouvera de l'orientation complémentaire dans la norme N288.4-M90 (R2008), *Guidelines for Radiological Monitoring of the Environment*.

9.0 Analyses de la sûreté

9.1 Généralités

Cette section est traitée de manière suffisante par la version 2 du document RD-337, *Conception des nouvelles centrales nucléaires*. Il n'est donc pas nécessaire de fournir de l'orientation supplémentaire à ce sujet.

9.2 Objectifs de l'analyse

Comme l'indique le *Règlement sur les installations nucléaires de catégorie I*, la demande de permis pour construire une installation nucléaire de catégorie I doit comprendre un rapport préliminaire d'analyse de la sûreté démontrant que la conception de la centrale nucléaire est adéquate. La demande de permis pour exploiter une installation nucléaire de catégorie I doit comprendre un rapport final d'analyse de la sûreté reflétant la conception de l'installation « telle que construite ».

9.3 Analyse des dangers

L'analyse des dangers vise à déterminer la pertinence de la protection de la centrale nucléaire contre les dangers internes et externes tout en tenant compte de la conception de la centrale et des caractéristiques de l'emplacement. Pour assurer la disponibilité des fonctions de sûreté et des interventions des opérateurs requises, tous les SSC importants pour la sûreté (y compris la salle de commande principale, la salle de commande auxiliaire et le centre de soutien d'urgence) devraient être protégés de façon adéquate contre les dangers internes et externes pertinents.

L'analyse des dangers devrait établir une liste des dangers internes et externes pertinents pouvant avoir une incidence sur la sûreté de la centrale. Pour les dangers pertinents, l'examen devrait démontrer, en utilisant des techniques déterministes et probabilistes, que la probabilité ou les conséquences du danger sont suffisamment faibles pour ne pas nécessiter de mesures de protection particulières, ou démontrer que le danger fait l'objet de mesures de prévention et d'atténuation adéquates.

Tous les dangers internes et externes sont considérés dans le cadre des événements initiateurs hypothétiques (EIH). Les dangers qui n'y sont pour presque rien dans les risques liés à la centrale peuvent être éliminés de l'analyse détaillée, mais la raison d'être de cette suppression devrait être donnée. Le reste des EIH constitue la portée de l'analyse des dangers. La conception devrait spécifier les dangers liés au dimensionnement en établissant des critères clairs. Les dangers liés au dimensionnement devraient être analysés à l'aide des règles et des critères relatifs à l'analyse déterministe de la sûreté présentés à la section 9.4. Une telle analyse devrait également démontrer que les caractéristiques de conception complémentaires permettent d'atténuer de façon adéquate les conséquences radiologiques des conditions additionnelles de dimensionnement.

L'analyse de dangers devrait démontrer que la conception comporte des marges de sûreté suffisantes pour atténuer les effets falaise.

Renseignements supplémentaires

D'autres renseignements sont disponibles dans les documents suivants :

- CCSN, RD-346, *Évaluation de l'emplacement des nouvelles centrales nucléaires* [2008]
- CCSN, RD/GD-369, *Guide de présentation d'une demande de permis : Permis de construction d'une centrale nucléaire* [2011].
- CSA N293-F07, *Protection contre l'incendie dans les centrales nucléaires CANDU* [2007]
- CSA N289.4-M86, *Testing procedures for Seismic Qualification of CANDU Nuclear Power Plant* [confirmée en 2008]

- AIEA, NS-G-3.1, *Les événements externes d'origine humaine dans l'évaluation des sites de centrales nucléaires* [2006]
- AIEA, SSG-18, *Meteorological and Hydrological Hazards in Site Evaluation for Nuclear Installations* [2011]
- AIEA, SSG-9, *Seismic Hazards in Site Evaluation for Nuclear Installations* [2010]
- AIEA, NS-G-1.5, *External Events Excluding Earthquakes in the Design of Nuclear Power Plants* [2003]
- AIEA, NS-G-3.4, *Meteorological Events in Site Evaluation for Nuclear Power Plants* [2003]
- AIEA, NS-G-3.5, *Flood Hazard for Nuclear Power Plants on Coastal and River Sites* [2003]
- AIEA, NS-G-1.6, *Seismic Design and Qualification for Nuclear Power Plants* [2003]
- AIEA, NS-G-3.3, *Evaluation of Seismic Hazards for Nuclear Power Plants* [2002]
- AIEA, NS-G-1.7, *Protection Against Internal Fires and Explosions in the Design of Nuclear Power Plants* [2004]
- AIEA NS-G-1.11, *Protection Against Internal Hazards other than Fires and Explosions in the Design of Nuclear Power Plants* [2004]

9.4 Analyse déterministe de la sûreté

On trouvera de l'information sur l'analyse déterministe de la sûreté dans les publications suivantes :

- CCSN, RD-310, *Analyses de la sûreté pour les centrales nucléaires* [2008]
- CCSN, GD-310, *Document d'orientation sur les analyses de la sûreté des centrales nucléaires* [2012]
- CCSN, RD/GD-369, *Guide de présentation d'une demande de permis : Permis de construction d'une centrale nucléaire* [2011].
- CSA N286.7-F99, *Assurance de la qualité des programmes informatiques scientifiques, d'analyse et de conception des centrales nucléaires* [confirmée en 2007]
- AIEA, SSG-2, *Deterministic Safety Analysis for Nuclear Power Plants* [2009]
- AIEA, collection Normes de sûreté n° NS-G-1.2, *Évaluation et vérification de la sûreté des centrales nucléaires – Guide de sûreté* [2005]

9.5 Analyse probabiliste de la sûreté

On trouvera de l'information sur l'analyse probabiliste de la sûreté dans les publications suivantes :

- CCSN, S-294, *Études probabilistes de sûreté (ÉPS) pour les centrales nucléaires* [2005]
- CCSN, RD/GD-369, *Guide de présentation d'une demande de permis : Permis de construction d'une centrale nucléaire* [2011]
- AIEA, SSG-3, *Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants* [2010]
- AIEA, SSG-4, *Development and Application of Level 2 Probabilistic Safety Assessment for Nuclear Power Plants* [2010]
- AIEA, collection Rapports de sûreté n° 10, *Treatment of Internal Fires in Probabilistic Safety Assessment for Nuclear Power Plants* [1998]
- AIEA, collection Sécurité n° 50-P-7, *Treatment of External Hazards in Probabilistic Safety Assessment for Nuclear Power Plants* [1995]
- AIEA, collection Sécurité n° 50-P-10, *Reliability Analysis in Probabilistic Safety Assessment for Nuclear Power Plants: A Safety Practice* [1995]
- AIEA, collection Rapports de sûreté n° 25, *Review of Probabilistic Safety Assessments by Regulatory Bodies* [2002]

- ASME/ANS RA-Sa-2009, *Standard for Level 1/Large Early Release Frequency PRA for Nuclear Power Plant Applications* [2009]

10.0 Protection environnementale et atténuation

10.1 Conception relative à la protection de l'environnement

La conception devrait intégrer le principe des « meilleures techniques existantes d'application rentable » (MTEAR) pour les aspects de la conception liés à la protection de l'environnement.

10.2 Rejet de substances nucléaires et dangereuses

L'autorité responsable de la conception devrait démontrer le respect des principes d'optimisation et de prévention de la pollution en démontrant l'application du principe ALARA et du principe des MTEAR.

L'évaluation du cycle de vie mentionnée dans la version 2 du document RD-337 devrait comprendre une estimation initiale de l'inventaire total de toutes les matières radioactives et dangereuses qui seront utilisées ou produites au cours de la durée de vie de la centrale. Il faudrait prendre en compte tous les systèmes présents sur le site du réacteur et tenir compte des substances telles que l'hydrazine, le dioxyde de carbone, les CFC (hydrocarbures halogénés), les COV (composés organiques volatils), les NO_x (oxydes d'azote), le COT (carbone organique total), les poussières ou les solides en suspension, les détergents, les solvants, les métaux lourds (p. ex. le cuivre), le chlore, le phosphore, l'ammoniac et l'ammonium, la morpholine, l'huile ou la graisse. Il faudrait prendre en compte la nature de telles substances (solide, liquide, gaz, pH, température), leur gestion et les déchets produits.

La technologie choisie pour le refroidissement du condenseur devrait intégrer les techniques d'atténuation les plus récentes.

Renseignements supplémentaires

D'autres renseignements sont disponibles dans les documents suivants :

- CCSN, P-223, *Protection de l'environnement* [2001]
- CCSN, S-296, *Politiques, programmes et procédures de protection de l'environnement aux installations nucléaires de catégorie I et aux mines et usines de concentration d'uranium* [2006]
- CCSN, G-296, *Élaboration de politiques, programmes et procédures de protection de l'environnement aux installations nucléaires de catégorie I et aux mines et usines de concentration d'uranium* [2006]

11.0 Autres méthodes

Cette section est traitée de manière suffisante par la version 2 du document RD-337, *Conception des nouvelles centrales nucléaires*. Il n'est donc pas nécessaire de fournir de l'orientation supplémentaire à ce sujet.

Abréviations

AD	accident de dimensionnement
AEP	alimentation électrique préférée
AEU	alimentation électrique d'urgence
AHD	accident hors dimensionnement
ALARA	aussi faible qu'il soit raisonnablement possible d'atteindre (de l'anglais <i>as low as reasonably achievable</i>)
APRP	accident de perte de réfrigérant primaire
CAD	condition additionnelle de dimensionnement
CDS	critère de défaillance simple
CSU	centre de soutien d'urgence
DOC	défaillance d'origine commune
EAG	état d'arrêt garanti
EIH	événement initiateur hypothétique
EMR	évaluation des menaces et des risques
EPS	étude probabiliste de sûreté
FAR	fuite avant rupture
FH	facteurs humains
FTC	flux thermique critique
HCLPF	faible probabilité de défaillance avec un niveau de confiance élevé
IC	instrumentation et contrôle
IEM	interférence électromagnétique
IFP	incident de fonctionnement prévu
LCE	limites et conditions d'exploitation
MI	menace improbable
MR	menace de référence
MTEAR	meilleures techniques existantes d'application rentable
PET	panne d'électricité totale de la centrale
OE	qualification environnementale
REL	réacteur à eau légère
REP	réacteur à eau sous pression
SAPS	système d'affichage des paramètres de sûreté
SCA	salle de commande auxiliaire
SCP	salle de commande principale
SEUC	système d'évacuation d'urgence de la chaleur
SFU	source froide ultime
SR	séisme de référence
SRR	système de refroidissement du réacteur
SRUC	système de refroidissement d'urgence du cœur du réacteur
SSC	structures, systèmes et composants
VIVP	vanne d'isolation de la vapeur principale

Glossaire

accident

Événement inattendu, y compris les erreurs d'exploitation, les défaillances de l'équipement ou autres incidents dont les conséquences réelles ou potentielles ne sont pas négligeables du point de vue de la protection ou de la sûreté.

Remarque : Dans le cadre de ce document, les accidents incluent les accidents de dimensionnement et les accidents hors dimensionnement. Les accidents excluent les incidents de fonctionnement prévus qui ont des conséquences négligeables en matière de protection ou de sûreté.

accident de dimensionnement

Conditions accidentelles auxquelles une centrale nucléaire est conçue pour résister conformément à des critères de conception spécifiés et dans lesquelles l'endommagement du combustible et le rejet de matières radioactives sont maintenus en dessous des limites autorisées.

accident grave

Conditions d'accident qui sont plus graves que celles causées par un accident de dimensionnement et qui entraînent une détérioration importante du cœur du réacteur.

acte malveillant

Acte illégal ou acte commis dans l'intention de causer des torts.

alimentation électrique hors site

Alimentation en courant alternatif qui provient du réseau électrique et qui est fournie aux systèmes de distribution d'électricité de la centrale.

alimentation électrique préférée

Alimentation électrique en provenance du réseau de transport ou de la génératrice de la centrale, destinée aux systèmes de distribution électrique classés comme importants pour la sûreté. Il s'agit de l'alimentation électrique préférée pour les fonctions de support de la sûreté en mode d'exploitation normale et en cas d'IFP, d'AD ou de CAD.

alimentation électrique sur le site

Énergie fournie à partir de systèmes d'alimentation en courant alternatif (CA), de systèmes d'alimentation en courant continu (CC) et de systèmes d'alimentation sans coupure en CA.

analyse des dangers

Processus utilisé pour systématiquement identifier et évaluer les dangers en vue de déterminer les événements internes, externes, naturels et d'origine humaine potentiels susceptibles de faire en sorte que les dangers identifiés génèrent des défauts qui se transforment en accidents.

analyse de sûreté

Analyse à l'aide d'outils analytiques appropriés qui établit et confirme le dimensionnement des composants importants pour la sûreté et permet de s'assurer que la conception globale de la centrale satisfait aux critères d'acceptation pour chaque état d'exploitation de la centrale.

analyse déterministe de sûreté

Analyse des interventions de la centrale nucléaire à la suite d'un événement effectuée à l'aide de règles et d'hypothèses prédéterminées (p. ex. celles concernant l'état initial de fonctionnement, la disponibilité et l'efficacité des systèmes de la centrale et les interventions de l'opérateur). Les analyses déterministes peuvent utiliser les méthodes conservatrices ou fondées sur la meilleure estimation.

autorité en matière de conception

L'entité qui a la responsabilité générale du processus de conception ou de l'approbation des modifications à la conception, et qui s'assure que les connaissances nécessaires sont tenues à jour.

capacité d'utilisation

Mesure dans laquelle un produit peut être utilisé par des utilisateurs spécifiés dans le but d'atteindre des objectifs précis et ce, de façon efficace, efficiente et satisfaisante dans un contexte d'utilisation spécifié.

caractéristique de conception complémentaire

Caractéristique de conception physique ajoutée à la conception sous forme de structure, système ou composant (SSC) autonome ou ajoutée à un SSC déjà en place pour prendre en considération les conditions additionnelles de dimensionnement.

centrale nucléaire

Toute installation d'un réacteur à fission nucléaire construite pour la production d'électricité à une échelle commerciale. Une centrale nucléaire est une installation nucléaire de catégorie IA telle que définie dans le *Règlement sur les installations nucléaires de catégorie I*.

chaleur résiduelle

Somme des chaleurs dégagées par la désintégration radioactive, la fission du combustible en mode d'arrêt du réacteur et la chaleur emmagasinée dans les structures, systèmes et composants du réacteur.

combustion

Processus chimique comprenant une oxydation suffisante pour produire de la chaleur ou de la lumière.

conception à sûreté intégrée

Conception dont les modes de défaillance les plus probables ne résultent pas en une réduction de la sûreté.

conditions additionnelles de dimensionnement

Conditions d'accident qui ne sont pas considérées comme des accidents de dimensionnement, mais qui sont prises en considération dans les processus de conception de la centrale.

conditions d'accident

Écarts par rapport à l'exploitation normale plus graves que les incidents de fonctionnement prévus, comprenant les accidents de dimensionnement et les conditions additionnelles de dimensionnement.

confinement

Enveloppe continue sans ouverture ou pénétrations (telle qu'une fenêtre) qui empêche le rejet de gaz ou de particules à l'extérieur de l'espace clos.

conservatisme

Recours à des hypothèses fondées sur l'expérience ou des données indirectes concernant un phénomène ou un comportement d'un système à la limite ou proche de la limite prévue, qui permettent d'augmenter les marges de sûreté ou de prédire des conséquences plus graves que si des hypothèses fondées sur la meilleure estimation avaient été utilisées.

crédité

Dans le cadre d'une analyse, présomption du fonctionnement correct d'un SSC ou d'une intervention appropriée de l'opérateur.

critères d'acceptation

Limites établies sur la valeur d'un indicateur fonctionnel ou conditionnel utilisé pour évaluer la capacité d'une structure, d'un système ou d'un composant à répondre à ses exigences de conception et de sûreté.

culture de sûreté

Caractéristiques de l'environnement de travail, comme les valeurs, les règles et la compréhension commune, qui influent sur les perceptions et les attitudes des employés à l'égard de l'importance que l'organisation accorde à la sûreté.

cybersécurité

Protection des systèmes ou composants informatiques numériques pendant le cycle de vie du système contre les menaces, les actes malveillants ou les gestes commis par inadvertance qui pourraient avoir des conséquences non intentionnelles. Cela inclut la protection contre des modifications non autorisées, non intentionnelles et non sécuritaires au système ainsi que la divulgation non autorisée et la conservation de renseignements, de logiciels ou de données associés au système qui pourraient être utilisés pour poser des gestes malveillants ou malavisés ayant un impact sur la fonctionnalité et la performance du système.

défaillance d'origine commune

Défaillance simultanée de deux ou plusieurs structures, systèmes ou composants attribuable à un événement ou une cause spécifique simple tel qu'un phénomène naturel (séismes, tornades, inondations, etc.), une défaillance de conception, des défauts de fabrication, des erreurs d'exploitation et d'entretien, des événements destructeurs d'origine humaine et autres.

défaillance simple

Défaillance résultant de la perte de la capacité d'un composant l'empêchant d'exécuter sa (ses) fonction(s) de sûreté prévue(s), et toute défaillance résultant de cette défaillance simple..

dimensionnement

Éventail des conditions et des événements pris explicitement en considération dans la conception d'une installation, conformément aux critères fixés, de façon que l'installation puisse y résister sans dépassement des limites autorisées quand les systèmes de sûreté fonctionnent comme prévu.

diversité

Présence de deux ou plusieurs systèmes ou composants redondants servant à exécuter une fonction définie, où les différents systèmes ou composants présentent des attributs distincts afin de diminuer la possibilité de défaillance d'origine commune.

division

Système ou ensemble de composants donné qui permet l'établissement et le maintien d'une indépendance physique, électrique et fonctionnelle par rapport à d'autres ensembles redondants de composants.

dommage au cœur du réacteur

Séquence d'accidents plus grave qu'un AD comportant une détérioration du cœur du réacteur.

effet falaise

Augmentation importante de la sévérité des conséquences découlant d'un petit changement de conditions.

Remarque : Un effet falaise peut être causé par des changements dans les caractéristiques de l'environnement ou de l'événement, ou dans la réponse de la centrale.

éliminé, à toute fin pratique

Le fait que la possibilité que certaines conditions se produisent soit physiquement impossible ou extrêmement improbable avec un degré élevé de confiance.

enceinte de confinement

Structure de confinement conçue pour maintenir le confinement à des températures et à des pressions élevées et qu'il est permis de pénétrer par des vannes d'isolation.

enveloppe de conception de la centrale

Éventail des conditions et des événements (y compris les CAD) explicitement pris en compte dans la conception de la centrale nucléaire de sorte que l'on puisse raisonnablement s'attendre à ce que tout rejet radioactif important soit pratiquement éliminé par le fonctionnement prévu des systèmes de procédé et de contrôle, des systèmes de sûreté, des systèmes de support en matière de sûreté et des caractéristiques de conception complémentaires.

enveloppe sous pression

Enveloppe de toute cuve, système ou composant sous pression d'un système nucléaire ou non nucléaire.

environnement

Composants terrestres comprenant :

1. les terres, les eaux et l'air, incluant toutes les couches de l'atmosphère;
2. toutes les matières organiques et inorganiques et les organismes vivants;
3. les systèmes naturels en interaction comprenant les composants susmentionnés (1 et 2).

état d'arrêt

État caractérisé par la sous-criticité du réacteur. Dans cet état d'arrêt, l'activation automatique des systèmes de sûreté pourrait être bloquée et les systèmes de support peuvent demeurer dans des configurations anormales.

état d'arrêt sûr

État caractérisé par la sous-criticité du réacteur, permettant d'assurer et de maintenir la stabilité des fonctions de sûreté fondamentales de façon prolongée.

états de fonctionnement

États définis en mode d'exploitation normale et d'incidents de fonctionnement prévus.

état de la centrale

Configuration de composants de la centrale, y compris les états physiques et thermodynamiques des matériaux et leur contenu en fluides de procédé.

étude probabiliste de sûreté (EPS)

Évaluation exhaustive et intégrée de la sûreté de la centrale nucléaire. L'EPS tient compte de la probabilité, de la progression et des conséquences des défaillances de l'équipement et de conditions transitoires pour calculer des estimations numériques qui fournissent une mesure cohérente de la sûreté de la centrale nucléaire, de la façon suivante :

1. Une EPS de niveau 1 identifie et quantifie les séquences d'événements qui peuvent entraîner la perte d'intégrité structurale du cœur et la défaillance généralisée du combustible;
2. Une EPS de niveau 2 s'appuie sur les résultats de l'EPS de niveau 1 pour analyser le comportement du confinement, évaluer les radionucléides libérés par le combustible défectueux et quantifier les rejets dans l'environnement;
3. Une EPS de niveau 3 s'appuie sur les résultats de l'EPS de niveau 2 pour analyser la répartition des radionucléides dans l'environnement et évaluer les répercussions sur la santé du public.

évaluation des menaces et des risques

Évaluation de la pertinence d'un système de protection physique existant ou projeté, conçu pour la protection contre :

1. les actes intentionnels qui pourraient constituer une menace pour la sécurité de l'installation nucléaire;
2. l'exploitation de faiblesses des mesures de protection physique d'une installation nucléaire.

événement d'origine commune

Événement qui mène à des défaillances d'origine commune.

événement externe

Événement sans lien avec l'exploitation d'une installation ou la réalisation d'une activité et qui pourrait avoir un effet sur la sûreté de l'installation ou de l'activité.

Remarque : Les événements externes englobent, sans toutefois s'y limiter, les tremblements de terre, les inondations et les ouragans.

événement initiateur hypothétique (EIH)

Événement identifié dans la conception et entraînant un IFP, un accident de dimensionnement ou un accident hors dimensionnement. Il en découle que l'EIH n'est pas nécessairement un accident en soi; il est plutôt l'initiateur d'une séquence susceptible de dégénérer en incident de fonctionnement, en accident de dimensionnement ou en accident hors dimensionnement, selon les défaillances supplémentaires qui surviennent.

événement interne

Événement se produisant dans la centrale attribuable à une erreur humaine ou à une défaillance d'un système, d'une structure ou d'un composant.

exploitation normale

Fonctionnement d'une centrale nucléaire à l'intérieur de limites et de conditions opérationnelles prescrites, y compris le démarrage, l'exploitation des réacteurs, l'arrêt, l'état d'arrêt, l'entretien, les essais et le rechargement du combustible.

facteurs humains

Facteurs qui influent sur le rendement du personnel au plan de la sûreté de la centrale, y compris les activités durant les phases de conception, de construction, de mise en service, d'exploitation, d'entretien et de déclassement.

formation de missiles

Danger associé à la projection soudaine de débris à grande vitesse.

fuite avant rupture

Situation où la fuite due à un défaut est détectée en mode d'exploitation normale, permettant ainsi d'arrêter le réacteur et de le dépressuriser avant que l'anomalie ne se transforme en rupture.

garanties

Système d'inspections internationales et autres activités de vérification entreprises par l'AIEA afin d'évaluer, sur une base annuelle, la conformité du Canada à ses obligations conformément aux accords de garanties conclus entre le Canada et l'AIEA.

gestion du vieillissement

Mesures d'ingénierie, d'exploitation et d'entretien destinées à contrôler, dans les limites acceptables, les effets du vieillissement physique et la vétusté des structures, systèmes et composants.

groupe de sûreté

Assemblage de structures, systèmes et composants conçu pour exécuter toutes les actions requises au cours d'un événement initiateur hypothétique particulier pour que les limites spécifiées des états d'IFP et d'AD ne soient pas dépassées. L'assemblage peut comprendre des systèmes de sûreté et des systèmes de support, ainsi que toute interaction entre les systèmes fonctionnels.

groupe essentiel

Groupe de membres du public raisonnablement homogène quant à son exposition à une source de rayonnement donnée et qui est typique des personnes recevant la dose efficace la plus élevée ou la dose équivalente (le cas échéant) d'une source donnée.

incendie

Processus de combustion caractérisé par des émissions de chaleur accompagnées de fumée ou de flammes ou les deux.

incident de fonctionnement prévu

Processus opérationnel qui s'écarte de l'exploitation normale et qui devrait survenir à tout le moins une fois au cours du cycle de vie utile de la centrale mais qui ne cause pas, selon les dispositions de conception appropriées, de dommage grave aux composants importants pour la sûreté ou qui ne se transforme pas en accident.

limites et conditions d'exploitation

Ensemble de règles qui établissent les limites des paramètres ainsi que la capacité fonctionnelle et les niveaux de rendement de l'équipement et du personnel, approuvées par l'organisme de réglementation afin d'assurer l'exploitation sûre d'une installation autorisée. Cet ensemble de limites et conditions d'exploitation est surveillé par l'exploitant ou en son nom, et peut être contrôlé par l'opérateur.

marge de sûreté

Marge attribuée à une valeur ou variable de sûreté d'une barrière ou d'un système, à laquelle des dommages ou des pertes pourraient se produire. Des marges de sûreté sont prises en compte pour les systèmes et les barrières dont la défaillance est susceptible de contribuer à des rejets radiologiques.

meilleure estimation

Estimation impartiale obtenue par l'utilisation d'un modèle mathématique ou d'une méthode de calcul pour prédire, de façon réaliste, le rendement de la centrale et les paramètres importants.

menace de référence

Ensemble d'actes malveillants que la CCSN estime possibles.

menace improbable

Conditions de menace plus graves qu'une menace de référence pouvant entraîner une détérioration structurale et impliquer une dégradation de la barrière de confinement.

mise en service

Processus consistant en une série d'activités visant à démontrer que les structures, les systèmes, les composants et équipements installés fonctionnent conformément à leurs spécifications et aux attentes de conception, avant la mise en service de la centrale.

panne d'électricité totale de la centrale

Perte complète d'alimentation en courant alternatif (CA) des sources hors site, de la génératrice principale sur le site et des sources d'alimentation de relève et d'urgence. Ne comprend pas la défaillance des sources

d'alimentation sans coupure en CA et des sources d'alimentation en courant continu, non plus que la défaillance de l'alimentation de remplacement en CA.

paramètre de déclenchement

Variable dont la mesure est utilisée pour enclencher un système de sûreté lorsque la valeur seuil de déclenchement est atteinte.

paramètre de déclenchement direct

Processus ou paramètre neutronique utilisé pour déclencher un arrêt et qui est une mesure directe d'un enjeu particulier à l'égard des critères d'acceptation dérivés ou une mesure directe de l'événement qui se déroule.

procédé

Ensemble d'activités inter-reliées qui transforment des intrants en extrants.

qualification de l'équipement

Processus servant à certifier que l'équipement respecte les exigences de fonctionnement dans les conditions applicables à ses fonctions de sûreté. Cela comprend la production et la tenue à jour de preuves que l'équipement fonctionnera sur demande, dans des conditions de service précises, pour répondre aux exigences de performance du système.

réalisable

Réalisable et justifiable du point de vue technique en tenant compte des facteurs coûts-avantages.

source froide

Système ou composant qui permet le transfert de chaleur depuis une source chaude telle que la chaleur produite par le combustible, jusqu'à un grand milieu qui absorbe la chaleur.

source froide ultime

Milieu auquel la chaleur résiduelle peut toujours être transférée, même si tous les autres moyens d'évacuation de la chaleur ont été perdus ou sont insuffisants. Ce milieu est normalement un plan d'eau ou l'atmosphère.

SSC importants pour la sûreté

Structures, systèmes et composants d'une centrale nucléaire qui sont associés au déclenchement, à la prévention, à la détection ou à l'atténuation de toute séquence de défaillance et qui ont le plus grand impact dans la réduction de la possibilité d'un endommagement au combustible, du rejet associé de radionucléides, ou les deux.

structures, systèmes et composants (SSC)

Terme général englobant tous les éléments d'une installation ou d'une activité qui contribuent à la protection et à la sûreté.

Les structures sont des éléments passifs : bâtiments, cuves, boucliers, etc. Un système comprend plusieurs composants assemblés de manière à exécuter une fonction (active) spécifique. Un composant est un élément discret d'un système, par exemple des câbles, des transistors, des circuits intégrés, des moteurs, des relais, des solénoïdes, des conduites, des raccords, des pompes, des réservoirs et des vannes.

système de gestion

Ensemble d'éléments interdépendants ou en interaction (système) qui permet d'établir des politiques et des objectifs et de réaliser ces objectifs de façon efficace et efficiente. Le système de gestion intègre tous les éléments d'une organisation en un système cohérent qui permet d'atteindre tous les objectifs de

l'organisation. Ces éléments comprennent les structures, les ressources et les processus. Le personnel, l'équipement et la culture organisationnelle ainsi que les politiques et les processus documentés font partie du système de gestion. Les processus de l'organisation doivent aborder la totalité des exigences relatives à l'organisation telles qu'elles sont établies, par exemple, dans les normes de sûreté de l'AIEA ou d'autres normes et codes internationaux.

système de procédé

Système dont la fonction principale est de soutenir la production de vapeur ou d'électricité ou d'y contribuer.

système de support en matière de sûreté

Système conçu pour assister le fonctionnement d'un système ou de plusieurs systèmes de sûreté.

système de sûreté

Système important pour la sûreté qui assure l'arrêt sûr du réacteur ou l'évacuation de la chaleur résiduelle du cœur du réacteur, ou qui atténue les conséquences des incidents de fonctionnement prévus et des accidents de dimensionnement.

système indépendant

Système qui est capable d'exécuter ses fonctions prévues tout en n'étant pas touché par l'exploitation ou la défaillance d'un autre système.

temps de mission

Période durant laquelle un système ou composant doit fonctionner ou être disponible et exécuter sa fonction, à la suite d'un événement.

valeur seuil de déclenchement

Valeur du paramètre de déclenchement à laquelle l'activation d'un système de sûreté est effectuée.

zone d'exclusion

Conformément à l'article 1 du *Règlement sur les installations nucléaires de catégorie I*, une parcelle de terre à l'intérieur ou à proximité d'une installation nucléaire sur laquelle il n'y a pas de résidence permanente et pour laquelle un titulaire de permis a le pouvoir légal d'en exercer le contrôle.

zone vitale

Zone contenant de l'équipement, des systèmes ou des dispositifs dont le sabotage pourrait directement ou indirectement entraîner des conséquences radiologiques inacceptables.

Références de la CCSN

1. S-98, révision 1, *Programmes de fiabilité pour les centrales nucléaires* [2005]
2. S-210, *Programmes d'entretien des centrales nucléaires* [2007]
3. RD-310, *Analyses de la sûreté pour les centrales nucléaires* [2008]
4. GD-310, *Document d'orientation sur les analyses de la sûreté des centrales nucléaires* [2012]
5. RD-327, *Sûreté en matière de criticité nucléaire* [2010]
6. GD-327, *Directives de sûreté en matière de criticité nucléaire* [2010]
7. RD-334, *Gestion du vieillissement des centrales nucléaires* [2011]
8. RD-336, *Comptabilisation et déclaration des matières nucléaires* [2010]
9. GD-336, *Document d'orientation pour la comptabilisation et la déclaration des matières nucléaires* [2010]
10. RD-346, *Évaluation de l'emplacement des nouvelles centrales nucléaires* [2008]
11. RD/GD-369, *Guide de présentation d'une demande de permis : Permis de construction d'une centrale nucléaire* [2011]
12. G-129, révision 1, *Maintenir les expositions et les doses au « niveau le plus bas qu'il soit raisonnablement possible d'atteindre (ALARA) »* [2004]
13. G-219, *Les plans de déclassement des activités autorisées* [2000]
14. G-225, *Planification d'urgence dans les installations nucléaires de catégorie I, les mines d'uranium et les usines de concentration d'uranium* [2001]
15. G-274, *Les programmes de sécurité pour les matières nucléaires de catégorie I ou II, ou pour certaines installations nucléaires* [2003]
16. P-119, *Politique sur les facteurs humains* [2000]
17. G-276, *Plan de programme d'ingénierie des facteurs humains* [2003]
18. G-278, *Plan de vérification et validation des facteurs humains* [2003]
19. G-306, *Programmes de gestion des accidents graves touchant les réacteurs nucléaires* [2006]
20. G-323, *Assurer la présence d'un nombre suffisant de travailleurs qualifiés aux installations nucléaires de catégorie I – Effectif minimal* [2007]
21. S-294, *Études probabilistes de sûreté (ÉPS) pour les centrales nucléaires* [2005]
22. P-223, *Protection de l'environnement* [2001]
23. S-296, *Politiques, programmes et procédures de protection de l'environnement aux installations nucléaires de catégorie I et aux mines et usines de concentration d'uranium* [2006].
24. G-296, *Élaboration de politiques, programmes et procédures de protection de l'environnement aux installations nucléaires de catégorie I et aux mines et usines de concentration d'uranium* [2006]
25. G-208, *Les plans de sécurité pour le transport des matières nucléaires de catégorie I, II ou III* [2003]

26. RD-363, *Aptitudes psychologiques, médicales et physiques des agents de sécurité nucléaire* [2008]

Renseignements supplémentaires

Les documents suivants contiennent des renseignements supplémentaires qui pourraient intéresser les personnes concernées par la conception de centrales nucléaires. Il conviendrait d'utiliser l'édition la plus récente ou celle qui a été approuvée.

Association canadienne de normalisation (CSA)

1. N285.0-F08, *Exigences générales relatives aux systèmes et aux composants sous pression des centrales nucléaires CANDU* [2008]
2. N285.4-F09, *Inspection périodique des composants des centrales nucléaires CANDU* [2009]
3. N285.4-08, *Inspection périodique des composants de confinement des centrales nucléaires CANDU*, troisième édition [2008]
4. N286-05F, *Exigences relatives au système de gestion des centrales nucléaires* [mise à jour n° 2 : décembre 2010]
5. N286.7-F99, *Assurance de la qualité des programmes informatiques scientifiques, d'analyse et de conception des centrales nucléaires* [confirmée en 2007]
6. N287.3-93 (2009), *Design Requirements for Concrete Containment Structures for CANDU Nuclear Power Plants* [confirmée en 2009]
7. N287.6-11, *Pre-operational Proof and Leakage Rate Testing Requirements for Concrete Containment Structures for Nuclear Power Plants* [2011]
8. N287.7-F08, *Exigences relatives à la mise à l'essai et à la vérification, en cours d'exploitation, des enceintes de confinement en béton des centrales nucléaires CANDU* [2008]
9. CSA N286.7.1-09, *Guideline for the application of N286.7-99, Quality assurance of analytical, scientific, and design computer programs for nuclear power plants* [2009]
10. CAN/CSA-N288.2-M91 (R2008), *Guidelines for Calculating Radiation Doses to the Public from a Release of Airborne Radioactive Material under Hypothetical Accident Conditions in Nuclear Reactors* [2008]
11. N288.4-M90 (R2008), *Guidelines for Radiological Monitoring of the Environment* [confirmée en 2008]
12. collection de normes CSA N289 consacrées à la conception et à la qualification parasismique des centrales nucléaires CANDU
13. N289.3-10, *Design procedures for seismic qualification of nuclear power plants* [2010]
14. N289.4-M86, *Testing procedures for Seismic Qualification of CANDU Nuclear Power Plant* [confirmée en 2008]
15. N289.5-M91, *Seismic, Instrumentation Requirements for CANDU Nuclear Power Plants* [confirmée en 2008]
16. N290.0-11/N290.3-11 COLLECTION – Contient les *General requirements for safety systems of nuclear power plants* et la norme N290.3-11, *Requirements for the containment system of nuclear power plants* [2011]
17. N290.1-80, *Requirements for the Shutdown Systems of CANDU Nuclear Power Plants* [confirmée en 2011]

18. N290.4-11, *Requirements for Reactor Control Systems of Nuclear Power Plants* [2011]
19. N290.5-F06 (R2011), *Exigences relatives aux systèmes d'alimentation électrique et en air d'instrumentation des centrales nucléaires CANDU* [confirmée en 2011]
20. N290.6-09, *Exigences relatives à la surveillance et à l'affichage des fonctions de sûreté d'une centrale nucléaire au moment d'un accident* [2009]
21. N290.13-05, *Environmental Qualification of Equipment for CANDU Nuclear Power Plants* [2009]
22. N290.14-07, *Qualification of pre-developed software for use in safety related instrumentation and control applications in nuclear power plants* [2007]
23. N290.15-F10, *Exigences relatives aux limites d'exploitation sûre des centrales nucléaires* [2010]
24. N291-08, *Exigences relatives aux enceintes reliées à la sûreté des centrales nucléaires CANDU* [mai 2009]
25. N292.3-08, *Gestion des déchets radioactifs de faible et de moyenne activité* [2008]
26. N293-F07, *Protection contre l'incendie dans les centrales nucléaires CANDU* [2007]
27. N294-09, *Decommissioning of Facilities Containing Nuclear Substances* [2009]
28. A23.3-F04 (C2010), *Calcul des ouvrages en béton* [2010]
29. S16-F09, *Règles de calcul des charpentes en acier* [2009]
30. S304.1-F04 (C2010), *Calcul des ouvrages en maçonnerie* [2010]

Agence internationale de l'énergie atomique (AIEA)

1. NS-R-1, *Sûreté des centrales nucléaires : conception* [2000]
2. SSR-2/1, *Sûreté des centrales nucléaires : conception* [2012] (version révisée du document NS-R-1)
3. SSR 2/2, *Sûreté des centrales nucléaires : mise en service et exploitation* [2012]
4. Collection Sécurité n° 110, *La sûreté des installations nucléaires* [1993]
5. 75-INSAG-3 Rev. 1, INSAG-12, *Basic Safety Principles for Nuclear Power Plants* [1999]
6. INSAG-10, *La défense en profondeur en sûreté nucléaire* [1997]
7. GS-R-2 – *Préparation et intervention en cas de situation d'urgence nucléaire ou radiologique* [2002]
8. GS-R-3, *Système de gestion des installations et des activités* [2006]
9. GS-G-3.3, *The Management System for the Processing, Handling and Storage of Radioactive Waste Safety Guide* [2008]
10. GS-G-3.5, *The Management System for Nuclear Installations* [2009]
11. INSAG-19, *Maintaining the Design Integrity of Nuclear Installations throughout their Operating Life* [2003]
12. Prescriptions générales de sûreté Partie 4 n° GSR Part 4, *Évaluation de la sûreté des installations et activités* [2009]

13. Collection Rapports de sûreté n° 46, *Assessment of Defence in depth for Nuclear Power Plants* [2005]
14. Collection Sécurité n° 50-P-1, *Application of the Single Failure Criterion* [1990]
15. Collection Sécurité n° 50-P-7, *Treatment of External Hazards in Probabilistic Safety Assessment for Nuclear Power Plants* [1995]
16. Collection Sécurité n° 50-P-10, *Human Reliability Analysis in Probabilistic Safety Assessment for Nuclear Power Plants* [1995]
17. Collection Rapports de sûreté n° 8, *Safe Preparation of Fire Hazard Analysis for Nuclear Power Plants* [1998]
18. TECDOC-967 (Rev.1)/F, *Orientations et considérations concernant l'application du document INFCIRC/225/Rev.4, La protection physique des matières et installations nucléaires* [mai 2002]
19. TECDOC-1276, *Handbook on the physical protection of nuclear materials and facilities* [2002]
20. TECDOC-1657, *Design Lessons Drawn from the Decommissioning of Nuclear Facilities* [2011]
21. WS-G-2.1, *Déclassement des centrales nucléaires et des réacteurs de recherche – Guide de sûreté* [novembre 2004]
22. Collection Rapports de sûreté n° 3, *Equipment qualification in operational nuclear power plants: upgrading, preserving and reviewing* [1999]
23. Collection Rapports de sûreté n° 25, *Review of Probabilistic Safety Assessments by Regulatory Bodies* [2002]
24. Guide de sûreté n° RS-G-1.1, *Radioprotection professionnelle* [2004]
25. NS-G-1.2, *Évaluation et vérification de la sûreté des centrales nucléaires – Guide de sûreté* [2005]
26. NS-G-1.4, *Design of Fuel Handling and Storage Systems in Nuclear Power Plants Safety Guide* [2003]
27. NS-G-1.5, *External Events Excluding Earthquakes in the Design of Nuclear Power Plants* [2003]
28. NS-G-1.6, *Seismic Design and Qualification for Nuclear Power Plants* [2003]
29. NS-G-1.8, *Design of Emergency Power Systems of Nuclear Power Plants* [2004]
30. NS-G-1.10, *Design of Reactor Containment Systems for Nuclear Power Plants* [2004]
31. NS-G-1.11, *Protection Against Internal Hazards other than Fires and Explosions in the Design of Nuclear Power Plants* [2004]
32. NS-G-1.12, *Design of the Reactor Core for Nuclear Power Plants* [2005]
33. NS-G-1.13, *Radiation Protection Aspects of Design for Nuclear Power Plants* [2005]
34. NS-G-2.1, *Protection contre l'incendie des centrales nucléaires en exploitation* [février 2004]
35. NS-G-2.2, *Limites et conditions d'exploitation et procédures de conduite des centrales nucléaires* [juillet 2005]
36. NS-G-2.5, *Core Management and Fuel Handling for Nuclear Power Plants* [2002]

37. NS-G-2.6, *Maintenance, Surveillance and In-Service Inspection in Nuclear Power Plants* [2002]
38. NS-G-2.9, *Commissioning for Nuclear Power Plants* [2003]
39. NS-G-2.11, *A System for the Feedback of Experience from Events in Nuclear Installations* [2006]
40. NS-G-3.1, *Les événements externes d'origine humaine dans l'évaluation des sites de centrales nucléaires* [2006]
41. NS-G-3.3, *Evaluation of Seismic Hazards for Nuclear Power Plants* [2002]
42. NS-G-3.4, *Meteorological Events in Site Evaluation for Nuclear Power Plants* [2003]
43. NS-G-3.5, *Flood Hazard for Nuclear Power Plants on Coastal and River Sites* [2003]
44. NS-G-4.6, *Radiation Protection and Radioactive Waste Management in the Design and Operation of Research Reactors* [2009]
45. SSG-2, *Deterministic Safety Analysis for Nuclear Power Plants* [2009]
46. SSG-3, *Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants* [2010]
47. SSG-4, *Development and Application of Level 2 Probabilistic Safety Assessment for Nuclear Power Plants* [2010]
48. SSG-9, *Seismic Hazards in Site Evaluation for Nuclear Installations* [2010]
49. SSG-18, *Meteorological and Hydrological Hazards in Site Evaluation for Nuclear Installations* [2011]
50. Collection Sécurité nucléaire n° 13, *Recommandations de sûreté nucléaire sur la protection physique des matières nucléaires et des installations nucléaires (INFCIRC/225/Révision 5)* [2011]
51. Collection Sécurité nucléaire n° 17, *Computer Security at Nuclear Facilities* [2011]

Nuclear Regulatory Commission des États-Unis (USNRC)

1. 10 CFR Part 50, Appendix B, *Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants* [2007]
2. NUREG/CR-6303, *Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems* [1994]
3. NUREG-6393, *Integrated System Validation: Methodology and Review Criteria* [1997]
4. NUREG/CR-7007, *Diversity Strategies for Nuclear Power Plant Instrumentation and Control Systems* [2010\$]
5. Branch Technical Position (BTP) 7-19, *Guidance for Evaluation of Diversity and Defense-in-Depth and in Digital Computer-Based Instrumentation and Control Systems* [2007]
6. Regulatory Guide 1.57, *Design Limits and Loading Combinations for Metal Primary Reactor Containment System Components* [2007]
7. SECY-08-0093, *Resolution of Issues Related to Fire-Induced Circuit Failures* [2008]
8. NUREG 1852, *Demonstrating the Feasibility and Reliability of Operator Manual Actions in Response to Fire* [2007]

9. NUREG/CR-2913- Rev. 4, *Two-Phase Jet Loads* [1983]
10. NUREG/CR-6850, EPRI 1011989, *Fire Probabilistic Risk Assessment Methods Enhancements* [2010]
11. Regulatory Guide 1.189, *Fire Protection for Operating Nuclear Power Plants* [2001]
12. NUREG-0700 Revision 2, *Human-System Interface Design Review Guidelines* [2002]
13. NUREG-0711 Revision 2, *Human Factors Engineering Program Review Model* [2004]
14. NUREG 0800, section 3.7.3, *Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition - Seismic Subsystem Analysis* [2007]
15. NUREG-0800, section 3.8.1, *Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition - Concrete Containment* [2007]
16. NUREG-0800, section 3.8.3, *Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition - Concrete and steel internal structures of steel or concrete containments* [2010]
17. NUREG-0800, section 3.8.4, *Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition – Other Seismic Category I Structures* [2010]
18. NUREG-0800, chapter 8, *Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition - Electric Power* [2007]
19. NUREG-0800, section 9.5.1.1, *Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition - Fire Protection Program* [2009]
20. NUREG-0800, chapter 10, *Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition – Steam and Power Conversion System* [2007]
21. NUREG-0800, chapter 14, *Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition – Initial Test Program and ITAAC – Design Certification* [2007]
22. NUREG-0800, section 14.3.10, *Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition - Emergency Planning – Inspections, Tests, Analyses, and Acceptance Criteria* [2007]
23. NUREG-0800, chapter 18, *Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants – Human Factors Engineering*
24. Regulatory Guide 1.76, *Design Basis Tornado and Tornado Missiles for Nuclear Power Plants* [2007]
25. Regulatory Guide 1.91, *Evaluations of Explosions Postulated to occur on Transportation Routes near Nuclear Power Plants* [1978]
26. NUREG/CR-6486, *Assessment of Modular Construction for Safety-Related Structures at Advanced Nuclear Power Plants* [1997]
27. TECDOC-1657, *Design Lessons Drawn from the Decommissioning of Nuclear Facilities* [2011]
28. NUREG/CR-1278, *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications-Final Report* [2011]
29. NUREG/CR-6633, *Advanced Information Systems Design: Technical Basis and Human Factors Review Guidelines* [2000]

30. NUREG-6684, *Advanced Alarm Systems: Revision of Guidance and Its Technical Basis* [2000]
31. NUREG-0696, *Functional Criteria for Emergency Response Facilities* [1981]
32. Regulatory Guide 1.77, *Assumptions Used for Evaluating a Control Rod Ejection Accident for Pressurized Water Reactors* [1974]
33. Regulatory Guide 1.203, *Transient and Accident Analysis Methods* [2005]
34. Regulatory Guide 5.71, *Cyber Security Programs for Nuclear Facilities* [2010]

Autres

1. American Concrete Institute (ACI), 349-06, *Code Requirements for Nuclear Safety-Related Concrete Structures & Commentary* [2007]
2. American National Standards Institute, *American National Standard Design Requirements for Light Water Reactor Fuel Handling System*, ANSI/ANS-57.1 [1992]
3. American National Standards Institute, *Time Response Design Criteria for Safety-Related Operator Actions*, ANSI/ANS-58.8 [1994]
4. American Nuclear Society (ANS), *Categorization of Nuclear Facility Structures, Systems, and Components for Seismic Design*, ANS 2.26 [confirmée en 2010]
5. American Nuclear Society (ANS) 2.3- 2011, *Estimating Tornado, Hurricane, and Extreme Straight Line Wind Characteristics at Nuclear Facility Sites* [2011]
6. American Society of Civil Engineers (ASCE), *Seismic Design Criteria for Structures, Systems and Components in Nuclear Facilities*, ASCE 43-05 [2005]
7. American Society of Civil Engineers (ASCE), *Seismic Analysis for Safety-Related Nuclear Structures*, ASCE 04-98 [2000]
8. American Society of Civil Engineers (ASCE), *Design of Blast-Resistant Buildings in Petrochemical Facilities* [2010]
9. American Society of Civil Engineers (ASCE), *Structural Analysis and Design of Nuclear Plant Facilities: 58 (ASCE Manual and Reports on Engineering Practice)* [1980]
10. American Society of Mechanical Engineers (ASME), *ASME Boiler and Pressure Vessel Code – 2010 edition* [2010]
11. American Society of Mechanical Engineers, *ASME Boiler and Pressure Vessel Code, Section III: Rules for Construction of Nuclear Power Plant Components, Division 1, Subsection NE: Class MC Components* [2010]
12. American Society of Mechanical Engineers, *ASME Boiler and Pressure Vessel Code, Section III, Division 2, Section 3, Code for Concrete Containments* [2010]
13. American Society of Mechanical Engineers, *Quality Assurance Requirements for Nuclear Facility Applications*, NQA-1-2008 [2008]
14. American Society of Mechanical Engineers, *Qualification of Active Mechanical Equipment Used in Nuclear Power Plants*, QME-1-2002 [2002]
15. American Society of Mechanical Engineers, *Standard for Level 1/Large Early Release Frequency PRA for Nuclear Power Plant Applications*, ASME/ANS RA-Sa-2009 [2009]

16. Association Française pour les règles de conception, de construction et de surveillance en exploitation des Chaudières Electro-Nucléaires (AFCEN), *Design and Construction Rules for Mechanical Components of PWR Nuclear Islands*, AFCEN RCC-M [2007]
17. Association Française pour les règles de conception, de construction et de surveillance en exploitation des Chaudières Electro-Nucléaires, *Design and Conception Rules for Electrical Components of Nuclear Islands*, AFCEN RCC-E [2005]
18. Association Française pour les règles de conception, de construction et de surveillance en exploitation des Chaudières Electro-Nucléaires, *Design and Conception Rules for Fuel Assemblies of Nuclear Power Plants of Nuclear Islands*, AFCEN RCC-C [2005]
19. Association Française pour les règles de conception, de construction et de surveillance en exploitation des Chaudières Electro-Nucléaires, *EPR Technical Code for Civil Works*, AFCEN ETC-C [2010]
20. Commission des codes du bâtiment et de prévention des incendies, *Code national du bâtiment du Canada*, Ottawa [2010]
21. Centre de la sécurité des télécommunications, *Méthodologie harmonisée d'évaluation des menaces et des risques (EMR)*, TRA-1 [2007]
22. Electric Power Research Institute (EPRI), *Methodology for Developing Seismic Fragilities*, TR-103959 [1994]
23. Electric Power Research Institute, Technical Report, *Nuclear Power Plant Equipment Qualification Reference Manual*, Revision 1 [2010]
24. Norme européenne NF EN 1337-3, Appareils d'appui structuraux – Partie 3 : Appareils d'appui en élastomère [septembre 2005]
25. Norme européenne NF EN 1337-1, Appareils d'appui structuraux – Partie 3 : Indications générales [décembre 2000]
26. Norme européenne NF EN 15129, *Dispositifs antisismiques* [janvier 2010]
27. Institute of Electrical and Electronics Engineers (IEEE), *Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems*, Standard 379-1988 [1988]
28. Institute of Electrical and Electronics Engineers, *IEEE Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations*, IEEE 344-2004 [2004]
29. Institute of Electrical and Electronics Engineers, *IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations*, IEEE 603 [2009]
30. Institute of Electrical and Electronics Engineers, *IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations*, IEEE 7-4.3.2 [2010]
31. Institute of Electrical and Electronics Engineers, IEEE 497-2010 - *IEEE Standard Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating Stations* [2010]
32. Institute of Electrical and Electronics Engineers, (IEEE), *IEEE Standard for Qualification of Equipment Used in Nuclear Facilities*, IEEE-627-2010 [2010]
33. Institute of Electrical and Electronics Engineers, *IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations*, IEEE-323-2003 [2003]
34. Institute of Electrical and Electronics Engineers, *IEEE Guide for the Application of Human Factors Engineering to Systems, Equipment, and Facilities of Nuclear Power Generating Stations*, IEEE 1023 [2004]

35. Institute of Electrical and Electronics Engineers, *IEEE Guide for the Application of Human Factors Engineering in the Design of Computer-Based Monitoring and Control Displays for Nuclear Power Generating Stations*, IEEE 1289 [1998]
36. Institute of Electrical and Electronics Engineers, *IEEE 308-2001, IEEE Standard Criteria for Class 1E Power Systems for Nuclear Power Generating Stations* [2001]
37. Institute of Electrical and Electronics Engineers, *IEEE 387-1995, IEEE Standard Criteria for Diesel-Generator Units Applied as Standby Power Supplies for Nuclear Power Generating Stations* [1995]
38. Institute of Electrical and Electronics Engineers, *IEEE 141-1993, IEEE Recommended Practice for Electric Power Distribution for Industrial Plants, (Red Book)* [1993]
39. Institute of Electrical and Electronics Engineers, *IEEE 242-2001, IEEE Recommended Practice for Protection and Coordination of Industrial and Commercial Power Systems, (IEEE Buff Book)* [2001]
40. Institute of Electrical and Electronics Engineers, *IEEE 279-1971, IEEE Standard: Criteria for Protection Systems for Nuclear Power Generating Stations* [1971]
41. Institute of Electrical and Electronics Engineers, *IEEE 665-1995, IEEE Standard for Generating Station Grounding (confirmée en 2001)*
42. Institute of Electrical and Electronics Engineers, *IEEE 1050-1996, Guide for Instrumentation and Control Equipment Grounding in Generating Stations* [1996]
43. Institute of Electrical and Electronics Engineers, *IEEE C62.23-1995, IEEE Application Guide for Surge Protection of Electric Generating Plants*
44. Organisation internationale de normalisation, norme ISO 9001:2008, *Systèmes de management de la qualité – Exigences* [2008]
45. Commission électrotechnique internationale (CEI), *Centrales nucléaires de puissance – Instrumentation et contrôle-commande importants pour la sûreté – Exigences générales pour les systèmes*, CEI 61513 [août 2011]
46. Commission électrotechnique internationale (CEI), *Centrales nucléaires de puissance – Instrumentation et contrôle-commande importants pour la sûreté – Aspects logiciels des systèmes programmés réalisant des fonctions de catégorie A*, CEI 60880 [mai 2006]
47. Commission électrotechnique internationale (CEI), *Centrales nucléaires de puissance – Instrumentation et contrôle-commande importants pour la sûreté – Exigences applicables à la conception du matériel des systèmes informatisés*, CEI 60987 [août 2007]
48. Commission électrotechnique internationale (CEI), *Centrales nucléaires de puissance – Instrumentation et contrôle-commande importants pour la sûreté – Essais de surveillance*, CEI 60671 [mai 2007]
49. Commission électrotechnique internationale (CEI), *Centrales nucléaires de puissance – Instrumentation et contrôle-commande importants pour la sûreté – Méthodes d'évaluation des performances des chaînes d'instrumentation des systèmes de sûreté*, CEI 62385 [juin 2007]
50. Commission électrotechnique internationale (CEI), *Centrales nucléaires – Équipements électriques de sûreté – Qualification*, CEI 60780, deuxième édition, [1998]
51. Commission électrotechnique internationale (CEI), *Centrales nucléaires de puissance – Conception des salles de commande – Analyse fonctionnelle et affectation des fonctions*, CEI 61839 [juillet 2000]

52. Commission électrotechnique internationale (CEI), *Centrales nucléaires de puissance – Salles de commande – Conception*, CEI 60964 [février 2009]
53. Commission électrotechnique internationale (CEI), *Centrales nucléaires de puissance – Salles de commande – Points de commande supplémentaires pour l'arrêt des réacteurs sans accès à la salle de commande principale (salle de commande de repli)*, CEI 60965 [juillet 2009]
54. National Fire Protection Association, (NFPA), NFPA 804: *Standard for Fire Protection for Advanced Light Water Reactor Electric Generating Plants* [2010]
55. National Fire Protection Association, NFPA 805: *Performance-Based Standard for Fire Protection for Light Water Reactor Electric Generating Plants* [2010]
56. National Fire Protection Association, *Fire Protection Handbook* [2008]
57. Society of Fire Protection Engineers (SFPE) *SFPE Handbook of Fire Protection Engineering* [2008]
58. Conseil national de recherches Canada, *Code national de prévention des incendies – Canada* (CNPI) [2010]
59. Agence pour l'énergie nucléaire (AEN), *Decommissioning Considerations for New Nuclear Power Plants*, NEA n° 6833, OCDE [2010]
60. Agence pour l'énergie nucléaire (AEN), *Intégration du retour d'expérience du démantèlement à la conception et l'exploitation des futures centrales nucléaires*, NEA n° 6946, OCDE [2010]
61. Nuclear Energy Institute (NEI), *Guidance for Post Fire Safe Shutdown Circuit Analysis*, NEI 00-01 [2005]
62. Nuclear Energy Institute, *Guidance for Implementing a Risk-Informed, Performance-Based Fire Protection Program under 10 CFR 50.48(c)*, NEI 04-02, Revision 1 [2005]
63. Nuclear Energy Institute, NEI 07-13, *Methodology for Performing Aircraft Impact Assessments for New Plant Designs* [2011]
64. Nuclear Energy Institute, NEI 08-09 Rev.6, *Cyber Security Plan for Nuclear Power Reactors* [2010]
65. Nuclear Information and Records Management Association/American National Standards Institute (NIRMA/ANSI), *Standard Configuration Management (CM)*, 1.0-2007
66. U.S. Department of the Army, TM 5-1300, *Structures to Resist the Effects of Accidental Explosions*, 1990. Remplacé par UFC 3-340-02 [2008]