COLLECTION NORMES DE SÛRETÉ DE L'AIEA

Systèmes d'instrumentation et de contrôle-commande importants pour la sûreté des centrales nucléaires

GUIDE DE SÛRETÉ

N° NS-G-1.3

IAEA
Agence internationale de l'énergie atomique

PUBLICATIONS DE L'AIEA CONCERNANT LA SÛRETÉ

NORMES DE SÛRETÉ

En vertu de l'article III de son Statut, l'AIEA a pour attributions d'établir ou d'adopter des normes de sûreté destinées à protéger la santé et à réduire au minimum les dangers auxquels sont exposés les personnes et les biens et de prendre des dispositions pour appliquer ces normes aux activités nucléaires pacifiques.

Les publications par lesquelles l'AIEA établit des normes paraissent dans la **collection Normes de sûreté de l'AIEA**. Cette collection couvre la sûreté nucléaire, la sûreté radiologique, la sûreté du transport et la sûreté des déchets, ainsi que la sûreté générale (c'est-à-dire l'ensemble de ces quatre domaines). Cette collection comporte les catégories suivantes: **fondements de sûreté, prescriptions de sûreté** et **guides de sûreté.**

Les normes de sûreté portent un code selon le domaine couvert : sûreté nucléaire (NS), sûreté radiologique (RS), sûreté du transport (TS), sûreté des déchets (WS) et sûreté générale (GS).

Des informations sur le programme de normes de sûreté de l'AIEA sont données sur le site suivant :

http://www-ns.iaea.org/standards/

Ce site donne accès aux textes en anglais des normes publiées et en projet. Les textes des normes publiées en arabe, chinois, espagnol, français et russe, le glossaire de la sûreté de l'AIEA et un état des normes en cours d'élaboration sont aussi consultables. Pour de plus amples informations, prière de contacter l'AIEA, B.P. 100, A-1400 Vienne (Autriche).

Tous les utilisateurs des normes de sûreté sont invités à faire connaître à l'AIEA leur expérience en la matière (par exemple en tant que base de la réglementation nationale, d'examens de la sûreté et de cours) afin que les normes continuent de répondre aux besoins des utilisateurs. Ces informations peuvent être communiquées par le biais du site Internet, par la poste (à l'adresse indiquée ci-dessus) ou par courriel (Official.Mail@iaea.org).

AUTRES PUBLICATIONS CONCERNANT LA SÛRETÉ

L'AIEA prend des dispositions pour l'application des normes et, en vertu de l'article III et du paragraphe C de l'article VIII de son Statut, elle favorise l'échange d'informations sur les activités nucléaires pacifiques et sert d'intermédiaire entre ses États Membres à cette fin.

Les rapports sur la sûreté et la protection dans le cadre des activités nucléaires sont publiés dans d'autres collections, en particulier la **collection Rapports de sûreté de l'AIEA**. Ces rapports donnent des exemples concrets et proposent des méthodes détaillées qui peuvent être utilisées à l'appui des normes de sûreté. D'autres publications de l'AIEA concernant la sûreté paraissent dans les collections **Provision for the Application of Safety Standards Series** et **Radiological Assessment Reports Series**, en anglais seulement, ainsi que dans la **collection INSAG** (Groupe international pour la sûreté nucléaire). L'AIEA édite aussi des rapports sur les accidents radiologiques et d'autres publications spéciales.

Des publications concernant la sûreté paraissent dans les collections **Documents techniques (TECDOC)** et **Cours de formation**, et en anglais uniquement dans les collections **IAEA Services Series, Practical Radiation Safety Manuals** et **Practical Radiation Technical Manuals**. Les publications concernant la sécurité paraissent dans la collection **IAEA Nuclear Security Series**.

SYSTÈMES D'INSTRUMENTATION ET DE CONTRÔLE-COMMANDE IMPORTANTS POUR LA SÛRETÉ DES CENTRALES NUCLÉAIRES

Les États ci-après sont Membres de l'Agence internationale de l'énergie atomique:

AFGHANISTAN
AFRIQUE DU SUD
ALBANIE
ALGÉRIE
ALLEMAGNE
ANGOLA
ARABIE SAOUDITE
ARGENTINE
ARMÉNIE
AUSTRALIE
AUTRICHE
AZERBAÏDJAN
BANGLADESH
BÉLARUS
BELGIQUE
BÉNIN
BOLIVIE
BOSNIE-HERZÉGOVINE
BOTSWANA
BRÉSIL
BULGARIE
BURKINA FASO
CAMEROUN
CANADA
CHILI
CHINE
CHYPRE
COLOMBIE
CORÉE, RÉPUBLIQUE DE
COSTA RICA
CÔTE D'IVOIRE
CROATIE
CUBA
DANEMARK
ÉGYPTE
EL SALVADOR
ÉMIRATS ARABES UNIS
ÉQUATEUR
ÉRYTHRÉE
ESPAGNE
ESTONIE
ÉTATS-UNIS D'AMÉRIQUE
ÉTHIOPIE
FÉDÉRATION DE RUSSIE
FINLANDE
FRANCE
GABON
GÉORGIE
GHANA
GRÈCE
GUATEMALA
HAÏTI
HONDURAS
HONGRIE
ILES MARSHALL
INDE
INDONÉSIE
IRAN, RÉP. ISLAMIQUE D'
IRAQ
IRLANDE
ISLANDE
ISRAËL
ITALIE
JAMAHIRIYA ARABE LIBYENNE
JAMAÏQUE
JAPON
JORDANIE
KAZAKHSTAN
KENYA
KIRGHIZISTAN
KOWEÏT
LETTONIE
L'EX-RÉPUBLIQUE YOUGOSLAVE DE MACÉDOINE
LIBAN
LIBÉRIA
LIECHTENSTEIN
LITUANIE
LUXEMBOURG
MADAGASCAR
MALAISIE
MALI
MALTE
MAROC
MAURICE
MEXIQUE
MONACO
MONGOLIE
MYANMAR
NAMIBIE
NICARAGUA
NIGER
NIGERIA
NORVÈGE
NOUVELLE-ZÉLANDE
OUGANDA
OUZBÉKISTAN
PAKISTAN
PANAMA
PARAGUAY
PAYS-BAS
PÉROU
PHILIPPINES
POLOGNE
PORTUGAL
QATAR
RÉPUBLIQUE ARABE SYRIENNE
RÉPUBLIQUE CENTRAFRICAINE
RÉPUBLIQUE DÉMOCRATIQUE DU CONGO
RÉPUBLIQUE DE MOLDOVA
RÉPUBLIQUE DOMINICAINE
RÉPUBLIQUE TCHÈQUE
RÉPUBLIQUE-UNIE DE TANZANIE
ROUMANIE
ROYAUME-UNI DE GRANDE-BRETAGNE ET D'IRLANDE DU NORD
SAINT-SIÈGE
SÉNÉGAL
SERBIE ET MONTÉNÉGRO
SEYCHELLES
SIERRA LEONE
SINGAPOUR
SLOVAQUIE
SLOVÉNIE
SOUDAN
SRI LANKA
SUÈDE
SUISSE
TADJIKISTAN
THAÏLANDE
TUNISIE
TURQUIE
UKRAINE
URUGUAY
VENEZUELA
VIETNAM
YÉMEN
ZAMBIE
ZIMBABWE

Le Statut de l'Agence a été approuvé le 23 octobre 1956 par la Conférence sur le Statut de l'AIEA, tenue au Siège de l'Organisation des Nations Unies, à New York; il est entré en vigueur le 29 juillet 1957. L'Agence a son Siège à Vienne. Son principal objectif est «de hâter et d'accroître la contribution de l'énergie atomique à la paix, la santé et la prospérité dans le monde entier».

Imprimé par l'AIEA en Autriche
Juin 2005
STI/PUB/1116

COLLECTION NORMES DE SÛRETÉ N° NS-G-1.3

SYSTÈMES D'INSTRUMENTATION ET DE CONTRÔLE-COMMANDE IMPORTANTS POUR LA SÛRETÉ DES CENTRALES NUCLÉAIRES

Guide de sûreté

AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE
VIENNE, 2005

CE VOLUME DE LA COLLECTION SÉCURITÉ
EST PUBLIÉ ÉGALEMENT
EN ANGLAIS, EN CHINOIS, EN ESPAGNOL ET EN RUSSE.

SYSTÈMES D'INSTRUMENTATION
ET DE CONTRÔLE-COMMANDE
IMPORTANTS POUR LA SÛRETÉ
DES CENTRALES NUCLÉAIRES
STI/PUB/1116
ISBN 92–0–201305–5
ISSN 1020–5829

AVANT-PROPOS

par Mohamed ElBaradei
Directeur général

Une des fonctions statutaires de l'AIEA est d'établir ou d'adopter des normes de sûreté destinées à protéger la santé, les personnes et les biens dans le cadre du développement et de l'utilisation de l'énergie nucléaire à des fins pacifiques et de prendre des dispositions pour appliquer ces normes à ses propres opérations, ainsi qu'à celles pour lesquelles elle fournit une assistance et, à la demande des parties, aux opérations effectuées en vertu d'un accord bilatéral ou multilatéral ou, à la demande d'un État, à telle ou telle des activités de cet État dans le domaine de l'énergie nucléaire.

Les organes consultatifs ci-après supervisent l'élaboration des normes de sûreté: Commission consultative pour les normes de sûreté (ACSS), Comité consultatif pour les normes de sûreté nucléaire (NUSSAC), Comité consultatif pour les normes de sûreté radiologique (RASSAC), Comité consultatif pour les normes de sûreté relatives au transport (TRANSSAC) et Comité consultatif pour les normes de sûreté relatives aux déchets (WASSAC). Les États Membres sont largement représentés au sein de ces comités.

Afin que les normes de sûreté puissent faire l'objet du consensus le plus large possible, elles sont aussi soumises à tous les États Membres pour observations avant d'être approuvées par le Conseil des gouverneurs de l'AIEA (fondements de sûreté et prescriptions de sûreté) ou par le Comité des publications au nom du Directeur général (guides de sûreté).

Les normes de sûreté de l'AIEA n'ont pas force obligatoire pour les États Membres, mais ceux-ci peuvent, à leur discrétion, les adopter pour application, dans le cadre de leur réglementation nationale, à leurs propres activités. L'AIEA est tenue de les appliquer à ses propres opérations et à celles pour lesquelles elle fournit une assistance. Tout État souhaitant conclure un accord avec l'AIEA en vue d'obtenir son assistance pour le choix du site, la conception, la construction, les essais de mise en service, l'exploitation ou le déclassement d'une installation nucléaire ou toute autre activité est tenu de se conformer aux parties des normes qui se rapportent aux activités couvertes par l'accord. Quoi qu'il en soit, il appartient toujours aux États de prendre les décisions finales et d'assumer les responsabilités juridiques dans le cadre d'une procédure d'autorisation.

Bien que les normes de sûreté établissent une base essentielle pour la sûreté, il est aussi parfois nécessaire d'incorporer des prescriptions plus détaillées conformément à l'usage national. De surcroît, il y aura souvent des aspects particuliers qui devront être soumis, cas par cas, à l'appréciation de spécialistes.

La protection physique des produits fissiles et des matières radioactives, comme celle de la centrale nucléaire dans son ensemble, est mentionnée là où il convient, mais n'est pas traitée en détail; pour connaître les obligations des États à cet égard, il convient de se reporter aux instruments et aux publications pertinents élaborés sous les auspices de l'AIEA. Les aspects non radiologiques de la sécurité du travail et de la protection de l'environnement ne sont pas non plus explicitement examinés; il est admis que les États devraient se conformer aux obligations et aux engagements internationaux qu'ils ont contractés dans ce domaine.

Les prescriptions et recommandations présentées dans les normes de sûreté de l'AIEA peuvent n'être pas pleinement satisfaites par certaines installations anciennes. Il appartient à chaque État de statuer sur la manière dont les normes seront appliquées à ces installations.

Il convient d'attirer l'attention des États sur le fait que les normes de sûreté de l'AIEA, bien que n'étant pas juridiquement contraignantes, visent à faire en sorte que l'énergie nucléaire et les matières radioactives utilisées à des fins pacifiques le soient d'une manière qui permette aux États de s'acquitter des obligations qui leur incombent en vertu des principes du droit international et de règles recueillant l'assentiment général, tels que ceux qui concernent la protection de l'environnement. En vertu de l'un de ces principes, le territoire d'un État ne doit pas servir à des activités qui portent préjudice à un autre État. Les États sont donc tenus de faire preuve de prudence et d'observer des normes de conduite.

Comme toute autre activité, les activités nucléaires civiles menées sous la juridiction des États sont soumises aux obligations que les États contractent au titre de conventions internationales, en sus des principes du droit international généralement acceptés. Les États sont censés adopter au niveau national les lois (et la réglementation), ainsi que les normes et mesures dont ils peuvent avoir besoin pour s'acquitter efficacement de toutes leurs obligations internationales.

NOTE DE L'ÉDITEUR

Lorsqu'une norme comporte un appendice, ce dernier est réputé faire partie intégrante de cette norme et avoir le même statut que celle-ci. En revanche, les annexes, notes infrapaginales et bibliographies ont pour objet de donner des précisions ou des exemples concrets qui peuvent être utiles au lecteur.

Le présent a été employé pour énoncer des prescriptions, des responsabilités et des obligations. Le conditionnel sert à énoncer des recommandations concernant une option souhaitable.

La version anglaise du texte est celle qui fait autorité. La présente traduction a été établie sous les auspices de l'Institut de radioprotection et de sûreté nucléaire (IRSN) (France).

TABLE DES MATIÈRES

1. INTRODUCTION

GÉNÉRALITÉS

1.1. Le présent guide de sûreté a été élaboré dans le cadre du programme de l'AIEA d'établissement de normes de sûreté pour les centrales nucléaires. Il vient en complément du document n° NS-R-1 de la collection Normes de sûreté intitulé «Sûreté des centrales nucléaires: conception» [1], qui établit les exigences relatives à la conception permettant de garantir la sûreté des centrales nucléaires. Ce guide de sûreté décrit comment il faudrait procéder pour satisfaire aux exigences relatives aux systèmes d'instrumentation et de contrôle-commande (CCI) importants pour la sûreté.

1.2. La présente publication est une révision et une combinaison de deux guides de sûreté précédents: n° 50-SG-D3 et 50-SG-D8 de la collection Sécurité qui sont remplacés par ce nouveau guide de sûreté.

1.3. La révision prend en compte les développements des systèmes CCI importants pour la sûreté intervenus depuis la publication des guides de sûreté antérieurs en 1980 et 1984, respectivement. Les principales modifications résultent des points suivants:

— Dans ce guide de sûreté, les développements relatifs à l'utilisation de systèmes CCI programmés importants pour la sûreté sont pris en considération.
— Cette révision des publications n° 50-SG-D3 et 50-SG-D8 de la collection Sécurité prend soin de traiter tous les systèmes CCI importants pour la sûreté. L'organisation et la présentation des directives ont été faites en relation avec les exigences et critères exposés dans la réf. [1].
— Ce guide de sûreté est destiné à être lu conjointement et en relation avec les Exigences relatives à la conception [1] et les guides de sûreté des domaines connexes, concernant le logiciel [2] et l'assurance de la qualité (réf. [3], guides de sûreté Q3 et Q10).
— Ce guide émet des recommandations concernant le classement des systèmes CCI importants pour la sûreté, à partir d'autres normes internationales.

OBJECTIF

1.4. L'objectif de ce guide de sûreté est de fournir des recommandations sur la conception des systèmes CCI importants pour la sûreté des centrales

nucléaires, y compris tous les composants des systèmes CCI, depuis les capteurs affectés aux systèmes mécaniques jusqu'aux actionneurs, interfaces opérateur et appareils auxiliaires.

1.5. Ce guide de sûreté traite principalement des exigences relatives à la conception des systèmes CCI importants pour la sûreté. Il s'étend sur les paragraphes de la réf. [1] relatifs au domaine des systèmes CCI importants pour la sûreté.

1.6. Cette publication est principalement destinée aux concepteurs de centrales nucléaires et aussi aux propriétaires et/ou exploitants et responsables de la réglementation des centrales nucléaires.

CHAMP D'APPLICATION

1.7. Le présent guide de sûreté émet des recommandations générales sur les systèmes CCI importants pour la sûreté qui s'appliquent dans une large mesure à de nombreuses centrales nucléaires. Des exigences et limitations plus détaillées concernant la sûreté de fonctionnement spécifiques à un type de centrale particulier devraient être établies dans le cadre du processus de conception. Les présentes recommandations se concentrent sur les principes de conception des systèmes importants pour la sûreté qui méritent une attention particulière, et elles devraient être appliquées à la conception de nouveaux systèmes CCI ainsi qu'à la modernisation des systèmes existants. Des recommandations sont données sur la façon dont les principes de conception devraient être appliqués sur la base d'une méthode de classement des systèmes en fonction de leur importance pour la sûreté.

1.8. Selon les définitions données dans la réf. [1], les systèmes CCI importants pour la sûreté sont les systèmes CCI qui font partie d'un groupe de sûreté et les systèmes CCI dont le dysfonctionnement ou la défaillance pourrait conduire à une exposition aux rayonnements du personnel du site ou des personnes du public. Ce sont, par exemple:

— le système de protection du réacteur,
— les systèmes de contrôle-commande du réacteur,
— les systèmes servant à surveiller et contrôler le refroidissement normal du réacteur,
— les systèmes servant à surveiller et contrôler les systèmes d'alimentation électrique de secours,
— les systèmes d'isolement du confinement.

1.9. Le n° 387 de la collection Rapports techniques de l'AIEA [4] présente un aperçu des concepts et des exemples de systèmes abordés dans ce guide de sûreté et peut fournir des données de base utiles pour certains utilisateurs.

STRUCTURE

1.10. La présente publication est organisée selon les exigences et les critères de la réf. [1] et fournit des recommandations en ce qui concerne les systèmes CCI importants pour la sûreté.

1.11. La section 2 traite de l'identification des fonctions et des systèmes CCI dans le cadre de ce guide de sûreté et de leur classement ultérieur en systèmes et fonctions de sûreté et systèmes et fonctions liés à la sûreté. La section 3 décrit la détermination du dimensionnement des systèmes CCI importants pour la sûreté. La section 4 donne des recommandations pour la conception des systèmes CCI importants pour la sûreté. Elle comporte des recommandations qui s'appliquent à tous les systèmes CCI importants pour la sûreté ainsi que des recommandations qui ne s'appliquent qu'aux systèmes de sûreté. L'applicabilité de ces recommandations à ces deux classes est identifiée dans le texte et résumée dans le tableau I. La section 5 fournit d'autres recommandations spécifiques à certains systèmes CCI, à savoir les systèmes de protection, les sources d'énergie et les systèmes programmés. Les recommandations concernant ces systèmes comprennent les recommandations générales données dans la section 4 et les recommandations spécifiques données dans la section 5. La section 6 s'étend sur les recommandations données dans la section 4 dans le domaine des interfaces homme–machine. La section 7 développe les recommandations données dans la section 4 concernant le processus de conception pour garantir la qualité.

1.12. Les sujets abordés dans les sections 4, 5, 6 et 7 sont structurés de manière à faire ressortir la pertinence de chaque rubrique pour la sûreté et les exigences relatives à la conception. Des recommandations spécifiques sont données pour chaque sujet.

2. SYSTÈMES D'INSTRUMENTATION ET DE CONTRÔLE-COMMANDE IMPORTANTS POUR LA SÛRETÉ

2.1. Les exigences relatives à la conception demandent que tous les systèmes et composants CCI (y compris le logiciel CCI) qui sont des éléments importants pour la sûreté soient tout d'abord identifiés puis classés sur la base de leur fonction et de leur importance pour la sûreté (réf. [1], par. 5.1).

IDENTIFICATION DES SYSTÈMES CCI

2.2. Les systèmes CCI importants pour la sûreté sont identifiés en se basant sur l'identification des fonctions de sûreté CCI nécessaires et sur la définition des systèmes qui remplissent certaines combinaisons de ces fonctions. Le processus type d'identification des systèmes importants pour la sûreté est abordé dans cette section.

Fonctions de la centrale importantes pour la sûreté

2.3. Il existe un certain nombre de fonctions vitales qui doivent être remplies pour garantir le fonctionnement sûr et efficace d'une centrale nucléaire et qui peuvent impliquer l'utilisation de systèmes CCI. Les principales fonctions de sûreté suivantes qui doivent être remplies pour garantir la sûreté sont identifiées dans la réf. [1], par. 4.6:

— contrôle de la réactivité,
— évacuation de la chaleur du cœur,
— confinement des matières radioactives et contrôle des rejets en exploitation, ainsi que limitation des rejets accidentels.

2.4. Une approche systématique devrait être suivie pour identifier les systèmes, structures et composants qui sont nécessaires pour remplir ces fonctions de sûreté à la suite d'un événement initiateur postulé (EIP).

2.5. Ces fonctions de sûreté principales sont décrites et traitées de façon détaillée dans les paragraphes suivants afin de décrire de manière plus approfondie les fonctions qui doivent être remplies pour assurer la sûreté. Cet ensemble étendu de fonctions inclut les fonctions nécessaires pour éviter ou prévenir les conditions accidentelles ainsi que les fonctions nécessaires pour limiter les conséquences des conditions accidentelles. Elles sont accomplies,

suivant le cas, en utilisant les structures, systèmes et composants mis en place pour le fonctionnement normal, ceux installés pour empêcher les incidents d'exploitation prévus de conduire à des conditions accidentelles et ceux mis en place pour limiter les conséquences des conditions accidentelles.

Les fonctions de sûreté destinées au contrôle de la réactivité:

— permettent le contrôle normal de la réactivité dans des limites sûres;
— préviennent les transitoires de réactivité inacceptables;
— arrêtent le réacteur lorsque cela est nécessaire pour éviter que les incidents d'exploitation prévus ne conduisent à des conditions accidentelles de dimensionnement;
— arrêtent le réacteur pour limiter les conséquences des conditions accidentelles;
— maintiennent le réacteur dans une condition d'arrêt sûr après les actions de mise à l'arrêt.

Les fonctions de sûreté destinées à l'évacuation de la chaleur du cœur:

— évacuent la chaleur du cœur lors du fonctionnement en puissance;
— évacuent la chaleur résiduelle lors d'états de fonctionnement représentatifs et dans des conditions accidentelles de dimensionnement lorsque l'enveloppe du réfrigérant du cœur est intacte;
— maintiennent une réserve de réfrigérant suffisante pour refroidir le cœur lors des états d'exploitation normaux et à la suite d'EIP;
— évacuent la chaleur du cœur après une défaillance de l'enveloppe sous pression du réfrigérant du cœur afin de limiter l'endommagement du combustible;
— transfèrent la chaleur des sources froides intermédiaires utilisées pour l'évacuation de la chaleur du cœur vers la source froide finale.

Les fonctions de sûreté utilisées pour le confinement des matières radioactives et le contrôle des rejets en exploitation, ainsi que pour la limitation des rejets accidentels:

— maintiennent l'intégrité des gaines du combustible dans le cœur du réacteur;
— maintiennent l'intégrité de l'enveloppe sous pression du réfrigérant du réacteur;
— limitent le rejet de matières radioactives et minimisent l'exposition aux rayonnements du public et du personnel.

2.6. Les fonctions susmentionnées importantes pour la sûreté devraient être remplies par des systèmes nécessitant des études particulières parmi lesquels se trouvent certains systèmes CCI. Pour les systèmes CCI, les fonctions principales types importantes pour la sûreté incluent:

— les fonctions de protection,
— les fonctions de contrôle-commande,
— les fonctions de surveillance et d'affichage,
— les fonctions de test.

2.7. En outre, il existe des fonctions support, également importantes pour la sûreté, qui devraient être accomplies en support aux fonctions principales. Ces fonctions support sont, entre autres, l'alimentation électrique, pneumatique et hydraulique, la transmission des données et les fonctions de test et de surveillance qui aident les systèmes à remplir les fonctions principales.

2.8. Les fonctions principales des systèmes CCI, importantes pour la sûreté, peuvent être caractérisées comme suit:

Fonctions de protection

2.9. Les fonctions de protection fournissent une ligne de défense contre les défaillances des autres systèmes de la centrale. Elles comptent parmi les fonctions de sûreté les plus critiques et se rapportent directement à la sûreté nucléaire du point de vue de la protection du personnel et du public en cas de défaillance grave.

Fonctions de contrôle-commande

2.10. Les fonctions de contrôle-commande apportent la garantie que la centrale est contrôlée et reste dans les limites de son domaine de fonctionnement dans des conditions normales et anormales. Les fonctions de contrôle-commande peuvent également limiter les effets des transitoires de la centrale ou des EIP, contribuant ainsi à la sûreté nucléaire en minimisant les sollicitations imposées aux fonctions de protection.

Fonctions de surveillance et d'affichage

2.11. Les fonctions de surveillance et d'affichage fournissent l'interface entre la centrale et le personnel de conduite et de maintenance. Ces fonctions sont importantes pour la sûreté car elles permettent au personnel de la centrale de

contrôler les transitoires et de maintenir la centrale dans des limites de fonctionnement sûres.

Fonctions de test

2.12. Les fonctions de test garantissent la disponibilité et l'efficacité des autres fonctions importantes pour la sûreté et confirment qu'elles n'ont pas été dégradées.

Exemples de systèmes CCI importants pour la sûreté

2.13. La liste suivante, organisée selon les fonctions associées de la centrale importantes pour la sûreté, donne des exemples de systèmes CCI importants pour la sûreté.

2.14. Les systèmes CCI mis en place pour remplir des fonctions en rapport avec le contrôle de la réactivité incluent:

— les systèmes d'arrêt du réacteur;
— les systèmes utilisés pour surveiller ou maintenir les paramètres de la centrale à l'intérieur
  • des limites de fonctionnement importantes pour la sûreté (comme les systèmes de contrôle de la température du réfrigérant), et
  • des limites adoptées comme conditions initiales dans l'analyse de sûreté (comme les systèmes de contrôle des limites de puissance du réacteur);
— des systèmes dont le dysfonctionnement ou la défaillance peut solliciter les systèmes ayant des fonctions de protection, comme les systèmes de contrôle de la réactivité;
— des systèmes qui remplissent des fonctions importantes pour maintenir des conditions d'arrêt sûres, par exemple les dispositifs permettant de calculer la marge à la criticité;
— des systèmes qui remplissent des fonctions importantes pour la prévention, la terminaison et la réduction des conséquences des incidents d'exploitation prévus ou des conditions accidentelles de dimensionnement, par exemple les systèmes de réduction lente de la puissance du réacteur;
— des systèmes mis en place spécialement pour servir de secours diversifié aux systèmes remplissant des fonctions de protection, par exemple les systèmes qui atténuent les conséquences des transitoires sans arrêt d'urgence ou les systèmes qui prennent en compte les erreurs possibles de conception.

2.15. Les systèmes CCI mis en place pour remplir des fonctions liées à l'évacuation de la chaleur du cœur incluent:

— les systèmes, comme les systèmes de protection du réacteur et les systèmes de commande des systèmes de sûreté, qui déclenchent automatiquement la mise en route des systèmes garantissant que les limites de conception spécifiées ne sont pas dépassées à la suite d'incidents d'exploitation prévus, détectant les conditions accidentelles de dimensionnement et limitant leurs conséquences ou annulant des actions dangereuses du système de contrôle-commande;
— les systèmes qui surveillent ou contrôlent les conditions environnementales de la centrale qui sont nécessaires au bon fonctionnement des équipements de la centrale importants pour la sûreté et l'habitabilité.

2.16. Les systèmes CCI mis en place pour remplir les fonctions de confinement des matières radioactives et contrôler les rejets en exploitation, ainsi que la limitation des rejets accidentels, incluent:

— les systèmes dont le dysfonctionnement ou la défaillance pourrait entraîner un rejet de matières radioactives dans l'environnement et pour lesquels aucun système de sûreté n'est prévu, par exemple ceux qui contrôlent la gestion des déchets et le refroidissement du combustible usé;
— les systèmes utilisés pour détecter et mesurer les fuites du système de refroidissement du réacteur;
— les systèmes qui surveillent ou contrôlent les phénomènes naturels ou d'origine humaine qui pourraient nuire à la sûreté, par exemple les détecteurs d'activité sismique;
— les systèmes utilisés pour surveiller et évaluer les accidents, par exemple ceux qui surveillent et enregistrent, selon les besoins, la pression de l'enceinte, l'activité de l'enceinte, le refroidissement du cœur du réacteur, les rejets radioactifs dans l'environnement et les données météorologiques.

2.17. Les systèmes CCI mis en place pour aider à l'accomplissement des autres fonctions importantes pour la sûreté incluent:

— les systèmes qui fournissent une fonction support à plusieurs systèmes CCI importants pour la sûreté, par exemple les systèmes de communication des données numériques qui transmettent les signaux entre les systèmes et entre les composants des systèmes;

— les systèmes utilisés pour surveiller l'état des systèmes de sûreté, par exemple ceux qui surveillent la défaillance des circuits de sûreté et les défauts des conduites, vannes ou pompes des systèmes de sûreté;
— les systèmes qui peuvent être utilisés pour le fonctionnement des systèmes de sûreté, par exemple pour tester le système de protection;
— les autres applications des systèmes CCI importantes pour la sûreté, par exemple celles relatives à la communication, à la détection et à l'extinction des incendies et au contrôle d'accès.

Types de système CCI importants pour la sûreté

2.18. En fonction de l'identification des fonctions de sûreté qui doivent être remplies, les systèmes CCI sont mis en place pour accomplir des fonctions importantes pour la sûreté. Les types de système suivants sont couramment utilisés.

Systèmes de protection

2.19. Les systèmes de protection sont un type particulièrement important de systèmes CCI importants pour la sûreté. D'après les exigences relatives à la conception (réf. [1], par. 6.80), le «système de protection doit être conçu de façon:

1) à faire fonctionner automatiquement les systèmes appropriés, y compris, s'il y a lieu, les systèmes d'arrêt du réacteur, de sorte que les limites de conception spécifiées ne soient pas dépassées à la suite d'incidents de fonctionnement prévus;
2) à détecter les accidents de dimensionnement et à faire fonctionner les systèmes requis pour maintenir les conséquences de ces accidents dans les limites de la base de conception;
3) à être capable de compenser les actions non sûres du système de commande».

2.20. Il faut noter que le terme 'système de protection' n'est pas utilisé par tous les États Membres et qu'il existe des variations acceptables sur la structure détaillée du système ou des systèmes qui prennent en charge ces fonctions de protection. Par exemple, certains États Membres emploient, au lieu d'un système de protection commun, des sous-systèmes CCI de systèmes de sûreté spéciaux indépendants pour remplir les fonctions de détection et de déclenchement des systèmes de sûreté comme ceux décrits précédemment.

Dans ces cas-là, les recommandations de ce guide de sûreté s'appliquent aux groupes de systèmes CCI concernés.

Systèmes de verrouillage

2.21. Les systèmes de verrouillage préviennent les situations ou opérations dangereuses, protègent le personnel et évitent les dangers. Le verrouillage empêche les actions qui pourraient entraîner un danger ou l'augmenter ou causer un endommagement de la centrale et ne déclenche habituellement aucune action visant à corriger la situation. Les fonctions de verrouillage peuvent être des fonctions actives qui agissent en continu pour empêcher une situation de dégénérer ou des fonctions passives qui empêchent une action.

2.22. Les fonctions de verrouillage peuvent être obtenues par des moyens mécaniques ou par des méthodes administratives ou électriques. Les fonctions de verrouillage mécanique ou administratif ne rentrent pas dans le cadre de ce guide de sûreté.

Systèmes de contrôle-commande

2.23. Les systèmes de contrôle-commande englobent tous les équipements et composants utilisés automatiquement ou manuellement pour contrôler les paramètres de la centrale, depuis la connexion aux capteurs du procédé jusqu'aux dispositifs de déclenchement qui ont un impact direct sur les procédés physiques affectant les valeurs des paramètres à contrôler.

2.24. Les systèmes de contrôle-commande maintiennent les variables de fonctionnement à l'intérieur des limites adoptées dans l'analyse de sûreté de la centrale. Pour que les hypothèses faites dans l'analyse de la sûreté restent valables, certains paramètres doivent être maintenus à l'intérieur des limites de conditions initiales d'un incident d'exploitation prévu ou d'un accident de dimensionnement. La probabilité que les paramètres importants restent dans ces limites spécifiées dépend de la fiabilité des systèmes de contrôle-commande qui gèrent les paramètres et de la fiabilité des systèmes d'instrumentation qui surveillent ces paramètres et signalent tout écart à l'opérateur pour qu'il mette en œuvre des actions correctives.

2.25. Les défaillances du système de contrôle-commande peuvent obliger le système de protection à réagir, c'est-à-dire qu'une défaillance d'un système de contrôle-commande peut éventuellement constituer un EIP. Toute défaillance des systèmes de contrôle-commande automatiques devrait automatiquement déclen-

cher un passage en commande manuelle. La défaillance d'un système de contrôle-commande automatique, conduisant au passage automatique en commande manuelle, devrait avertir l'opérateur de la modification du mode de commande.

Systèmes d'information

2.26. Les systèmes d'information englobent les équipements et composants tels que capteurs, les équipements qui convertissent les signaux des capteurs en signaux permettant l'affichage ou l'enregistrement, dispositifs de transmission sonore, voyants, appareils de mesure, écrans de visualisation, enregistreurs, imprimantes et affichages des positions de relayage.

2.27. Le système d'information informe les opérateurs de la centrale de l'état de sûreté des systèmes ou de la centrale permettant ainsi à ces opérateurs d'identifier les actions manuelles nécessaires au maintien de la sûreté de la centrale. En fonctionnement normal les opérateurs surveillent en continu l'état de la centrale à l'aide des tableaux de signalisation et des indicateurs ou des écrans de visualisation se trouvant dans la salle de commande principale.

2.28. Le système d'information informe également les experts en sûreté sur place et à l'extérieur du site de l'état de la centrale lors de conditions accidentelles. La salle de commande principale est, pour les opérateurs, le centre d'information et de commande de la centrale en fonctionnement normal, lors d'incidents d'exploitation prévus, d'accidents de dimensionnement et d'accidents graves. Elle peut également être utilisée comme centre principal pour diriger les activités à l'extérieur du site pendant la phase initiale des situations d'urgence.

2.29. En situation d'urgence, un grand nombre d'experts peuvent être appelés sur le site. Lorsque des zones séparées (centre de support technique, centre de secours ou centre d'intervention d'urgence) sont prévues pour accueillir les experts, ces zones devraient contenir les systèmes d'information (écrans de visualisation, procédures d'exploitation, manuels des systèmes) permettant aux experts d'accomplir leurs tâches. Les systèmes d'information peuvent comporter des lignes de communication directe avec les experts autorisés à se trouver dans la salle de commande principale.

2.30. Le système d'information enregistre ou imprime les évolutions à court et long terme des paramètres de fonctionnement importants pour la sûreté qui serviront aux analyses immédiates ou ultérieures, aux rapports internes de l'organisation d'exploitation et à ceux destinés aux autorités extérieures. Les enregistrements ou sorties sur imprimante sont conservés dans et à proximité de

la salle de commande principale (et sont éventuellement stockés sur le disque dur d'un ordinateur afin d'en faciliter l'accès) dans le cas des paramètres de fonctionnement analogiques et des signaux tout ou rien, afin de mettre à disposition les informations chronologiques sur le fonctionnement et le comportement de la centrale. Ces informations sont nécessaires en tant: (1) qu'informations support pour les équipes de conduite (en donnant les évolutions à court et long terme), (2) qu'informations opérationnelles générales pour la direction de la centrale et (3) qu'analyses à long terme du fonctionnement et des accidents.

Systèmes de limitation

2.31. Les systèmes de limitation englobent tous les équipements et composants mis en place pour réduire la fréquence des EIP et sont pris en compte dans l'analyse de la sûreté de la centrale dans cette optique si cela se justifie. Le blocage des barres de commande et la réduction de la puissance du réacteur sont des fonctions parfois mises en œuvre par les systèmes de limitation.

2.32. Certains États Membres incorporent explicitement les systèmes de limitation dans leur réglementation et leur conception. Dans d'autres États Membres, les fonctions de limitation peuvent être affectées aux systèmes de contrôle-commande normaux.

Systèmes de réduction des risques

2.33. Les systèmes de réduction des risques englobent tous les équipements et composants mis en place spécialement pour réduire la probabilité d'un endommagement du cœur dans le cas d'une séquence de défaillances multiples et pour prévenir l'événement initiateur (par exemple en activant un système d'arrêt dédié supplémentaire ou un moyen supplémentaire de mise en route du système d'eau d'alimentation de secours) plutôt que pour limiter les conséquences de l'événement (par exemple l'utilisation de générateurs diversifiés dans le cas d'une perte totale d'alimentation électrique).

2.34. Dans certains États Membres, les systèmes de réduction des risques sont incorporés explicitement dans la réglementation et la conception. Dans d'autres États Membres, les fonctions de réduction des risques peuvent être affectées aux systèmes de contrôle-commande normaux.

2.35. Il faut noter que les fonctions CCI types sont rarement mutuellement exclusives au sein d'un système; par exemple, les systèmes de contrôle-commande sont souvent la source des données utilisées par les systèmes

d'information et les systèmes de verrouillage comportent rarement des systèmes distincts.

CLASSEMENT DES SYSTÈMES CCI

2.36. Dans les par. 2.13–2.35, les systèmes importants pour la sûreté sont associés aux fonctions de sûreté principales identifiées dans les exigences relatives à la conception [1]. Toutefois, ceci n'implique aucune gradation d'importance pour la sûreté de ces systèmes CCI; un système CCI particulier peut participer à l'exécution d'une ou plusieurs fonctions principales de sûreté. La gradation de l'importance pour la sûreté de ces systèmes CCI est toutefois nécessaire et est faite grâce au classement de ces systèmes. Ce classement est exigé dans la réf. [1], par. 5.1.

2.37. En particulier, les exigences relatives à la conception exigent (réf. [1], par. 5.2) que la méthode de classement de l'importance pour la sûreté d'une structure, d'un système ou d'un composant soit principalement basée sur des méthodes déterministes, complétées le cas échéant par des méthodes probabilistes et un jugement technique et qu'il soit tenu compte de facteurs tels que:

— la ou les fonctions de sûreté à remplir;
— les conséquences d'une défaillance du système CCI;
— la probabilité pour le système CCI d'être sollicité pour accomplir une fonction de sûreté;
— à la suite d'un EIP, le moment où le système CCI sera sollicité ou la période pendant laquelle il devra fonctionner.

2.38. Dans la méthode de classement, outre la prise en considération des facteurs susmentionnés, comme exigé dans la réf. [1], les facteurs suivants devraient également être pris en compte lors de la détermination de la classe du système CCI. Les critères, comme indiqué pour les facteurs suivants à titre d'exemple, devraient être choisis de manière à fournir une indication quantitative et/ou qualitative de l'importance relative pour la sûreté du système CCI en cours de classement:

— la probabilité des EIP et la gravité potentielle de leurs conséquences si le système CCI utilisé tombe en panne (par exemple, probabilité forte, moyenne ou faible avec des conséquences importantes, moyennes ou faibles (conséquences radiologiques, par exemple));
— le potentiel du système CCI à causer lui-même un EIP (c'est-à-dire les modes de défaillances du système CCI), les mesures prises pour les

systèmes de sûreté ou pour d'autres systèmes CCI traités dans le présent guide de sûreté dans le cas d'un EIP de ce type (c'est-à-dire les mesures prises pour la détection d'une défaillance du système CCI) et la combinaison de la probabilité et des conséquences de cet EIP (c'est-à-dire la fréquence de défaillance et les conséquences radiologiques);
— la durée pendant laquelle le système est nécessaire après le déclenchement de la fonction de sûreté (par exemple, 12 heures maximum ou supérieure à 12 heures);
— la promptitude et la fiabilité avec lesquelles d'autres actions peuvent être mises en œuvre (par exemple, immédiatement/fiabilité faible, au-delà de 30 minutes/fiabilité élevée);
— la promptitude (par exemple, 12 heures maximum, plus de 12 heures) et la fiabilité avec lesquelles une défaillance du système CCI peut être détectée et corrigée.

2.39. Une fois chacun de ces facteurs étudié pour chaque système CCI, une décision devrait être prise en ce qui concerne le classement du système CCI.

2.40. Les systèmes CCI se répartissent en gros en deux classes: ceux qui remplissent des fonctions importantes pour la sûreté et ceux qui remplissent des fonctions qui ne sont pas importantes pour la sûreté (voir fig. 1). Les systèmes CCI importants pour la sûreté sont ceux utilisés pour accomplir les fonctions principales importantes pour la sûreté, comme décrit précédemment dans cette section. Au sein de la classe 'système CCI importants pour la sûreté' on distingue deux subdivisions principales:

— les 'systèmes CCI de sûreté' sont des systèmes CCI importants pour la sûreté qui remplissent les fonctions de sûreté primordiales comme identifiées dans les exigences relatives à la conception; c'est-à-dire qu'ils assurent l'arrêt sûr du réacteur ou l'évacuation de la chaleur résiduelle du cœur ou qu'ils limitent les conséquences des incidents de fonctionnement prévus et des accidents de dimensionnement;
— les 'systèmes CCI liés à la sûreté' sont des systèmes CCI importants pour la sûreté qui remplissent les autres fonctions importantes pour la sûreté qui ne sont pas prises en charge par les systèmes CCI de sûreté.

2.41. Les systèmes CCI de sûreté incluent les systèmes qui remplissent les fonctions de protection. Ces fonctions sont généralement remplies par un système dénommé système de protection du réacteur ou par les sous-systèmes CCI des systèmes de sûreté spécifiques, comme les systèmes d'arrêt du réacteur, le systèmes de refroidissement de secours du réacteur et les systèmes

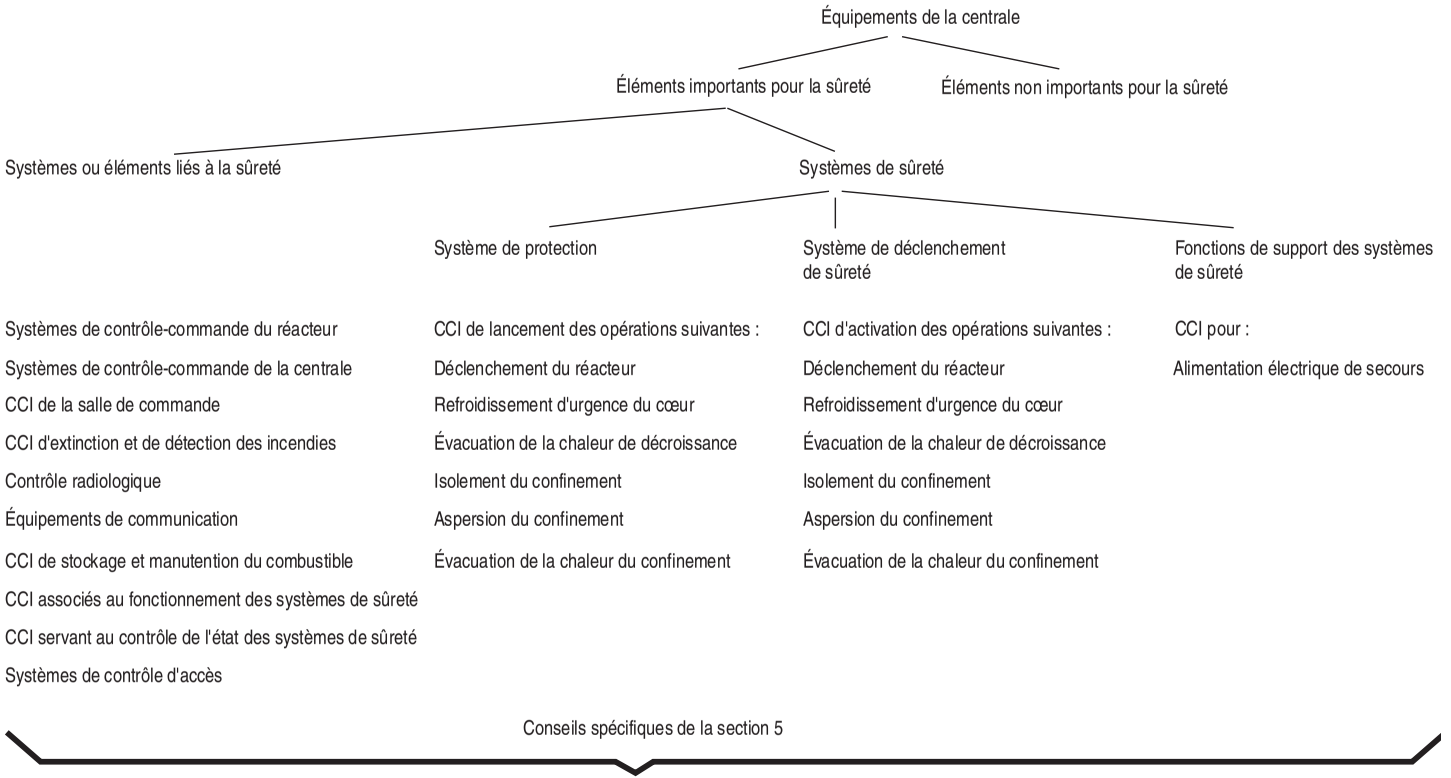

FIG. 1. Exemples de systèmes CCI importants pour la sûreté. (Les exemples sont donnés à titre indicatif. Certains systèmes sont listés dans une colonne bien qu'ils puissent également appartenir à une autre colonne, par exemple instrumentation et contrôle-commande de la salle de commande).

d'isolement du confinement. Les systèmes CCI de sûreté peuvent également remplir les fonctions de surveillance post-accidentelle et les fonctions support (par exemple, les systèmes de transmission des données principales des systèmes de protection ou des systèmes de sûreté spécifiques).

2.42. Les exemples types de systèmes CCI liés à la sûreté incluent les systèmes de contrôle-commande, les systèmes de surveillance et les systèmes d'affichage autres que ceux inclus sous la rubrique systèmes de sûreté ou classés en tant que systèmes de sûreté, systèmes de limitation ou systèmes de réduction des risques.

2.43. Il faudrait s'assurer que le classement des systèmes support nécessaires (alimentation électrique, pneumatique ou hydraulique, systèmes de lubrification) est en rapport avec le classement des fonctions de sûreté qu'ils prennent en charge.

2.44. Tous les systèmes et équipements CCI remplissant des fonctions importantes pour la sûreté devraient avoir des interfaces conçues de manière appropriée avec les systèmes et appareils de classes différentes afin de garantir que toute défaillance d'un système appartenant à une classe inférieure n'aura pas de répercussion sur un système de classe supérieure. Les équipements chargés d'empêcher la propagation d'une défaillance devraient être considérés comme appartenant à la classe supérieure.

2.45. Tous les systèmes et équipements CCI devraient être conçus, construits et entretenus de façon à ce que leur spécification, vérification et validation, assurance de la qualité, contrôle qualité et fiabilité soient en rapport avec leur classement.

3. DIMENSIONNEMENT

3.1. Le dimensionnement d'une centrale spécifie les capacités nécessaires de la centrale pour faire face à un éventail donné d'états d'exploitation et de conditions accidentelles de dimensionnement, en conformité avec les exigences qui ont été définies pour la radioprotection. Le dimensionnement inclut généralement les spécifications relatives au fonctionnement normal, les conditions créées par les EIP, les hypothèses importantes et, dans certains cas, les méthodes particulières d'analyse.

3.2. Les performances de la centrale devraient également être étudiées pour certains événements pour lesquels la centrale n'a pas été conçue, c'est-à-dire les conditions accidentelles hors-dimensionnement (ou graves). Les systèmes CCI importants pour la sûreté jouent un rôle majeur dans ces cas car ils peuvent être sollicités pour fournir les informations critiques sur l'état de la centrale ou pour fonctionner hors des limites de conception des systèmes mécaniques de la centrale.

3.3. Les exigences relatives à la conception identifient un certain nombre d'activités qui influent sur le dimensionnement des systèmes CCI importants pour la sûreté. Ces activités sont abordées dans les paragraphes suivants. (Les recommandations se rapportant à ces exigences de conception des systèmes CCI sont données dans les sections 4, 5 et 6 du présent guide de sûreté.)

CATÉGORIES RELATIVES AUX ÉTATS DE LA CENTRALE

3.4. Les exigences relatives à la conception prévoient que les états de la centrale soient identifiés et regroupés en un nombre limité de catégories en fonction de leur probabilité d'occurrence (réf. [1], par. 5.7). Les catégories couvrent généralement le fonctionnement normal, les incidents d'exploitation prévus, les accidents de dimensionnement et les accidents graves.

États d'exploitation normaux

3.5. Les exigences relatives à la conception prévoient (réf. [1], par. 5.25) que la possibilité d'accident lors d'états à puissance faible et d'arrêt du réacteur comme le démarrage, le renouvellement du combustible et la maintenance, lorsque la disponibilité de certains systèmes CCI de sûreté peut être réduite, soit prise en compte dans la conception et que les limitations appropriées concernant l'indisponibilité des systèmes CCI de sûreté soient identifiées (voir sections 4 et 5).

3.6. Le fonctionnement normal sûr d'une centrale nucléaire, destiné à couvrir tous les modes normaux de fonctionnement, devrait être pris en compte dans le processus de conception. Le processus de conception devrait établir un ensemble d'exigences et de limitations concernant le fonctionnement normal des systèmes CCI suffisant pour assurer un fonctionnement sûr de la centrale. Ces exigences devraient couvrir (réf. [1], par. 5.26):

— les informations nécessaires pour établir les points de consigne des systèmes de sûreté;

— les contraintes du système de contrôle-commande et les contraintes administratives concernant les variables de fonctionnement et autres paramètres importants;
— la maintenance, le test et l'inspection de la centrale pour garantir que les structures, systèmes et composants fonctionnent comme prévu;
— les configurations de fonctionnement clairement définies, y compris les restrictions de fonctionnement dans le cas de mises hors service des systèmes de sûreté.

3.7. Ces exigences et limitations servent de base pour établir les spécifications techniques d'exploitation qui définissent le domaine au sein duquel la centrale est autorisée à fonctionner.

Événements initiateurs postulés (EIP)

3.8. Les exigences relatives à la conception prévoient que les sollicitations que peuvent subir tous les niveaux de la défense en profondeur soient prises en compte lors de la conception de la centrale et que des mesures soient prises pour garantir que les fonctions de sûreté requises sont remplies et que les objectifs de sûreté sont atteints (réf. [1], par. 5.8). Les systèmes CCI sont mis en place pour détecter l'apparition d'une sollicitation due à un EIP et pour déclencher les actions nécessaires pour assumer les fonctions de sûreté requises et pour garantir ainsi que les limites identifiées dans le dimensionnement ne sont pas dépassées.

3.9. Afin de déterminer les capacités de détection, de traitement et de déclenchement nécessaires aux systèmes CCI pour remplir les fonctions de sûreté, une liste définitive des EIP devrait être établie dans le dimensionnement de la centrale. Dans cette liste, l'emplacement de la centrale, la fréquence d'occurrence prévue des événements et les conséquences qui en découlent en l'absence d'actions protectrices devraient être pris en compte.

3.10. Ces EIP sont étudiés individuellement dans l'analyse de la sûreté de la centrale. En outre, la nature d'un événement initiateur peut être telle qu'elle conduise à une cascade d'occurrences ou de défaillances. Ces occurrences ou défaillances consécutives à étudier dans l'analyse de la sûreté de la centrale devraient être établies dans le dimensionnement. Des limites acceptables pour les conséquences des EIP devraient être établies.

3.11. Ces EIP et les limites acceptables de leurs conséquences constituent les bases d'entrée des analyses de sûreté, qui à leur tour établissent, quantita-

tivement, les exigences relatives aux performances fonctionnelles globales des systèmes nécessaires pour accomplir la tâche de sûreté.

3.12. Ces exigences relatives aux performances fonctionnelles sont ensuite affectées aux systèmes CCI importants pour la sûreté appropriés. Le présent guide de sûreté ne traite pas spécifiquement de ces analyses de sûreté et ne donne pas les méthodes d'évaluation de l'adéquation des exigences de performances résultantes. Toutefois, il définit les informations d'entrée nécessaires pour servir de ligne directrice à la conception ultérieure du système de protection. Ce qui suit est une séquence type de ces analyses de sûreté qui peut être réitérée un certain nombre de fois au fur et à mesure que la conception progresse:

— les EIP applicables à chaque mode de fonctionnement de la centrale sont identifiés et une estimation de leur fréquence d'occurrence est faite;
— les limites acceptables de chacun de ces événements sont ensuite déterminées;
— les limites relatives aux conditions de la centrale sont établies pour éviter, grâce à une marge adéquate, que les limites acceptables des conséquences des EIP soient dépassées (voir la section 5 de la réf. [1]);
— les actions de sûreté requises pour maintenir les conditions de la centrale à l'intérieur de ces limites acceptables sont identifiées et la fiabilité de réalisation requise de ces tâches est établie;
— sur la base de la configuration matérielle de la centrale, les domaines de conditions environnementales dans lesquels les composants du système de protection doivent fonctionner sont déterminés; ils incluront les conditions ayant le potentiel de dégrader les fonctions des composants du système de protection et pour lesquelles des dispositifs comme des barrières matérielles doivent être incorporés pour conserver la capacité des composants du système de protection à remplir leurs fonctions de sûreté nécessaires.

Dimensionnement pour les accidents de dimensionnement

3.13. Les exigences relatives à la conception prévoient que, lorsqu'une action rapide et fiable est nécessaire en réponse à un EIP, des mesures soient prises pour initier automatiquement les actions nécessaires du système de sûreté afin d'éviter l'évolution vers une condition plus sévère pouvant menacer la barrière suivante. Des recommandations relatives à la conception de la réponse automatique du système de protection sont données dans la section 5.

3.14. Les exigences relatives à la conception prévoient que, lorsqu'une action rapide n'est pas obligatoire, le déclenchement manuel des systèmes ou d'autres actions de l'opérateur soient autorisés, à condition que la nécessité de ces actions soit décelée suffisamment tôt et que des procédures adéquates soient définies afin de garantir la fiabilité de ces actions. Des recommandations concernant la conception de l'interface homme–machine, garantissant que l'opérateur reçoit des informations fiables et appropriées, sont données dans la section 6.

Dimensionnement pour les accidents hors-dimensionnement

3.15. L'analyse de la sûreté envisage la possibilité d'accidents graves où certains événements très improbables peuvent menacer l'intégrité d'une grande partie ou de la totalité des barrières contre le rejet de matières radioactives. L'analyse de la sûreté identifie les séquences d'accidents graves pour lesquelles des mesures préventives ou des mesures d'atténuation des conséquences pouvant raisonnablement être mises en œuvre peuvent être identifiées. Des stratégies et procédures relatives à la gestion des accidents sont développées dans ces cas-là conformément à la section 5 de la réf. [1].

Exigences relatives à la conception des systèmes CCI

3.16. Le dimensionnement des systèmes CCI importants pour la sûreté devrait être établi à partir du dimensionnement de la centrale afin de documenter les systèmes appropriés et leurs caractéristiques. Le dimensionnement des systèmes CCI devrait être documenté conformément aux recommandations données dans la section 7 du présent guide de sûreté. Les exigences relatives aux performances, celles relatives à la disponibilité du système et les conditions environnementales (y compris les conditions pendant et après l'accident) dans lesquelles les systèmes CCI doivent fonctionner devraient être prises en compte dans la conception des systèmes CCI.

3.17. Les exigences fonctionnelles et les exigences relatives aux performances des systèmes CCI devraient être spécifiées en fonction des exigences de l'organisation d'exploitation, des capacités du personnel de la centrale, des exigences de sûreté et de l'analyse de la sûreté de la centrale nucléaire. Les exigences relatives aux performances comme la gamme de mesure des paramètres, l'exactitude, le temps de réponse, la bande passante et les niveaux des signaux de sortie devraient être déterminées. Les effets des variations transitoires ou normales des caractéristiques des systèmes d'alimentation électrique, comme les fluctuations de tension, les variations de fréquence et les

variations de pression d'air pour les équipements à air comprimé, devraient être pris en compte dans la conception des systèmes liés à la sûreté, dans la mesure nécessaire pour garantir que les systèmes CCI rempliront convenablement leurs fonctions de sûreté.

3.18. Les exigences relatives à la conception prévoient qu'un ensemble de limites de conception cohérentes avec les paramètres physiques essentiels de chaque structure, système ou composant soient spécifiées pour les états d'exploitation et les accidents de dimensionnement. Pour les systèmes CCI importants pour la sûreté, ceci devrait inclure les spécifications des conditions environnementales auxquelles le système devra résister et la durée de fonctionnement prévues dans ces conditions, pour les états d'exploitation et les conditions accidentelles de dimensionnement. Les conditions environnementales, comme les valeurs maximales ou minimales de température, pression, humidité, intensité du rayonnement ionisant, interférence électromagnétique, variations de l'alimentation électrique, vibration, corrosion, fatigue et contrainte, devraient être prises en considération.

4. RECOMMANDATIONS GÉNÉRALES RELATIVES À LA CONCEPTION

4.1. Un certain nombre d'attributs clés ou d'aspects essentiels ont été identifiés pour les systèmes CCI importants pour la sûreté. Les paragraphes suivants donnent des recommandations générales pour ces attributs. Pour chaque attribut, le raisonnement sous-tendant les recommandations est présenté et rappelle en même temps au concepteur les problèmes ou les préoccupations qui ont conduit au développement des attributs. Après chaque raisonnement, les recommandations sont structurées et présentées en fonction du classement de l'importance du système pour la sûreté (voir section 2) en utilisant deux niveaux. Le premier niveau comporte les recommandations données pour tous les systèmes importants pour la sûreté. Elles s'appliquent de la même manière à tous les systèmes, qu'il s'agisse de systèmes de sûreté ou de systèmes liés à la sûreté. Les recommandations du deuxième niveau s'appliquent spécifiquement aux systèmes de sûreté et complètent le premier niveau. Bien qu'il existe, pour chaque attribut, deux niveaux possibles de recommandations, dans certains cas les recommandations ne sont pas identifiées comme étant applicables soit à des systèmes de sûreté soit à des systèmes liés à la sûreté. L'applicabilité de ces recommandations à ces deux classes de systèmes est précisée dans le texte et résumée dans le tableau I.

TABLEAU I. APPLICABILITÉ DES PARAGRAPHES DE LA SECTION 4 AUX SYSTÈMES LIÉS À LA SÛRETÉ OU AUX SYSTÈMES DE SÛRETÉ

Paragraphe	Sujet	Applicable aux	
		Systèmes liés à la sûreté	Systèmes de sûreté
4.1–4.2	Recommandations générales relatives à la conception	oui	oui
4.3–4.7	Exigences relatives aux performances	oui	oui
4.8–4.13	Conception et fiabilité	oui	oui
4.14	Conception et fiabilité	non	oui
4.15	Critère de défaillance unique	oui	oui
4.16	Le critère	oui	oui
4.17–4.21	Application du critère de défaillance unique aux systèmes CCI importants pour la sûreté	oui	oui
4.22	Redondance	oui	oui
4.23–4.30	Diversité	oui	oui
4.31	Diversité	non	oui
4.32–4.34	Évaluation de la fiabilité	oui	oui
4.35	Fiabilité du logiciel	oui	oui
4.36–4.48	Indépendance	oui	oui
4.49–4.50	Modes de défaillance	oui	oui
4.51–4.53	Contrôle d'accès aux appareils	oui	oui
4.54–4.60	Points de consigne	oui	oui
4.61	Interface homme–machine	oui	oui
4.62–4.65	Qualification des équipements	oui	oui
4.66–4.69	Programme de qualification des équipements	oui	oui
4.70	Programme de qualification des équipements	non	oui
4.71–4.73	Méthodes de qualification	oui	oui
4.74–4.76	Qualité	oui	oui
4.77–4.78	Conception et compatibilité électromagnétique	oui	oui
4.79–4.80	Test et testabilité	oui	oui
4.81–4.83	Programme de test	oui	oui
4.84–4.85	Dispositions de test	oui	oui
4.86–4.87	Dispositions de test	non	oui
4.88–4.89	Détection de défaillance	oui	oui

TABLEAU I. (suite)

Paragraphe	Sujet	Applicable aux Systèmes liés à la sûreté	Applicable aux Systèmes de sûreté
4.90	Détection de défaillance	non	oui
4.91–4.92	Démonstration des performances du système	non	oui
4.93	Mise hors service	oui	oui
4.94–4.95	Mise hors service	non	oui
4.96	Contrôle et conduite des tests	non	oui
4.97–4.103	Maintenabilité	oui	oui
4.104–4.106	Documentation	oui	oui
4.107–4.108	Identification des éléments importants pour la sûreté	oui	oui

4.2. D'autres recommandations détaillées spécifiques à la conception de certains systèmes individuels sont données dans la section 5. Les recommandations de la section 4 associées aux recommandations spécifiques de la section 5 constituent l'ensemble des recommandations pour ces systèmes individuels.

EXIGENCES RELATIVES AUX PERFORMANCES

4.3. Les exigences relatives aux performances définissent les actions des systèmes CCI à exécuter et les caractéristiques techniques essentielles. Ces exigences incluent les gammes de mesure des variables à respecter ainsi que l'exactitude, le temps de réponse, la bande passante et les niveaux des signaux de sortie.

4.4. Les exigences de performances nécessaires et les objectifs de fiabilité des systèmes CCI importants pour la sûreté et leurs fonctions support sont établis à l'aide de l'analyse de la sûreté de la centrale concernée et sont précisés dans le dimensionnement de la centrale.

4.5. Les systèmes CCI importants pour la sûreté devraient remplir les fonctions attribuées dans l'analyse de la sûreté de la centrale et leurs caractéristiques techniques devraient être cohérentes avec les hypothèses faites dans l'analyse de la sûreté et avec les exigences du dimensionnement.

4.6. Lorsqu'un système CCI important pour la sûreté doit fonctionner dans un domaine de conditions environnementales (voir par. 4.62–4.65), il devrait être conçu de façon à satisfaire à toutes les exigences lorsqu'il est soumis à des conditions faisant partie de cette gamme.

4.7. Lorsque des équipements au sein d'un système sont utilisés pour différentes fonctions, les spécifications de performance de ces équipements (par exemple, l'exactitude et le temps de réponse) devraient être telles que les exigences relatives à toutes ces fonctions soient respectées.

CONCEPTION ET FIABILITÉ

4.8. La fiabilité est un attribut important des systèmes importants pour la sûreté. Les exigences relatives à la conception exigent que toutes les structures, systèmes et composants qui sont des éléments importants pour la sûreté soient conçus de telle manière que leur qualité et leur fiabilité soient en rapport avec leur classement. En particulier, des systèmes CCI fiables sont nécessaires pour éviter des sollicitations excessives pour l'intégrité des barrières matérielles et pour garantir la fiabilité des systèmes de protection actifs. Dans le cas d'un système de protection, la réf. [1], par. 6.81 exige spécifiquement que la conception garantisse une grande fiabilité fonctionnelle.

4.9. Pour garantir que les exigences de fiabilité du dimensionnement des systèmes CCI importants pour la sûreté sont respectées, une combinaison appropriée de critères de conception probabilistes et déterministes devrait normalement être appliquée. Pour les défaillances des systèmes liées au matériel, des valeurs quantifiées devraient normalement être définies pour la fiabilité. Dans la conception de systèmes importants pour la sûreté, des caractéristiques techniques comme la tolérance aux défaillances aléatoires, la tolérance aux défaillances de cause commune, la conception à position de repli sécurisée, l'indépendance des équipements et systèmes, la sélection d'équipements de grande qualité, la testabilité et la maintenabilité devraient être prises en considération suivant le cas.

4.10. En pratique, un compromis entre certains de ces facteurs peut être nécessaire pour optimiser les objectifs comme la limitation des temps de mise hors service pour réparation et la réduction de la fréquence des tests. Quelle que soit la manière dont un système CCI est optimisé, il devrait néanmoins satisfaire aux exigences relatives à sa fiabilité.

4.11. Plus la fiabilité des composants individuels d'un système CCI est grande, plus la fiabilité du système global est grande. Toutefois, le niveau de fiabilité des composants individuels comporte, en pratique, des limites. L'utilisation de la redondance ou de la diversité permet d'atteindre une plus grande fiabilité. Par exemple, il peut être possible de surveiller la puissance du réacteur avec plusieurs circuits ou par des moyens diversifiés comme la mesure du flux neutronique ou de la température et de la pression ou du débit de fluide. L'utilisation de la redondance apporte une protection contre les défaillances aléatoires. L'utilisation de la diversité apporte une protection contre certaines défaillances de cause commune.

4.12. La fiabilité requise pour chaque système dépend de l'importance pour la sûreté des fonctions du système et devrait normalement être spécifiée dans le dimensionnement. Plus un système CCI est important pour la sûreté, plus sa fiabilité devrait être grande. Une des méthodes pour spécifier la fiabilité exigée est d'attribuer une valeur numérique à la fiabilité pour chaque classe mentionnée dans la section 2. Une autre méthode consiste à spécifier des critères de conception déterministes pour les différentes classes en se basant sur le jugement de l'ingénieur, en affectant les systèmes aux classes puis en établissant l'ensemble des exigences qui s'appliquent à chaque classe. Tous les systèmes appartenant à une même classe sont ensuite comparés aux systèmes types. Dans la plupart des cas, on applique une combinaison de critères déterministes et probabilistes.

4.13. Certains États Membres utilisent des exigences de fiabilité explicites. Dans d'autres États Membres, la fiabilité n'est qu'un aspect de la démonstration des performances exigées pour les équipements et les systèmes de sûreté. Diverses pratiques nationales ont défini des objectifs de performance du système de protection en plus du critère de défaillance unique. Cette fiabilité supplémentaire est parfois obtenue en utilisant une protection contre les doubles défaillances dans certaines parties du système de protection et/ou en utilisant des équipements possédant une marge de conception plus grande.

4.14. Les systèmes de sûreté devraient satisfaire au critère de défaillance unique et le potentiel de défaillances de cause commune devrait être étudié. Dans certains cas, des exigences minimales de redondance en-dessous desquelles l'exploitation ne serait pas autorisée peuvent être imposées. Lors de la conception des systèmes de sûreté, les causes potentielles de défaillance devraient être soigneusement identifiées et examinées pour déterminer s'il convient d'appliquer le principe de diversité.

Critère de défaillance unique

4.15. Le critère de défaillance unique est une approche déterministe permettant de s'assurer qu'un système ou un groupe d'équipements fournissent une redondance minimale. Il se base sur le fait, confirmé par l'expérience, que même les composants et équipements fabriqués selon des normes rigoureuses de qualité peuvent parfois tomber en panne, de manière aléatoire et imprévisible à n'importe quel moment. Si un système est conçu de telle manière que ses fonctions liées à la sûreté soient assurées même s'il subit une défaillance aléatoire de l'un de ses composants, son niveau de fiabilité sera accru.

Le critère

4.16. Les exigences relatives à la conception précisent que la conformité au critère doit être considérée comme ayant été obtenue lorsque chaque groupe de sûreté aura prouvé qu'il remplit ses fonctions de sûreté dans les conditions suivantes (réf. [1], par. 5.37):

— toute conséquence d'un EIP potentiellement nuisible pour le groupe de sûreté est supposée se produire; et
— la configuration acceptable la plus défavorable des systèmes de sûreté remplissant la fonction de sûreté nécessaire est prise comme hypothèse, compte tenu des temps de mise hors service admissibles pour maintenance, test, inspection et réparation.

Un déclenchement intempestif devrait être considéré comme un mode de défaillance lorsque ce concept est appliqué. À aucun moment plus d'une défaillance n'est supposée se produire.

Application du critère de défaillance unique aux systèmes CCI importants pour la sûreté

4.17. Pour interpréter le critère de défaillance unique tel qu'il est défini dans les exigences relatives à la conception, celui-ci devra être appliqué à chaque groupe de sûreté incorporé dans la conception de la centrale. Un 'groupe de sûreté' est défini comme étant un assemblage d'équipements (fréquemment appelé 'train') qui exécute toutes les actions nécessaires à la suite d'un EIP afin que les limites spécifiées dans le dimensionnement pour cet événement ne soient pas dépassées (réf. [1], par. 5.34).

4.18. Pour les systèmes CCI auxquels le critère doit être appliqué, les fonctions de sûreté prévues des systèmes devraient d'abord être identifiées, ainsi que le groupe de sûreté nécessaire pour remplir ces fonctions. Cette identification devrait également inclure tous les autres systèmes associés à un système CCI dont la défaillance pourrait influer sur les fonctions de sûreté définies du système. Lorsque le groupe de sûreté correspondant a été identifié, l'analyse suivante devrait être effectuée:

— Les EIP du dimensionnement qui correspondent aux fonctions de sûreté prévues devraient être identifiés. Les probabilités d'occurrence des EIP devraient être déterminées. Si elles sont plausibles, les effets induits par les EIP devraient être déterminés.
— Les fonctions de sûreté, les systèmes de sûreté et les fonctions support nécessaires pour faire face aux EIP (comme l'insertion de barres de commande ou la fermeture des vannes d'isolement du confinement) devraient être déterminés. Cette liste devrait inclure les «chemins de succès alternatifs» qui pourraient permettre de remplir les fonctions de sûreté.
— L'apparition d'une défaillance unique dans le système devrait être prise comme hypothèse et les conséquences de cette défaillance unique devraient être déterminées.
— Il faudrait prouver que les fonctions de sûreté peuvent encore être remplies.
— Lors de la détermination des conséquences, le respect des exigences relatives à l'indépendance au sein des groupes de sûreté (réf. [1], par. II.11) devrait être établi. Le processus devrait inclure une phase consistant à vérifier que les groupes de sûreté ne partagent aucun équipement et qu'il n'existe aucun point de vulnérabilité, dans la mesure du possible.
— Si les redondances indépendantes et les trains des systèmes nécessaires ont été reconnus comme étant à l'épreuve d'une défaillance unique, ces systèmes n'ont pas besoin d'une analyse plus détaillée des défaillances potentielles selon le critère de défaillance unique.
— Si dans des cas exceptionnels le critère de défaillance unique n'est pas respecté, la conception est alors modifiée de manière à satisfaire au critère ou, si cela peut être justifié, une exemption est accordée. Il faudrait s'assurer ensuite que le niveau de fiabilité des systèmes est toujours très élevé à l'aide d' inspections en service, de procédures de maintenance et de conduite convenables afin de rendre non crédible leur défaillance en service.
— Si une défaillance unique peut éventuellement empêcher un système de sûreté d'être suffisamment fiable, il faudrait s'assurer que d'autres

systèmes permettant d'éviter des conséquences inacceptables sont présents.

— L'application du critère de défaillance unique suppose implicitement la détectabilité des défaillances. Toutefois, certaines défaillances peuvent ne pas être détectées par des tests ou révélées par des alarmes ou des indications anormales. Les systèmes devraient faire l'objet d'une analyse portant sur ces défaillances non détectées. De préférence, la solution devrait être de revoir la conception du système ou des programmes de test afin de rendre les défaillances facilement décelables. Si cela n'est pas possible, il faudrait supposer que ces défaillances non détectées se sont produites puis prendre comme hypothèse qu'une défaillance unique vient se rajouter. Il faudrait s'assurer que les fonctions de sûreté peuvent être remplies dans ces circonstances.
— Les actions des opérateurs prescrites pour les séquences d'événements concernées devraient être identifiées. Les effets résultant d'omissions ou de mauvaises exécutions aléatoires des actions prescrites par l'opérateur devraient être analysés. Il faudrait s'assurer que, dans ces circonstances, les fonctions de sûreté pourront être remplies.
— Dans certains États Membres, le critère de défaillance unique n'est pas appliqué lorsque l'un des trains redondants est mis hors service pour test ou maintenance. Dans ces cas-là, les temps de mise hors service admissibles qui garantissent la fiabilité nécessaire devraient être déterminés.
— Les défaillances de cause commune ne sont habituellement pas incluses dans l'analyse. Les défaillances de cause commune plausibles devraient être évaluées séparément à l'aide de mesures déterministes ou d'une analyse probabiliste de la sûreté ou d'une combinaison des deux. Une indépendance et une diversité suffisantes devraient être incorporées pour garantir de manière raisonnable que les fonctions de sûreté peuvent être remplies dans l'éventualité de défaillances de cause commune.

4.19. Bien que certains composants de systèmes CCI (câbles, cartes de circuits imprimés ou armoires) puissent être considérés comme passifs, il est rarement nécessaire ou possible d'utiliser ceci de manière efficace pour assouplir l'analyse de défaillance unique.

4.20. Le non-respect du critère de défaillance unique peut être justifié pour:

— les EIP très rares;
— les conséquences d'EIP très improbables;
— la mise hors service de certains composants pour maintenance, réparation ou test périodique, pendant des périodes limitées;

— les dispositions qui préviennent ou atténuent les conséquences des accidents graves;
— les composants pour lesquels on peut prouver que la probabilité de défaillance est suffisamment faible pour être écartée.

4.21. La réf. [5] donne d'autres recommandations concernant l'application du critère de défaillance unique et les stratégies pour obtenir la conformité.

Redondance

4.22. La redondance est couramment utilisée dans les systèmes CCI importants pour la sûreté pour atteindre les objectifs de fiabilité et/ou de conformité du système au critère de défaillance unique. Pour que la redondance soit vraiment efficace, il faudrait que l'indépendance existe (voir par. 4.36–4.48). Prise séparément, la redondance augmente la fiabilité des actions de sûreté ou des actions liées à la sûreté mais elle augmente également la probabilité de fonctionnement intempestif. La coïncidence des signaux redondants pour les équipements ou un mécanisme d'élimination des signaux intempestifs basé sur des intercomparaisons des signaux redondants sont couramment utilisés pour obtenir un bon compromis entre la fiabilité et l'absence d'actions intempestives.

Diversité

4.23. La diversité pour les systèmes CCI consiste à surveiller différents paramètres en utilisant différentes technologies, différents algorithmes ou logiques ou différents moyens de déclenchement afin d'offrir plusieurs possibilités pour détecter et répondre à un événement significatif. La diversité offre une défense contre les défaillances de cause commune, complète le principe de défense en profondeur et accroît la probabilité d'exécution des tâches de sûreté lorsqu'elles sont nécessaires. Les défenses à différents niveaux de profondeur peuvent également être différentes entre elles. Les types de diversité pouvant être pris en considération incluent la diversité humaine, la diversité de conception, la diversité logicielle, la diversité fonctionnelle, la diversité des signaux, la diversité des équipements et la diversité des systèmes.

4.24. Une prudence accrue est impérative lorsqu'il n'est pas possible de faire la démonstration nécessaire de la fiabilité du système, par exemple lorsque la fiabilité d'un système redondant multiple sera limitée par des facteurs tels que les défaillances de cause commune ou les incertitudes de la conception. Des

difficultés spécifiques peuvent, par exemple, survenir lors de la démonstration de la fiabilité des systèmes électroniquement programmés. La diversité est un moyen prudent de compenser la difficulté à démontrer que le niveau nécessaire de fiabilité a été obtenu.

4.25. L'adéquation de la diversité mise en place par rapport aux critères précédents devrait être justifiée. Le champ d'application ainsi que le type de diversité devraient être pris en considération. Le respect de la prudence peut ne pas nécessiter l'élargissement du champ d'application de la diversité pour couvrir des EIP très improbables ou des EIP ayant de faibles conséquences étant donné que le risque de ces événements peut être acceptable malgré la possibilité de défaillance de cause commune.

4.26. Il devrait normalement exister plusieurs types de diversité. La diversité fonctionnelle (systèmes fournissant différentes fonctions physiques qui ont des effets sur la sûreté qui se recouvrent) et la diversité des signaux (utilisation de différents paramètres surveillés pour déclencher une action protectrice) peuvent également être particulièrement efficaces.

4.27. Pour chaque application, il faudrait soigneusement vérifier que la diversité est réellement présente dans la conception mise en œuvre et maintenue tout au long de la durée de vie de la centrale. Le concepteur devrait sérieusement examiner la conception afin d'éviter les modes communs potentiels pour l'application de la diversité, comme les matériaux, les composants, les procédés de fabrication similaires, les logiciels similaires ou les similarités imperceptibles des principes de fonctionnement ou des fonctions support communes.

4.28. La justification de la diversité des équipements, ou de la diversité des logiciels des systèmes CCI connexes comme le système d'exploitation en temps réel, devrait être étendue aux composants des équipements pour vérifier qu'il existe une diversité réelle. Par exemple, différents fabricants peuvent utiliser le même processeur ou le même système d'exploitation, introduisant ainsi potentiellement des modes de défaillance communs. Déclarer que la diversité existe en se basant seulement sur une différence entre le nom des fabricants est insuffisant si la possibilité précédente n'est pas étudiée.

4.29. En ce qui concerne la diversité du logiciel, l'expérience montre que l'indépendance des modes de défaillance peut ne pas être obtenue si plusieurs versions du logiciel sont développées selon des spécifications identiques pour le logiciel. En particulier, il est possible que des versions de programmes

développées indépendamment aient des défaillances de cause commune. La mise en place de types de diversité comme la diversité fonctionnelle ou la diversité des signaux peut être la méthode la plus efficace lorsque l'on se trouve face à cette limitation.

4.30. L'application étendue de concepts comme la redondance, la diversité, l'utilisation d'équipements éprouvés, la testabilité, la surveillance continue et la maintenabilité est utilisée pour obtenir une fiabilité supérieure à celle obtenue en ne respectant que le seul critère de défaillance unique.

4.31. Dans certains États Membres, des exigences de fiabilité ont été imposées au système de protection en plus du critère de défaillance unique. Cette fiabilité supplémentaire est parfois obtenue en utilisant une protection contre les doubles défaillances dans certaines parties du système de protection et/ou en utilisant des équipements possédant une marge d'exploitation plus grande. Dans certains États Membres, un objectif chiffré de fiabilité est établi et des méthodes analytiques ainsi que des tests sont utilisés pour vérifier que le système de protection atteint cet objectif.

Évaluation de la fiabilité

4.32. Pour tous les systèmes importants pour la sûreté, le degré de redondance, de diversité, de testabilité et de robustesse devrait être justifié pour permettre d'atteindre la fiabilité requise des fonctions de sûreté que les systèmes doivent remplir. Cette démonstration peut être basée sur une combinaison équilibrée entre des critères déterministes et une analyse quantitative de la fiabilité.

4.33. Lors de l'évaluation de la fiabilité de systèmes CCI programmés, les effets des défaillances éventuelles du matériel et du logiciel devraient être étudiés ainsi que les caractéristiques de conception visant à prévenir ou limiter leurs effets. Les types de défaillance du matériel à prendre en compte devraient inclure les défaillances des composants de l'ordinateur lui-même et celles des éléments des systèmes de communication. Les défaillances permanentes ainsi que les défaillances transitoires devraient être étudiées.

4.34. La contribution d'une défaillance d'un composant à l'indisponibilité d'un système CCI devrait être déterminée avec un certain niveau de confiance, par exemple à l'aide d'un niveau de confiance donné lorsqu'une approche probabiliste est utilisée.

Fiabilité du logiciel

4.35. Les défaillances logicielles sont des défaillances systématiques causées par des erreurs de conception et n'ont donc pas le comportement de défaillance aléatoire pris comme hypothèse dans l'analyse de la fiabilité du matériel. En conséquence, différentes méthodes peuvent être nécessaires pour évaluer la défiabilité introduite par le matériel et par le logiciel. Par exemple, la fiabilité des systèmes programmés peut être prouvée en se basant sur une évaluation qualitative en tenant compte de la complexité de la conception, de la qualité de la vérification, de la validation et du test du processus de développement sur un large éventail de conditions d'entrée et du retour d'expérience.

INDÉPENDANCE

4.36. L'indépendance empêche: (1) la propagation des défaillances d'un système à l'autre ou (2) la propagation des défaillances entre les parties redondantes des systèmes et (3) les défaillances de cause commune dues aux agressions internes de la centrale. L'indépendance est également importante pour garantir que la redondance et la diversité mises en place pour assurer une grande fiabilité des systèmes importants pour la sûreté sont efficaces.

4.37. L'indépendance devrait également être envisagée pour éviter la propagation des défaillances:

— entre ou parmi des composants d'un système à la suite d'EIP;
— entre et parmi des systèmes de même importance pour la sûreté; et
— de systèmes de moindre importance vers des systèmes plus importants pour la sûreté.

4.38. Les systèmes de sûreté devraient être indépendants des systèmes liés à la sûreté et des systèmes non liés à la sûreté. Des systèmes de moindre importance pour la sûreté peuvent être associés à un système de sûreté à condition que l'indépendance soit conservée entre ces systèmes et que l'indépendance des groupes de sûreté redondants ne soit pas dégradée.

4.39. Les groupes de sûreté redondants au sein des systèmes CCI importants pour la sûreté devraient être indépendants les uns des autres.

4.40. L'indépendance devrait être assurée entre les parties redondantes des systèmes liés à la sûreté.

4.41. Une indépendance appropriée devrait être assurée entre les fonctions diversifiées. L'adéquation de l'indépendance mise en place devrait être justifiée.

4.42. L'indépendance est obtenue grâce à l'isolement électrique, la séparation physique et l'indépendance des communications entre les systèmes.

4.43. L'isolement électrique est nécessaire pour contrôler ou empêcher les interactions nuisibles entre les équipements et les composants dues à des facteurs tels que l'interférence électromagnétique, la surcharge électrostatique, les courts-circuits, les circuits ouverts, la mise à la terre, l'application de la tension maximale envisageable (courant alternatif ou continu) et l'interaction mécanique. Les dispositifs d'isolement optiques et électriques, le blindage des câbles, les structures mécaniques internes ou dispositifs similaires sont des exemples de dispositifs permettant l'isolement électrique. Lorsque des dispositifs d'isolement sont utilisés entre des systèmes dont l'importance pour la sûreté est différente, ils devraient être associés au système de plus grande importance.

4.44. Aucune défaillance envisageable du côté 'non-sûreté' d'un dispositif d'isolement ne devrait empêcher une portion quelconque d'un système de sûreté de satisfaire à ses exigences de performances minimales au cours et à la suite d'un EIP qui nécessite l'exécution d'une fonction de sûreté.

4.45. La séparation physique des systèmes entre eux est obtenue par l'éloignement, par des barrières ou une combinaison des deux et peut être utilisée pour réduire la probabilité de défaillances de cause commune résultant de défaillances consécutives à des EIP (incendie, missile, inondation ou rupture d'une conduite à haute énergie). Cette séparation physique réduit en plus la probabilité d'erreurs involontaires de mise en service lors de l'exploitation ou lors de la maintenance se produisant dans plus d'une partie de ces systèmes.

4.46. Le choix de la séparation physique (éloignement, barrières ou combinaison des deux) peut différer d'un emplacement à l'autre dans la centrale nucléaire. Il dépendra du besoin de se protéger contre tous les EIP envisagés dans le dimensionnement, y compris les effets d'un incendie, d'une explosion chimique, d'une chute d'avion et des missiles. Les réf. [6–9] donnent des recommandations supplémentaires.

4.47. Certaines zones de la centrale ont tendance à devenir des centres naturels de convergence des appareils redondants ou du câblage. Dans ces zones,

l'ampleur de la perte d'indépendance à la suite de certains EIP devrait être soigneusement établie et servir de base à l'élaboration d'une conception globale qui satisfait aux exigences et objectifs de fiabilité. Les centres de ce type sont par exemple les pénétrations du confinement, les centres de commande des moteurs, les salles de tableaux électriques, les salles de faisceaux de câbles, les salles des équipements, la salle de commande et l'ordinateur de contrôle de la centrale.

4.48. L'indépendance des communications n'est nécessaire que pour les conceptions qui incorporent des transmissions de données. L'indépendance des communications s'obtient en sélectionnant des architectures système et des protocoles de communication de données de telle manière qu'un dysfonctionnement de la logique ou du logiciel d'un système n'affecte pas les systèmes connectés. L'indépendance des communications est obtenue grâce à des dispositifs appropriés pour la mise en mémoire tampon des données (y compris toute logique matérielle et/ou logique logicielle utilisée pour prendre en charge la commutation des données, la détection et la correction des erreurs de transmission, le contrôle de flux ou de transmission ou la gestion du protocole) conçus de telle manière que des dysfonctionnements des modules d'envoi et de réception n'affecteront pas le fonctionnement des modules de traitement.

MODES DE DÉFAILLANCE

4.49. Concevoir de telle manière que les défaillances conduisent à des modes de défaillance connus est un moyen de faire face aux défaillances prévisibles des systèmes ou des composants. Les défaillances devraient provoquer non seulement des modes de défaillance prévisibles mais également des modes de défaillance qui placent le système dans un état sûr. Les exigences relatives à la conception exigent que le principe de conception à position de repli sécurisée soit étudié et incorporé s'il y a lieu dans la conception des systèmes et composants de la centrale importants pour la sûreté (réf. [1], par. 5.40).

4.50. Pour faciliter la conception globale des systèmes de sûreté, les équipements devraient dans la mesure du possible présenter un mode de défaillance prévisible et détecté. Les modes de défaillance les plus probables d'un système important pour la sûreté devraient dans la mesure du possible placer le système dans un état sûr. L'incorporation de dispositifs à position de repli sécurisée tels que «chutes de barres de commande par manque de tension» ou «horloges chien de garde» dans la conception des systèmes CCI (réf. [1], par. 5.40) devrait être envisagée. Toutefois, lorsque cette pratique est appliquée, elle ne supprime pas l'obligation

de satisfaire aux exigences de sûreté pour les défaillances qui peuvent se produire dans le dispositif à position de repli sécurisée lui-même.

CONTRÔLE D'ACCÈS AUX ÉQUIPEMENTS

4.51. L'accès aux équipements des systèmes importants pour la sûreté devrait faire l'objet de restrictions appropriées, dans l'optique de la nécessité d'empêcher un accès non autorisé et toute possibilité d'erreur de la part du personnel autorisé. Les méthodes efficaces sont, entre autres, des combinaisons de sécurité physique (enceintes fermées, salles fermées à clé, alarmes sur les portes du tableau de commande) et de mesures administratives selon le niveau de surveillance dans la zone où se trouvent les équipements.

4.52. Deux domaines dont il faut se préoccuper du point de vue du contrôle d'accès sont le réglage des points de consigne et les réglages d'étalonnage à cause de leur importance dans la prévention d'une dégradation des performances des systèmes due aux erreurs potentielles d'exploitation ou de maintenance.

4.53. Dans le cas du contrôle d'accès aux systèmes numériques programmés, des moyens devraient être employés pour restreindre l'accès électronique au logiciel et aux données. Ces restrictions devraient être appliquées à l'accès aux connexions réseau et des équipements de maintenance.

POINTS DE CONSIGNE

4.54. La centrale nucléaire doit être conçue de façon à fonctionner sans risque à l'intérieur de limites définies des paramètres afin que les risques radiologiques pour le public et l'environnement restent dans les limites réglementaires (réf. [1], par. 5.24). L'état de la centrale devrait changer en réponse aux événements initiateurs, mais la centrale peut éventuellement s'approcher d'un état dépassant les limites correspondant à un fonctionnement sûr. Certains systèmes importants pour la sûreté se déclenchent pour effectuer les actions nécessaires au retour de la centrale à un état sûr. Ces systèmes se déclenchent lorsqu'une variable surveillée atteint un point de consigne prédéfini.

4.55. Pour une variable surveillée donnée (pression du circuit primaire, pression du confinement, par exemple) ou une variable calculée donnée (puissance du réacteur, rapport de flux thermique critique, par exemple), une limite de sûreté est établie en se basant sur les critères de sûreté. Cette limite

devrait être la valeur de la variable au-dessus de laquelle des conséquences inacceptables pour la sûreté sont censées se produire (voir fig. 2).

4.56. La limite d'analyse[1] est une valeur théorique découlant de l'analyse de la sûreté. L'analyse de la sûreté devrait démontrer que, à la suite d'un événement initiateurs, la limite de sûreté ne sera pas atteinte si l'action de limitation commence lorsque la limite d'analyse est atteinte. Cette analyse suppose la disponibilité de la configuration des systèmes et équipements envisagée dans la conception et des hypothèses appropriées pour les défaillances. De ce fait, la différence entre la limite de sûreté et la limite analytique prendra en compte les incertitudes de la simulation et les erreurs potentielles concernant le comportement des instruments de contrôle dû au transitoire.

4.57. Le point de consigne nominal est la valeur sur laquelle est réglée la fonction de déclenchement. La marge entre le point de consigne nominal et la limite d'analyse devrait être telle que l'action de limitation soit terminée avant que la limite d'analyse ne soit atteinte.

4.58. La 'limite admissible' est utilisée pour les instruments qui nécessitent un test périodique et une surveillance. La marge entre la limite admissible et le point de consigne nominal comprend les incertitudes aléatoires d'étalonnage de l'appareil, les erreurs aléatoires de l'appareil et les erreurs dues à la dérive de l'appareil. Si un point de consigne se révèle dépasser la limite admissible, une action corrective devrait être mise en œuvre immédiatement.

4.59. Les bases ayant servi à définir les points de consigne et les limites admissibles devraient être documentées et justifiées.

4.60. Dans certains cas la variable surveillée n'est pas identique à la variable utilisée pour spécifier une limite de sûreté. Ce sont par exemple:

— La température maximum de la gaine après une perte accidentelle de réfrigérant qui n'est pas surveillée. La pression du réfrigérant du réacteur est surveillée à sa place car une décroissance de la pression peut indiquer un accident qui mettrait en danger l'intégrité du combustible.
— Le flux neutronique axial, les températures des branches chaudes et froides et la pression du circuit primaire sont surveillés dans un réacteur

[1] La limite d'analyse est une valeur théorique dérivée de l'analyse de la sûreté telle que si, à la suite d'un événement initiateur, une action de limitation démarre à la limite d'analyse, la limite de sûreté ne sera pas atteinte.

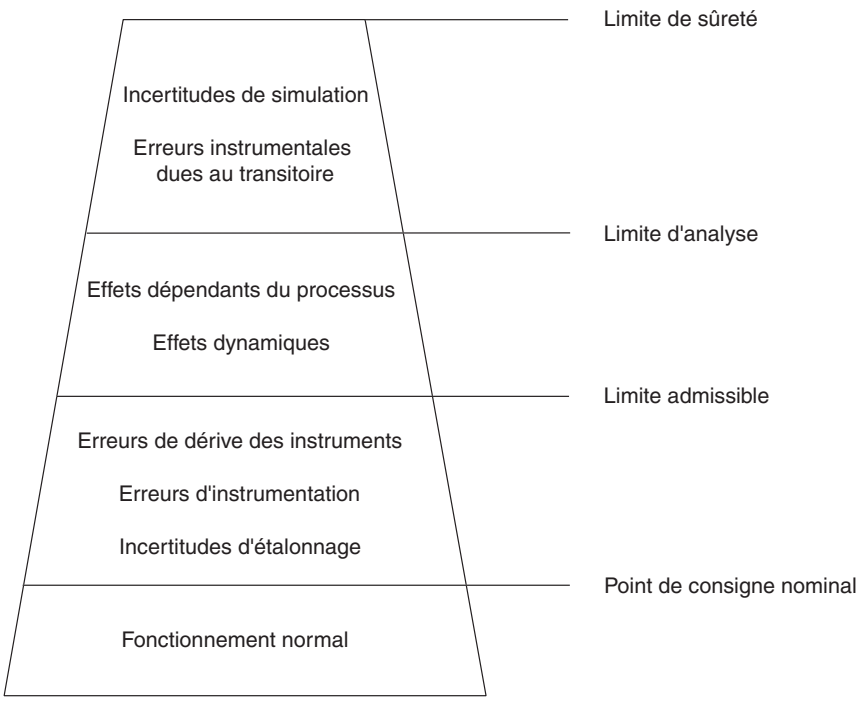

FIG. 2. Exemple de relation entre les points de consigne et les limites.

à eau sous pression car, ensemble, ils peuvent indiquer le début d'une ébullition nucléée qui ne peut pas être mesurée directement.

INTERFACE HOMME–MACHINE

4.61. Il est nécessaire d'avoir, pour les systèmes importants pour la sûreté, des interfaces homme–machine efficaces afin de fournir à l'opérateur des informations en temps voulu, exactes et complètes sur l'état de la centrale et pour permettre une exploitation correcte des systèmes contrôlés par les systèmes CCI. Les exigences relatives à la conception prévoient qu'une prise en compte systématique des facteurs humains et de l'interface homme–machine fasse partie du processus de conception (réf. [1], par. 5.50). L'interface homme–machine des systèmes CCI importants pour la sûreté devrait être conforme aux recommandations données dans la section 6 du présent guide de sûreté.

QUALIFICATION DES ÉQUIPEMENTS

4.62. Il faudrait s'assurer que les systèmes importants pour la sûreté sont capables de remplir leurs fonctions de sûreté lorsque cela est nécessaire en fonctionnement normal, lors d'événements externes et lors d'incidents d'exploitation prévus ainsi que pendant et après des conditions accidentelles de dimensionnement. Ceci est essentiel pour éviter le rejet de matières radioactives et pour prévenir ou atténuer les conséquences radiologiques pour la santé et l'environnement si cela se produit.

4.63. Les conditions radiologiques et les conditions thermodynamiques associées aux ruptures de conduites, y compris les ruptures du système de refroidissement du réacteur, sont des exemples de conditions environnementales dangereuses dues à des conditions accidentelles de dimensionnement qui pourraient entraîner la défaillance des équipements. Des conditions de fonctionnement potentiellement dangereuses sont, par exemple, un écoulement biphasique à grande vitesse, de hauts niveaux de vibration ou des fluides chargés de débris. Outre les événements en fonctionnement potentiellement dangereux, des effets comme la surchauffe, l'interférence électromagnétique, les décharges électrostatiques et les variations d'alimentation électrique, qui peuvent également entraîner potentiellement des défaillances de cause commune, devraient être pris en considération.

4.64. Les exigences relatives à la conception prévoient une procédure de qualification pour confirmer que les équipements sont capables de satisfaire, tout au long de leur durée de vie prévue à la conception, aux exigences concernant l'accomplissement des fonctions de sûreté lorsqu'ils sont soumis aux conditions environnementales (vibration, température, pression, impacts de jets de fluides, interférence électromagnétique, rayonnement, humidité ou toute combinaison probable des conditions précédentes) qui peuvent se présenter au moment où ils sont nécessaires (réf. [1], par. 5.45). La qualification consiste à identifier les risques dans l'environnement de travail des équipements et à exécuter un programme de tests et/ou analyses pour déterminer si les équipements peuvent remplir convenablement leurs fonctions de sûreté dans des conditions de service données et consigner les résultats dans un rapport. La qualification est une méthode qui permet de minimiser la possibilité pour des effets ou des événements environnementaux d'entraîner une défaillance de cause commune des équipements.

4.65. La qualification des équipements devrait prouver que les équipements sont capables de fonctionner dans des conditions d'exploitation et

environnementales. Les recommandations suivantes, bien que spécifiques à la conception des systèmes importants pour la sûreté, devraient être appliquées en même temps que d'autres recommandations concernant la qualification, réf. [10] par exemple.

Programme de qualification des équipements

4.66. Un programme de qualification devrait être réalisé pour confirmer que les équipements importants pour la sûreté seront capables, jusqu'à la fin de leur durée de vie prévue à la conception, de satisfaire aux exigences de performances du dimensionnement (comme la plage de mesure, l'exactitude et la réponse) pour la mission de sûreté assignée, dans les conditions environnementales (température, pression, rayonnement, humidité ou brouillard corrosif) susceptibles d'exister au moment où les appareils seront nécessaires.

4.67. Ces conditions environnementales devraient inclure les combinaisons prévues en fonctionnement normal, lors d'incidents d'exploitation prévus et pendant et après des accidents de dimensionnement. La prise en compte des conditions d'accident grave n'est pas obligatoire dans le programme de qualification des équipements. Toutefois, il faudrait prouver, avec un niveau de confiance raisonnable et dans la mesure du possible, que les équipements chargés d'intervenir en cas d'accidents graves fonctionnent dans les conditions d'accident grave prévues (réf. [1], par. 5.46).

4.68. Lorsque les équipements sont soumis à des événements externes comme des phénomènes naturels ou autres influences extérieures et doivent accomplir une mission de sûreté pendant ou à la suite d'un événement de ce type, le programme de qualification devrait inclure les conditions imposées aux équipements par ces événements externes. En outre, toutes les conditions environnementales inhabituelles pouvant raisonnablement être anticipées et qui pourraient résulter de conditions d'exploitation spécifiques, comme lors des tests périodiques d'étanchéité du confinement, devraient être incluses dans le programme de qualification.

4.69. Le programme devrait inclure un plan permettant de garantir que les équipements sont qualifiés pour la période d'utilisation prévue et de prévoir des requalifications en temps voulu ou le remplacement, si nécessaire. Il faudrait prendre en compte les effets combinés des différents facteurs environnementaux et l'effet cumulé des facteurs environnementaux ambiants normaux pendant la durée de vie des équipements après installation. Il faudrait faire preuve de prudence, le cas échéant, en tenant compte des mécanismes de vieillissement

imprévus. Des dispositions appropriées devraient être prises pour la surveillance, le test et l'inspection des équipements de la centrale afin d'identifier un comportement imprévu ou une dégradation (réf. [1], par. 5.47).

4.70. Lors de la qualification des équipements du système de sûreté, il faudrait de préférence qualifier un équipement complet plutôt que les parties directement liées à la tâche de sûreté considérée.

Méthodes de qualification

4.71. Une combinaison appropriée des méthodes de qualification suivantes devrait être utilisée pour atteindre les objectifs susmentionnés:

— exécution de tests sur le type d'équipement à fournir;
— exécution de tests sur l'équipement réellement fourni;
— prise en compte de l'expérience antérieure pertinente dans des applications similaires; et/ou
— analyse sur la base d'une extrapolation technique raisonnable des données de test ou de l'expérience d'exploitation collectées dans des conditions pertinentes.

4.72. La méthode de qualification choisie devrait instaurer un niveau de confiance en rapport avec l'importance de l'équipement pour la sûreté du système, comme décrit dans la section 2. Des tests devraient être effectués pour la qualification des équipements et, chaque fois que cela est réalisable, pour les équipements de sûreté.

4.73. Lorsque des barrières de protection sont mises en place pour isoler les appareils des effets environnementaux éventuels, les barrières elles-mêmes devraient être soumises à un programme de qualification pour valider leur adéquation.

QUALITÉ

4.74. Une conception et une fabrication de grande qualité sont nécessaires pour garantir que l'on peut prouver que les systèmes importants pour la sûreté satisfont aux exigences de sûreté. Une conception et une fabrication conformes aux niveaux de qualité appropriés sont des éléments importants pour respecter l'exigence stipulée dans la réf. [1], par. 5.1.

4.75. La qualité des composants et des modules des systèmes importants pour la sûreté devrait être cohérente avec le but visé qui est de minimiser les besoins en maintenance et les taux de défaillance.

4.76. Les équipements sélectionnés pour les systèmes importants pour la sûreté devraient être de conception éprouvée chaque fois que possible, devraient être adaptés aux objectifs de fiabilité et devraient faciliter le respect des exigences relatives à l'étalonnage, aux tests, à la maintenance et aux réparations. Lors de la sélection des appareils, il faudrait prendre en compte les fonctionnements intempestifs et les modes de défaillance non sûrs, par exemple l'impossibilité d'obtenir le déclenchement lorsque cela est nécessaire.

CONCEPTION ET COMPATIBILITÉ ÉLECTROMAGNÉTIQUE

4.77. Les équipements et systèmes CCI, y compris les câbles associés, devraient être conçus et installés de façon à résister à l'environnement électromagnétique des centrales nucléaires.

4.78. Des dispositions appropriées pour la mise à la terre, le blindage et le découplage des interférences devraient être prises lors de la conception. Les pratiques relatives à l'installation et à la maintenance devraient être adaptées afin de garantir que ces dispositions sont convenablement mises en œuvre lors de l'installation et de la maintenance. La référence [11] donne des recommandations supplémentaires sur la mise à la terre. La référence [4] donne des exemples de pratiques types pour la mise à la terre et le blindage.

TEST ET TESTABILITÉ

4.79. Les tests en fonctionnement garantissent que les systèmes importants pour la sûreté restent opérationnels et capables d'accomplir leurs missions de sûreté. La fréquence des tests devrait être établie en fonction des exigences concernant la disponibilité et la fiabilité du système. La testabilité — la capacité d'un système à être testé — devrait être intégrée dans le cadre de la conception. Lors de la conception d'un système testable, il faudrait étudier si: (1) l'emplacement des appareils convient, (2) l'accès est convenablement contrôlé, (3) les défauts des équipements sont facilement décelables et (4) la démonstration du maintien de la fonctionnalité est faite de telle manière que la sûreté de la centrale en exploitation n'est pas compromise.

4.80. La testabilité est un élément nécessaire de la conception que ce soit pour la fiabilité du système décrite dans les par. 5.32–5.42 des exigences relatives à la conception ou pour le test, l'inspection et la surveillance en exploitation exigés dans les par. 5.43–5.44 de ces mêmes exigences. En outre, le système de protection devrait satisfaire aux exigences spéciales de fiabilité et de testabilité décrites dans les par. 6.81–6.84 des exigences relatives à la conception.

Programme de test

4.81. La conception des systèmes CCI importants pour la sûreté devrait inclure l'identification d'un programme de test et d'étalonnage adapté aux exigences concernant leur disponibilité.

4.82. Ce programme de test devrait garantir que les capacités fonctionnelles des systèmes et composants importants pour la sûreté sont conservées. Ce programme devrait inclure la confirmation périodique du respect des exigences du dimensionnement telles que l'exactitude, le temps de réponse et les points de consigne.

4.83. Dans la mesure du possible, le test des systèmes CCI importants pour la sûreté devrait être une vérification générale (des capteurs aux actionneurs), pouvant être effectuée in situ avec un minimum d'effort. Le programme de test peut être éventuellement constitué de tests qui se recoupent et forment ensemble un test du circuit complet. Toutes les fonctions de sortie importantes pour la sûreté, comme les alarmes, les actions de commande et la mise en marche des actionneurs, devraient être testées.

Dispositions de test

4.84. Tous les systèmes importants pour la sûreté devraient inclure des dispositions permettant l'exécution des tests nécessaires, y compris des équipements de test intégrés le cas échéant. Ils devraient eux-mêmes pouvoir être vérifiés à intervalles réguliers pour s'assurer qu'ils fonctionnent toujours correctement. Lorsque les équipements à tester ne peuvent pas être placés dans des zones non dangereuses, des aménagements devraient être faits pour permettre d'effectuer les tests à distance en dehors de la zone dangereuse.

4.85. Lorsque des moyens de test sont mis à disposition, la conception devrait garantir que le système ne peut pas involontairement être laissé dans une configuration de test. Lorsque des moyens fixes sont mis à disposition pour le

test périodique, les interfaces devraient faire l'objet d'un verrouillage matériel afin de garantir que l'interaction avec le système de test est impossible sans intervention manuelle délibérée.

4.86. Pour les systèmes de sûreté, la méthode de test devrait dans l'absolu comporter un seul test en ligne pour chaque fonction, englobant tous les composants depuis les capteurs jusqu'aux actionneurs. Cependant, ce type de test n'est pas toujours réalisable. Dans ces cas-là, le programme de test devrait combiner des tests en ligne (états d'exploitation où la fonction de sûreté est ou peut être nécessaire) et hors ligne (états d'exploitation où la fonction de sûreté n'est pas nécessaire) dans une séquence de phases de test qui se recouvrent, autant que nécessaire, pour atteindre les objectifs du test. L'adéquation de l'utilisation de phases de test qui se recouvrent devrait être prouvée.

4.87. La conception des systèmes de sûreté et de leurs dispositifs de test devrait garantir la sûreté de la centrale pendant le test lui-même et devrait de préférence minimiser le déclenchement intempestif de toute action de sûreté et tout autre effet préjudiciable des tests sur la disponibilité de la centrale. La conduite du programme de test ne devrait pas causer de détérioration de composants de la centrale supérieure à celle qui est prévue dans la conception.

Détection des défaillances

4.88. Les dispositions prévues pour le test périodique devraient fournir des informations objectives sur l'état du système et devraient, suivant le cas, fournir des données sur les évolutions afin de faciliter la détection d'une dégradation du système et de conditions qui laissent présager la naissance d'une défaillance dans le système. Dans la mesure du possible, la conception des systèmes importants pour la sûreté devrait incorporer des dispositifs d'autocontrôle. Toutefois, la fourniture de dispositifs d'autocontrôle devrait être mise en balance avec le besoin de simplicité.

4.89. Dans la mesure du possible, chaque capteur affecté à une variable mesurée devrait être testé individuellement, par exemple par:

— la perturbation de la variable surveillée;
— l'introduction et la variation, selon le cas, d'une entrée de substitution dans le capteur de même nature que la variable mesurée; ou
— la comparaison entre des variables qui sont liées l'une à l'autre par une relation connue et pour lesquelles des mesures sont possibles.

4.90. Les tests demandés devraient déceler les défauts des systèmes de sûreté des capteurs aux actionneurs. Les tests devraient être capables de détecter les défauts de chaque partie redondante de ces systèmes. Lorsque des équipements redondants sont mis en place dans une voie, les tests devraient vérifier l'opérabilité de chaque partie redondante.

Démonstration des performances du système

4.91. Les tests périodiques sélectionnés et les dispositions prises pour l'étalonnage devraient être tels que les caractéristiques de performance spécifiées dans le dimensionnement pour les voies redondantes du système de protection, des systèmes actionneurs de sûreté et des fonctions support du système de sûreté puissent être confirmées. Le test et l'étalonnage devraient normalement être effectués à différents intervalles périodiques.

4.92. Lorsque des combinaisons de variables sont utilisées pour générer un signal particulier pour le système de protection, toutes les variables devraient être testées et étalonnées.

Mise hors service

4.93. Lorsque la réalisation des tests périodiques est en conflit avec la fiabilité du groupe de sûreté (par exemple, lorsqu'un circuit a été mis hors service pour être testé et doit néanmoins être remis en service pour la sûreté), la méthode de test devrait garantir que les deux objectifs ont été atteints de manière satisfaisante. Par exemple, lorsqu'un capteur a été mis hors service pour un test périodique, une comparaison visuelle avec les capteurs redondants (ou autre moyen équivalent) devrait être utilisée pour vérifier sa remise en service ultérieure. En outre, l'état des éléments qui ont été dérangés pour répondre aux besoins du test périodique (par exemple la position de la vanne d'un instrument, les dérivations pour la maintenance) devrait être vérifié pour s'assurer qu'il est revenu à l'état de fonctionnement d'origine. À cet égard, il faudrait prêter attention aux erreurs humaines éventuelles.

4.94. Dans la conception des systèmes de sûreté il faudrait veiller à ce que, lorsque des tests périodiques sont effectués, les parties restant en service soient capables d'accomplir la mission de sûreté nécessaire. Dans le cas d'un système de sûreté, la mise hors service d'un seul composant ou d'une voie ne devrait entraîner aucune perte de la redondance requise sauf s'il est possible de prouver que le système peut fonctionner de manière suffisamment fiable (voir réf. [1], par. 6.81). La méthode de test choisie devrait, dans la mesure du

possible, minimiser le temps d'immobilisation des appareils. La méthode préférée de mise hors service est de placer la sortie de la voie enlevée dans un état sûr défini.

4.95. Les procédures de test pour le test périodique des systèmes CCI de sûreté ne devraient ni exiger ni permettre des configurations de test improvisées, l'utilisation de connexions temporaires, l'enlèvement de fusibles ou l'ouverture de coupe-circuits. Le branchement temporaire des appareils de test peut être utilisé lorsque les appareils du système de sûreté à tester sont équipés de dispositifs spécialement conçus pour le branchement de ces appareils de test. Ces dispositifs devraient être considérés comme faisant partie du système de sûreté et devraient se conformer à toutes les recommandations du présent guide de sûreté, que les appareils de test portables soient déconnectés ou restent connectés à ces dispositifs.

Contrôle et conduite des tests

4.96. Les mesures prises pour le test ne devraient ni nuire à l'indépendance des systèmes de sûreté ni provoquer de défaillances de cause commune.

MAINTENABILITÉ

4.97. Un certain nombre de facteurs inhérents aux systèmes CCI des centrales nucléaires obligent à concevoir ces systèmes de façon à permettre une maintenance fiable et efficace. Ces facteurs incluent:

— la longue durée de vie d'une centrale nucléaire comparée aux durées de vie habituelles des divers composants matériels des systèmes CCI;
— la dérive, la dégradation ou la détérioration inévitable des équipements; et
— l'usure du matériel CCI (c'est-à-dire les taux de défaillances des composants qui rendent inévitable le remplacement des composants au moins une fois au cours de la durée de vie de la centrale).

4.98. Dans le cas des systèmes importants pour la sûreté, il faudrait veiller tout particulièrement à faciliter les activités de maintenance qui permettent de maintenir la qualification du système pour les environnements dans lesquels ce système doit fonctionner. La minimisation du temps nécessaire pour effectuer les réparations contribue à la fiabilité globale et la disponibilité. La maintenabilité est un élément important pour la mise en œuvre des principes de défense en profondeur exposés dans les par. 2.9–2.11 de la réf. [1].

4.99. Les systèmes CCI devraient être conçus et implantés de manière à faciliter la surveillance et la maintenance, à permettre un accès en temps voulu et, dans le cas de défaillance ou d'erreur, de permettre un diagnostic et une réparation rapides.

4.100. Les systèmes CCI importants pour la sûreté devraient être conçus en tenant compte des capacités et des limites humaines dans l'accomplissement des tâches de maintenance requises. Lorsque cela est possible, les systèmes CCI devraient être implantés de manière à minimiser les risques pour le personnel de maintenance et à faciliter la maintenance des appareils. Il faudrait prévoir un espace suffisant autour des appareils pour garantir que le personnel de maintenance peut accomplir ses tâches dans des conditions de travail normales. Lorsque cela est possible, les appareils ne devraient pas être placés dans des endroits où il existe un risque d'intensité de rayonnement élevée (voir réf. [12]) ou des endroits où des conditions de température ou d'humidité extrêmes sont habituelles.

4.101. Les systèmes possédant des équipements situés dans des zones inaccessibles devraient être soigneusement étudiés afin de déterminer si d'autres stratégies pour faire face aux défaillances pourraient convenir. Ces stratégies peuvent être, par exemple, d'installer des équipements redondants de secours, de mettre en place des dispositifs permettant l'intervention à distance et d'envisager un fonctionnement de la centrale à puissance réduite si les équipements tombent en panne et ne peuvent pas être rapidement réparés ou remplacés. Lorsque le réacteur est en fonctionnement, l'emplacement de certains composants peut empêcher leur étalonnage régulier. Dans ce cas, l'accent devrait être mis sur la stabilité et l'exactitude à long terme des équipements sélectionnés et il faudrait prévoir le moyen de permettre la comparaison avec d'autres équipements, par exemple, en comparant la puissance neutronique et la puissance thermique.

4.102. Dans les systèmes auxquels s'applique le critère de défaillance unique, si un circuit est bipassé au cours de l'exploitation de la centrale à des fins de maintenance, de test, de réparation ou d'étalonnage, les circuits opérationnels restants du système devraient continuer à satisfaire au critère de défaillance unique sauf justification contraire comme indiqué dans les par. 4.15–4.21 du présent guide de sûreté.

4.103. Les moyens fournis pour la maintenance des systèmes CCI importants pour la sûreté devraient être conçus de telle manière que tout effet sur la sûreté de la centrale soit acceptable. Ces moyens sont par exemple la déconnexion

d'un circuit dans un système possédant des circuits redondants et la possibilité de procéder à des actions manuelles de remplacement.

DOCUMENTATION

4.104. La confiance accordée à la conception des systèmes importants pour la sûreté est basée dans une large mesure sur le bien-fondé des procédés utilisés. La documentation joue un rôle important pour l'établissement de la confiance dans la conception et dans la transmission de cette confiance aux autres. La documentation concernant la conception et la mise en œuvre des systèmes importants pour la sûreté devrait être claire et précise.

4.105. Un ensemble de documents devrait être élaboré et conservé afin d'assurer la traçabilité des fondements de la conception. Les documents appropriés devraient être rédigés à chaque étape du processus de développement et, lors de la livraison d'un système, l'ensemble des documents le concernant devrait être joint. Les détails sur l'étendue, le type et le contenu de la documentation sont abordés dans la section 7. Tous les documents associés aux systèmes importants pour la sûreté devraient posséder les caractéristiques suivantes:

— ils devraient être compréhensibles sans ambiguïté pour les personnes possédant une expérience et des niveaux de connaissance différents qui pourraient participer à la conception, à la construction, à la mise en service, à l'exploitation, à la maintenance et à la délivrance des autorisations réglementaires;
— le langage utilisé devrait être clair et basé sur une terminologie bien définie; et
— la notation, la terminologie, les textes et les diagrammes devraient être utilisés de manière cohérente d'un bout à l'autre de la documentation.

4.106. La documentation devrait être écrite dans l'optique de sa facilité d'utilisation, c'est-à-dire en tenant compte des besoins de ses utilisateurs:

— les exigences, spécifications et descriptions de la conception ne devraient permettre qu'une seule interprétation de chaque exigence, spécification ou description prise individuellement;
— la traçabilité de documents de niveau supérieur vers les documents de conception devrait être possible afin de pouvoir vérifier l'exhaustivité;

— la traçabilité de documents de conception vers les documents de niveau supérieur devrait être possible afin de pouvoir vérifier les éléments inutiles;
— les documents ne devraient pas contenir de déclarations contradictoires ou incohérentes;
— chaque élément d'information devrait avoir une place unique et identifiable dans le document et ne devrait pas être répété ou fractionné;
— chaque exigence ou élément de conception devrait posséder un identificateur unique (ce qui aide également à la traçabilité);
— les exigences et informations relatives à la conception devraient être exprimées de telle manière qu'il soit possible de vérifier que les systèmes importants pour la sûreté satisfont aux exigences et sont réalisés conformément à la conception;
— la structure et le style des documents devraient être tels que toute modification nécessaire puisse être faite facilement, complètement et de manière cohérente; et
— les documents devraient être compréhensibles pour les utilisateurs auxquels ils sont destinés.

IDENTIFICATION DES ÉLÉMENTS IMPORTANTS POUR LA SÛRETÉ

4.107. Les éléments importants pour la sûreté devraient être identifiés afin de s'assurer que les exigences relatives aux systèmes importants pour la sûreté sont appliquées dans la conception, construction, maintenance et exploitation de la centrale. L'identification devrait être faite afin de satisfaire aux exigences du classement de sûreté énoncées dans les par. 5.1–5.3 de la réf. [1].

4.108. Les systèmes de sûreté et leurs composants devraient être identifiés de manière unique, par exemple par un étiquetage ou un codage couleur. En outre, au sein d'un système de sûreté, les voies redondantes devraient être convenablement identifiées afin de réduire la probabilité d'effectuer involontairement la maintenance, les tests, la réparation ou l'étalonnage sur une mauvaise voie. Cette identification ne devrait pas dépendre de la référence aux plans, manuels ou autre document de référence. Il faudrait pouvoir faire la distinction entre cette identification et les autres marques d'identification utilisées à d'autres fins. Cette pratique devrait être adoptée également pour les systèmes liés à la sûreté. Les composants ou modules montés dans des équipements ou des assemblages clairement identifiés n'ont pas besoin eux-mêmes d'une identification. La gestion de la configuration est habituellement suffisante pour gérer l'identification de ces composants, modules et logiciels informatiques intégrés.

5. RECOMMANDATIONS DE CONCEPTION SPÉCIFIQUES AUX SYSTÈMES

5.1. Les recommandations spécifiques données dans cette section s'appliquent *en plus* des recommandations générales données dans la section 4.

SYSTÈMES DE SÛRETÉ

5.2. Le système de protection est la partie d'un système de sûreté qui détecte une déviation par rapport aux conditions acceptables de la centrale et déclenche des actions pour éviter une situation dangereuse ou potentiellement dangereuse. Différentes configurations de système sont utilisées à cet effet et le terme 'système de protection' n'est pas universel dans tous les États Membres. Les recommandations données dans la section traitant des systèmes de protection s'appliquent à tout système qui remplit ces fonctions.

SYSTÈMES DE PROTECTION

5.3. Le système de protection sert à maintenir la sûreté dans des situations où les systèmes de contrôle-commande n'arrivent pas à maintenir les variables de la centrale à l'intérieur de limites définies. Ces situations peuvent se produire à cause d'une panne au sein du système de contrôle-commande ou parce qu'un événement s'est produit et entraîne, pour les variables de fonctionnement, une modification trop rapide pour que les systèmes de contrôle-commande réagissent de manière adéquate ou à cause d'une défaillance d'un élément important pour la sûreté. Dans ces cas-là, une action rapide est nécessaire pour éviter que la situation ne s'aggrave et induise un accident potentiel.

5.4. Généralement, l'action rendue nécessaire par une situation particulière, à savoir la mission de sûreté correspondant à cette situation, implique la mise en route de nombreux systèmes de la centrale de manière coordonnée. Le système de protection est mis en place pour accomplir toutes les actions de sûreté spécifiées, en même temps que les systèmes de commande de sûreté et les fonctions support du système de sûreté.

5.5. Le système de protection surveille les variables appropriées de la centrale. Celles-ci peuvent être des variables de fonctionnement comme les débits de

fluence[2] (flux) ou les températures et pressions du réfrigérant ou des variables spécifiques aux incidents d'exploitation prévus ou aux conditions accidentelles de dimensionnement, comme les vitesses d'évolution des variables de fonctionnement, les niveaux d'humidité, les changements de position des équipements ou les niveaux de rayonnement. Les variables mesurées de la centrale, soit individuellement soit sous forme de combinaisons sélectionnées, devraient permettre la détection de toutes les situations où une mission de sûreté doit être accomplie.

But du système de protection

5.6. Les exigences relatives à la conception prévoient que (réf. [1], par. 6.80) le système de protection soit conçu de façon à:

— déclencher automatiquement la mise en route des systèmes appropriés, comportant, suivant les besoins, les systèmes d'arrêt du réacteur, pour garantir que les limites de conception spécifiées ne sont pas dépassées à la suite d'incidents d'exploitation prévus;
— détecter les accidents de dimensionnement et déclencher la mise en route des systèmes nécessaires pour limiter les conséquences de ces accidents à l'intérieur du dimensionnement;
— pouvoir éliminer des actions dangereuses du système de commande.

5.7. Le système de protection est généralement nécessaire pour:

— détecter qu'une variable de la centrale a atteint le point de consigne;
— identifier une situation nécessitant une protection;
— déclencher, dans le bon ordre, toutes les actions de sûreté exigées par la mission de sûreté correspondante dans le système de protection lui-même, les systèmes de commande de sûreté et les fonctions support des systèmes de sûreté; et
— dans certains États Membres, surveiller les variables de la centrale et afficher leurs valeurs pour que l'opérateur les utilise pour mettre en œuvre une action protectrice manuellement.

5.8. Les fonctions de sûreté courantes suivantes, identifiées dans le dimensionnement, sont initiées par le système de protection:

---

[2] Le débit de fluence ($\perp$) est l'augmentation de particules $d\Phi$ dans un intervalle de temps suffisamment petit divisé par cet intervalle de temps: $\perp = d\Phi/dt$.

— arrêt sûr du réacteur;
— maintien de l'enveloppe sous pression du réfrigérant du réacteur dans les limites nominales pour tous les états d'exploitation;
— évacuation de la chaleur résiduelle lors d'incidents d'exploitation prévus et dans des conditions accidentelles;
— refroidissement d'urgence du cœur pendant et à la suite de conditions accidentelles de dimensionnement;
— isolement du confinement du réacteur pendant et à la suite de conditions accidentelles de dimensionnement;
— réduction de la pression et de la température du confinement du réacteur après un accident;
— purification de l'atmosphère du confinement;
— isolement des stockages d'effluents radioactifs; et
— contrôle des matières radioactives en suspension dans l'air, y compris le contrôle de leur entrée dans des zones d'exploitation et de leur rejet dans l'environnement.

5.9. Les actions protectrices sont déclenchées lorsque la valeur d'une variable de la centrale atteint une valeur prédéterminée, à savoir, le point de consigne nominal.

Étendue du système de protection

5.10. Le système de protection englobe tous les équipements électriques et mécaniques et tous les circuits participant à l'émission de signaux d'actions protectrices à partir de mesures des variables de fonctionnement. La figure 3 présente les interfaces avec:

— le procédé de la centrale protégé grâce aux capteurs du système de protection;
— les systèmes de commande de sûreté, via les actionneurs des systèmes de commande de sûreté;
— tout affichage d'informations pour l'opérateur non inclus dans le système de protection mais qui extrait les signaux du système de protection à travers des dispositifs d'isolement situés dans le système de protection; et
— les systèmes de contrôle-commande, à travers des dispositifs d'isolement du système de protection.

5.11. Pour des raisons de clarté, la fig. 3 n'essaie pas de présenter tous les points d'interface possibles entre le système de protection et les autres systèmes

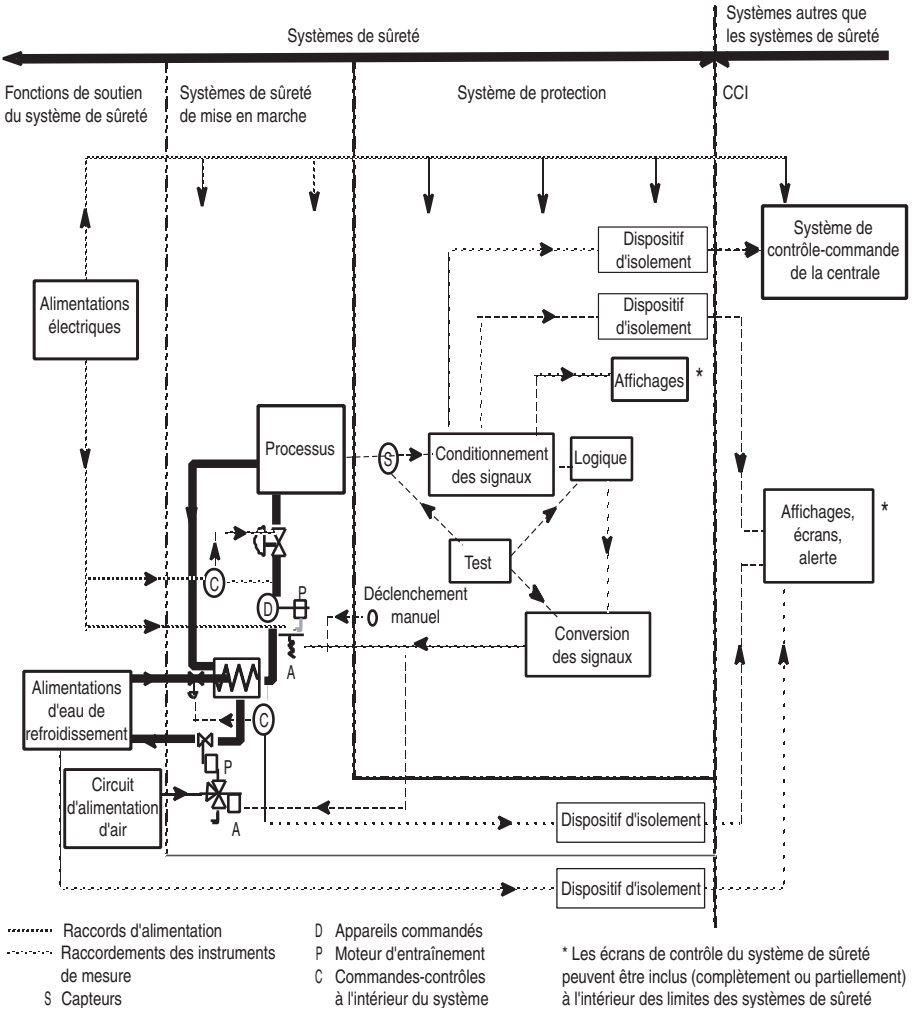

FIG. 3. Schéma type d'un système de protection et de ses interconnexions avec les autres systèmes.

comme les systèmes de surveillance et d'information, les dispositifs support des systèmes de sûreté et les commandes des panneaux de commande locaux.

5.12. Le système de protection comporte les éléments suivants:

— des capteurs, qui peuvent être:
  • des lignes d'instrumentation de contrôle du procédé, comprenant jusqu'au détecteur (par exemple, capteurs de pression, de débit ou de position); et

- des capteurs primaires utilisés pour la mesure des variables de la centrale (par exemple, thermocouples et chambres d'ionisation);

— des équipements de mise en forme des signaux pour les capteurs primaires, comprenant des comparateurs à seuil et des convertisseurs analogiques-numériques;
— la logique de décision utilisée pour chaque variable mesurée;
— les équipements de conversion du signal fournissant les données de sorties, sous forme d'actions protectrices, aux actionneurs;
— les affichages nécessaires pour le déclenchement manuel des actions protectrices;
— les dispositifs d'isolement faisant l'interface avec les systèmes d'information de l'opérateur et les systèmes de classement de sûreté différent;
— les panneaux, châsses et cabinets contenant des équipements du système de protection;
— les câbles de connexion et les chemins de câbles;
— les pénétrations de l'enceinte pour les câbles électriques et les câbles d'instrumentation; et
— tous les autres équipements intervenant entre la connexion du procédé et les bornes d'entrée de l'actionneur.

5.13. Les recommandations de cette section peuvent également s'appliquer aux autres équipements des systèmes de sûreté qui doivent fonctionner pour garantir que les fonctions du système de protection sont remplies. Parmi ces autres équipements des systèmes de sûreté on peut citer:

— les actionneurs recevant les signaux de sortie du système de protection;
— les dispositifs moteurs mis en route par les actionneurs; et
— les équipements entraînés actionnés par les dispositifs moteurs.

Dispositifs de détection

5.14. Le système de protection devrait être utilisé pour surveiller les variables de la centrale et détecter les écarts par rapport aux limites spécifiées afin que les fonctions de sûreté spécifiées puissent être remplies. La mesure des variables de la centrale devrait être cohérente avec les exigences de performance spécifiées dans le dimensionnement. Autant que possible, les conditions de la centrale devraient être surveillées à l'aide d'une mesure directe plutôt qu'être déduites à partir d'autres mesures, moins directes.

5.15. Lors de la sélection de la plage de mesure de chaque variable surveillée, l'exactitude, le temps de réponse et le risque de dépassement nécessaires pour la

fonction concernée ainsi que la capacité de surveillance nécessaire après accident devraient être pris en compte. Si plusieurs capteurs sont nécessaires pour couvrir convenablement l'intégralité de la plage de valeurs de la variable surveillée, un chevauchement raisonnable d'un capteur à l'autre devrait être prévu pour chaque point de transition afin de garantir que les effets de saturation ou de distorsion n'empêchent pas l'exécution de la fonction de protection.

5.16. Les points de consigne peuvent être fixes ou dépendre de certains autres paramètres ou conditions de la centrale. Lorsqu'on utilise des points de consigne variables, les dispositifs employés pour effectuer le réglage du point de consigne sont classés en tant que partie du système de protection et devraient satisfaire à ses exigences. La conception du système devrait fournir à l'opérateur le moyen de déterminer la valeur des points de consigne de chaque voie du système de protection.

'Mémorisation' du système de protection

5.17. L'action déclenchée par le système de protection devrait être mémorisée[3]. La mémorisation ne devrait pas être annulée sauf par une action manuelle de l'opérateur après exécution complète de l'action de sûreté ou par une action du système de protection visant à empêcher que les limites établies dans le dimensionnement soient dépassées. Une fois l'action mémorisée, la séquence prévue devrait se poursuivre jusqu'à ce que la mission de sûreté ait été accomplie. Après mémorisation de l'action, le système de protection devrait surveiller automatiquement les conditions de la centrale, permettre la mise en œuvre des actions de sûreté imposées par les conditions de la centrale et fournir les informations utiles à toute action autorisée de l'opérateur. L'accomplissement de la fonction de sûreté ne devrait pas empêcher le système de protection de déclencher les autres actions protectrices que pourraient nécessiter les conditions ultérieures de la centrale.

5.18. Les composants ajoutés pour les fonctions de mémorisation ne devraient pas entraîner une diminution inacceptable de la fiabilité de l'action de sûreté.

---

[3] La mémorisation est la propriété d'un composant qui fait que son signal de sortie prend un nouvel état et le conserve après que le signal ou les signaux d'entrée responsables de l'initiation du nouvel état sont revenus à leurs valeurs précédentes.

Action de sûreté manuelle

5.19. Les actions de l'opérateur sont nécessaires pour:

— suppléer aux actions de sûreté;
— déclencher ou arrêter directement certaines actions de sûreté; et
— réinitialiser le système de protection après son fonctionnement.

5.20. La conception des moyens de commande manuelle devrait être suffisamment flexible pour permettre le déclenchement des actions de sûreté dans des situations anormales et le fonctionnement à long terme à la suite d'un accident.

5.21. Les exigences pour la plupart des actions protectrices sont telles que le déclenchement automatique des actions sera nécessaire. En outre, la possibilité de déclenchement manuel de l'arrêt du réacteur et de déclenchement d'actions au niveau des systèmes comme l'isolement du confinement devrait exister. Ceci n'exclut pas une intervention de l'opérateur à un niveau plus complet. Lorsqu'un déclenchement manuel est prévu, il devrait, dans la mesure du possible, être indépendant des équipements du système de protection automatique.

5.22. Dans le cas d'un déclenchement manuel involontaire d'une action de sûreté, le système de protection devrait protéger la centrale à l'aide d'une action automatique. Le déclenchement ou l'arrêt manuel des actions de sûreté peut être utilisé seul à condition que l'on puisse prouver que les limites acceptables ne seront pas dépassées. Ces actions manuelles sont par exemple:

— l'initiation de certaines actions de sûreté après exécution complète de séquences automatiques;
— le passage de la centrale arrêtée dans son état le plus favorable à long terme après un accident; et
— la réalisation de certaines actions de sûreté qui ne sont exigées que bien après l'EIP.

5.23. Pour justifier qu'une action manuelle seule est acceptable, il faudrait prouver que:

— l'opérateur possède suffisamment d'informations classées de sûreté et que celles-ci sont clairement présentées afin de pouvoir porter un jugement rationnel et initier les actions de sûreté nécessaires;
— l'opérateur possède des procédures écrites et a reçu une formation adaptée;

— l'opérateur a suffisamment de moyens à sa disposition pour accomplir les actions nécessaires;
— l'opérateur a suffisamment de temps pour évaluer l'état de la centrale et accomplir les actions nécessaires; et
— les liaisons de communication entre les opérateurs leur permettent d'accomplir correctement leurs actions.

5.24. Le temps imparti pour l'action prévue de l'opérateur à partir de l'apparition d'un incident de fonctionnement prévu ou de conditions accidentelles de dimensionnement varie selon les États Membres et va de 10 à 30 minutes. Ce temps dépend de facteurs comme la complexité de la décision, les affichages présents, le besoin de faire la distinction entre différents EIP et les conséquences d'une mauvaise décision.

5.25. Les actions de sûreté manuelles devraient être facilitées par la conception et l'implantation en salle de commande. Toutes les commandes, affichages et alarmes nécessaires à un fonctionnement sûr, à l'arrêt du réacteur, à l'évacuation de la chaleur résiduelle du réacteur et aux fonctions du système de confinement devraient être rapidement et facilement utilisables et devraient présenter clairement les informations à l'opérateur.

5.26. Les informations concernant les actions importantes pour la sûreté réalisées par les opérateurs à l'extérieur de la salle de commande principale devraient être disponibles immédiatement dans la salle de commande, sauf lorsque la salle de commande a été endommagée ou abandonnée. Dans ce cas, les informations nécessaires devraient être disponibles dans une salle de commande supplémentaire.

5.27. Les exigences relatives à la conception prévoient que (réf. [1], par. 6.84) la conception soit telle qu'elle minimise la probabilité qu'une action d'un opérateur puisse éventuellement nuire à l'efficacité du système de protection en fonctionnement normal et lors d'incidents d'exploitation prévus mais sans annuler les actions correctes de l'opérateur dans des conditions accidentelles de dimensionnement.

Déclenchement intempestif

5.28. Un déclenchement intempestif peut avoir de nombreuses causes, en particulier, une défaillance des équipements, des marges de déclenchement inadéquates pour certains paramètres compte tenu des variations se produisant lors d'un fonctionnement normal ou une erreur humaine au cours d'interventions. Elles peuvent résulter des points suivants:

— mauvaise prise en compte des réponses de la centrale aux perturbations en exploitation et des variations qui en découlent pour les paramètres surveillés;
— mauvaise prise en compte de l'inexactitude des instruments, des incertitudes relatives à l'étalonnage et à la dérive, et des erreurs lors du réglage des seuils de déclenchement;
— mauvais traitement du rapport signal–bruit; ou
— combinaison de ces facteurs.

5.29. La principale exigence pour le système de protection devrait être d'exécuter correctement les actions de protection qui lui ont été assignées. Néanmoins, le nombre de déclenchements intempestifs devrait être minimisé dans la mesure du possible car ils peuvent conduire à:

— une contrainte et une fatigue inutile des équipements;
— la nécessité d'autres actions de sûreté;
— une perte de confiance de l'opérateur vis-à-vis des équipements, ce qui peut éventuellement conduire à négliger des signaux valides; et
— une perte de capacité de production dans la centrale.

5.30. Le système de protection devrait donc être conçu de façon à satisfaire aux exigences pertinentes tout en minimisant le nombre de déclenchements intempestifs. Une action intempestive du système de protection ne devrait pas déclencher d'événement affectant la sûreté. Si un déclenchement intempestif du système de protection peut éventuellement entraîner un état de la centrale exigeant une protection de cette dernière, des conditions de sûreté devraient être maintenues grâce à des actions déclenchées par les parties non affectées du système de protection, les systèmes de commande de sûreté et les fonctions support des systèmes de sûreté.

5.31. Les mesures efficaces pour réduire le nombre de déclenchements intempestifs incluent le filtrage du signal en ligne, la validation des paramètres, la logique de vote des signaux redondants et la mise en service par mise en tension.

Interaction entre le système de protection et les autres systèmes

5.32. Les interactions possibles entre le système de protection et les systèmes de contrôle-commande devraient être évaluées. Les exigences relatives à la conception prévoient que l'interférence entre le système de protection et les systèmes de contrôle-commande soit empêchée en évitant les interconnexions

ou en mettant en place un isolement fonctionnel convenable (réf. [1], par. 6.86). Si des signaux sont utilisés conjointement par le système de protection et un système de contrôle-commande, une séparation appropriée (comme un découplage adéquat) doit être assurée.

5.33. Si une défaillance d'un système de contrôle-commande peut conduire à une condition de la centrale nécessitant une action de sûreté et peut simultanément désactiver une voie à l'intérieur du groupe de sûreté qui protège contre cette condition, les exigences de sûreté devraient continuer à être respectées dans l'hypothèse d'une défaillance unique simultanée n'importe où dans ce groupe de sûreté. S'il lui est permis de fonctionner avec une voie de protection bipassée ou mise hors service pour test ou maintenance, son bipasse ou sa mise hors service devraient être pris comme hypothèse dans l'analyse.

5.34. Si un EIP peut entraîner une action du système de contrôle-commande qui conduit à une condition de la centrale nécessitant une action de sûreté, le même EIP ne devrait pas empêcher une action appropriée du groupe de sûreté mis en place pour offrir une protection contre cette condition de la centrale. Parmi les mesures efficaces empêchant des interactions de ce type, on peut citer:

— des équipements supplémentaires dans le groupe de sûreté destinés à faire face à l'interaction potentielle;
— la mise en place de barrières et/ou d'autres dispositifs dans la centrale pour limiter les dommages résultant de l'EIP; ou
— une combinaison de ces éléments afin que le groupe de sûreté et/ou la conception de la centrale soient suffisants pour maintenir la condition de la centrale dans des limites acceptables.

5.35. Lorsqu'un actionneur individuel comme un moteur de pompe ou un actionneur de vanne est commandé par le système de contrôle-commande de la centrale et par le système de protection, le système de protection devrait être capable d'annuler l'action demandée par le système de contrôle-commande. Par exemple, si le système de contrôle-commande demande à une pompe de fonctionner à la moitié de sa puissance et le système de protection demande à cette pompe de fonctionner à pleine puissance, la demande du système de protection devrait être prioritaire et la pompe devrait fonctionner à pleine puissance. De même, si le système de contrôle-commande demande à une vanne de se fermer et le système de protection lui demande de s'ouvrir, la demande du système de protection devrait être prioritaire et la vanne devrait s'ouvrir.

Inhibitions d'exploitation

5.36. Les seuils d'arrêt d'urgence qui protègent le réacteur lors d'un mode de fonctionnement normal peuvent empêcher le passage à d'autres états de fonctionnement. Par exemple, les seuils d'arrêt d'urgence qui protègent le réacteur à faible puissance empêcheront le réacteur d'atteindre sa pleine puissance. Pour permettre de tels changements, le déclenchement d'une action protectrice inutile et non souhaitée devrait être inhibé au moyen d'une inhibition d'exploitation (appelé parfois circuit permissif). Ce circuit permissif devrait être intégré dans le système de protection.

5.37. Chaque fois que les conditions d'autorisation du permissif ne sont pas remplies, les systèmes de sûreté devraient automatiquement empêcher l'activation du permissif opérationnel et devraient accomplir une des actions suivantes:

— supprimer le permissif opérationnel activé;
— placer la centrale dans un état où le permissif est autorisé, ou
— déclencher les actions protectrices appropriées.

5.38. Quelle que soit la manière dont l'activation est faite, les moyens employés pour activer le permissif sont considérés comme faisant partie du système de protection et devraient se conformer au présent guide de sûreté.

ALIMENTATION EN ÉNERGIE

5.39. L'alimentation en énergie (électrique, pneumatique ou hydraulique, suivant le cas) devrait être compatible avec les systèmes CCI. Le classement, la qualification, la testabilité, la maintenabilité et l'indication de mise hors service de la source d'énergie des systèmes CCI importants pour la sûreté devraient être cohérents avec les exigences de fiabilité des systèmes CCI qu'elle dessert.

5.40. L'alimentation en énergie fournit habituellement un moyen de propagation des effets de l'interférence électrique qui peuvent être générés à l'extérieur des systèmes CCI ou peuvent provenir des autres systèmes CCI reliés directement ou indirectement à la même alimentation en énergie. La conception de l'alimentation en énergie et des systèmes CCI devrait garantir que ces effets d'interférence ne seront pas assez importants pour affecter les fonctions du système CCI. Ce point devrait être confirmé par des tests, une analyse ou d'autres moyens appropriés d'évaluation des systèmes CCI intégrés

importants pour la sûreté et leur(s) système(s) d'alimentation associé(s) (voir également la section 4).

5.41. Les systèmes CCI importants pour la sûreté qui doivent être utilisables à tout moment lors d'états d'exploitation ou dans des conditions accidentelles de dimensionnement devraient être connectés à une alimentation en énergie ne pouvant pas être interrompue. Les exigences de performance des alimentations en énergie non interruptibles devraient satisfaire aux exigences du système qu'elles desservent.

5.42. Les systèmes CCI importants pour la sûreté peuvent être connectés par les opérateurs de la centrale ou à l'aide de commutations automatiques à une alimentation de secours au lieu de l'alimentation normale lorsque les circonstances de fonctionnement le justifient, à condition que les fonctions des systèmes CCI puissent supporter l'interruption d'approvisionnement en énergie associée. Le circuit de transfert devrait dans la plupart des cas être considéré comme un prolongement du ou des systèmes d'alimentation en énergie.

SYSTÈMES PROGRAMMÉS

5.43. Les systèmes programmés sont utilisés dans les systèmes CCI importants pour la sûreté pour remplir les fonctions de protection, d'acquisition de données, de calcul, de surveillance et d'affichage. S'ils sont bien conçus, ils peuvent offrir plus d'avantages que les systèmes analogiques en ce qui concerne la fiabilité, l'exactitude et la fonctionnalité. Le système programmé peut se présenter sous différentes formes, depuis une unité centrale de taille importante prenant en charge de nombreuses fonctions jusqu'à un réseau réparti de petits processeurs affectés à des applications spécifiques.

5.44. Les systèmes programmés peuvent être utilisés avec profit pour la détection et la surveillance des défaillances internes et externes aux systèmes et équipements de la centrale importants pour la sûreté.

5.45. Le matériel et le logiciel des systèmes programmés devraient être configurés de façon à ce que le système fonctionne de manière sûre et prédéfinie dans des conditions de défaillances plausibles du matériel et du logiciel.

5.46. Avec les ordinateurs il est possible d'avoir un ensemble d'équipements qui remplissent plusieurs fonctions système. Un des inconvénients est que, si un

des composants se retrouve hors service, plusieurs fonctions peuvent tomber en panne simultanément. Ce facteur devrait donc être pris en compte lors de la conception et de l'analyse des systèmes.

5.47. Lorsque l'utilisation d'un ordinateur met en jeu deux ou plusieurs fonctions qui appartiennent à des classes de sûreté différentes, le système programmé devrait satisfaire aux exigences de la classe de sûreté supérieure.

5.48. Le démarrage et la réinitialisation d'un système programmé (par exemple après une coupure provisoire de l'alimentation électrique) devraient placer le système dans un état prédéfini garantissant un fonctionnement sûr ininterrompu.

5.49. Le logiciel du système programmé devrait être bien documenté et développé en utilisant une procédure d'ingénierie contrôlé.

5.50. Un guide de sûreté de l'AIEA [2] donne d'autres recommandations sur l'utilisation de systèmes programmés.

Maintenance

5.51. Une expertise technique adéquate de la technologie d'origine du matériel et du logiciel devrait être maintenue pendant toute la durée de vie de la centrale. Contrairement à ce qui se passe normalement pour les autres systèmes de la centrale, la maintenance des systèmes programmés n'est pas une maintenance de routine. Le personnel de maintenance devrait posséder une connaissance approfondie des exigences des systèmes programmés et du processus de développement utilisé pour la mise à niveau informatique.

Mises à niveau des systèmes numériques

5.52. Il faudrait admettre que les systèmes CCI programmés des nouvelles centrales nucléaires vieilliront eux aussi, deviendront obsolètes et devront finalement être remplacés. Étant donné que les fournisseurs d'équipements numériques changent fréquemment leurs gammes de produits, il devient difficile de conserver un stock de pièces détachées pour toute la durée de vie de la centrale. L'utilisateur doit stocker une quantité importante de composants numériques et, ce faisant, devrait envisager la détérioration possible de ces équipements électroniques stockés pendant une longue période.

Communication de données

5.53. La communication de données telle qu'elle est définie dans le cadre du présent guide de sûreté est la transmission d'un endroit à un autre de deux ou plusieurs signaux ou messages sur un seul canal de transmission de données en utilisant la répartition dans le temps, la répartition en fréquence, les techniques de codage des impulsions ou techniques similaires. La communication de données englobe une gamme variée de solutions techniques allant du simple matériel ne faisant que le multiplexage aux protocoles de communication complexes autocorrecteurs et multicouche contrôlés par le logiciel.

5.54. Les voies de communication de données importantes pour la sûreté devraient satisfaire aux recommandations concernant l'indépendance données dans la section 4, en particulier les par. 4.36–4.48.

5.55. La conception du système de communication des données devrait assurer la détection et, dans la mesure du possible, la correction des erreurs et prévoir l'état des données dans les informations transmises.

5.56. Le contrôle de la transmission de données peut être effectué périodiquement sous forme d'une fonction d'autocontrôle automatique. La fréquence choisie pour cet autocontrôle devrait être adaptée à l'utilisation des données et à la fréquence de sollicitations pour les fonctions de sûreté assurées par le système. Des dispositifs de détection et de correction des erreurs peuvent être utilisés pour augmenter la fiabilité de la transmission des signaux et atteindre ainsi les objectifs de fiabilité.

5.57. La technologie des communications devrait être choisie et convenablement configurée de façon à garantir sa capacité à satisfaire aux exigences de temps de réponse dans toutes les conditions possibles de chargement de données.

5.58. Lorsque la fiabilité des données et de la liaison entre données ont une grande importance, une technologie de communication appropriée devrait être sélectionnée. La sélection et l'utilisation d'une technologie plus complexe peut présenter des avantages fonctionnels mais peut également amener des modes de défaillance supplémentaires et des difficultés de validation. L'utilisation de la redondance pour la liaison de données, le niveau de confiance accordée à la liaison de données en général et la capacité des systèmes d'émission et de réception à faire face à tous les modes de défaillance possibles devraient être sérieusement étudiés. L'utilisation de la communication de données ne devrait

pas aller à l'encontre du découpage en canaux physique ou fonctionnel du traitement ou des éléments logiques dans l'architecture du système.

5.59. La circulation de données de systèmes appartenant à une classe de sûreté inférieure vers des systèmes de classe supérieure devrait être évitée dans la mesure du possible. Lorsque ce type de circulation de données est indispensable, des mesures (comme la validation des données ou le contrôle de la plage de données) devraient être prises pour garantir que les données du système de classe inférieure ne peuvent pas compromettre des fonctions importantes pour la sûreté.

6. INTERFACE HOMME–MACHINE

6.1. La surveillance et la commande des systèmes importants pour la sûreté mettent en jeu une combinaison de fonctions automatiques de mesure et de contrôle-commande ainsi que la surveillance et le contrôle par des opérateurs. Bien que le contrôle automatique et le déclenchement automatique des systèmes de sûreté soient couramment utilisés dans les centrales nucléaires modernes, les opérateurs gardent la maîtrise globale de la centrale.

6.2. Un des principaux objectifs devrait être de réaliser une conception compatible avec les forces et les faiblesses des êtres humains que sont les opérateurs. Afin d'obtenir une interface efficace entre le personnel d'exploitation et la centrale, la conception de l'interface homme–machine avec les fonctions et responsabilités du personnel de la centrale devrait faire l'objet d'une attention toute particulière. Ceci inclut la prise en considération non seulement des opérateurs mais également du personnel de maintenance, des inspecteurs, du personnel administratif et du personnel affecté aux situations d'urgence.

6.3. L'établissement des principes de conception des dispositifs de commande et d'affichage des informations doit tenir compte du double rôle de l'opérateur: celui de gestionnaire des systèmes, y compris la gestion des accidents, et celui d'opérateur en ce qui concerne les équipements.

6.4. Les exigences relatives à la conception exigent (réf. [1], par. 5.54) que l'opérateur, dans son rôle de gestionnaire des systèmes, possède les informations qui lui permettent:

— l'évaluation directe de l'état général de la centrale, quelle que soit sa condition, en fonctionnement normal, lors d'un incident d'exploitation prévu ou lors d'une condition accidentelle, et la confirmation de la mise en œuvre des actions de sûreté automatiques prévues;
— la détermination des actions appropriées, déclenchées par l'opérateur, à mettre en œuvre.

6.5. Les exigences relatives à la conception prévoient (réf. [1], par. 5.55) que l'opérateur, dans son rôle d'opérateur des équipements, ait à sa disposition suffisamment d'informations sur les paramètres associés aux systèmes et équipements individuels de la centrale pour confirmer que les actions de sûreté nécessaires peuvent être mises en œuvre de façon efficace.

6.6. En général, vu le nombre important de paramètres et d'équipements de la centrale qui sont généralement instrumentés et gérés dans une centrale nucléaire moderne, un soin particulier devrait être apporté à l'interface homme–machine pour garantir que toutes les informations nécessaires sont à la disposition de l'opérateur à tout moment et partout où cela est nécessaire. Cependant, il ne faudrait pas que l'opérateur soit submergé par des volumes importants de données qui pourraient être difficiles à assimiler à cause des limites humaines de perception, connaissance et mémoire. De même, lors de la conception de systèmes comportant des actions de commande déclenchées par l'opérateur, il faudrait veiller particulièrement à réduire la probabilité d'une erreur humaine et à garantir que le système peut faire face aux erreurs qui pourraient se produire.

6.7. Les exigences relatives à la conception prévoient (réf. [1], par. 5.50) que les facteurs humains et l'interface homme–machine soient systématiquement pris en compte dans le processus de conception au début du développement de la conception et tout au long du processus afin de garantir une distinction nette et appropriée des fonctions entre le personnel d'exploitation et les systèmes automatiques mis en place.

6.8. Il faudrait veiller à ce que les opérateurs de la centrale et le personnel de maintenance aient à leur disposition les informations nécessaires pour comprendre l'état de la centrale et leur permettre ainsi d'accomplir leurs tâches. La mise en œuvre d'un programme d'ingénierie des facteurs humains commençant dans les toutes premières phases de conception est une bonne méthode pour atteindre cet objectif (voir par. 7.6–7.10).

6.9. La conception, la formation, les procédures de conduite et l'organisation de l'équipe liées aux systèmes CCI devraient être étudiées dans un cycle de

conception intégré (de telle manière que, par exemple, les conséquences de l'utilisation d'une interface homme–machine informatisée sur le comportement de l'opérateur puissent être analysées). L'examen détaillé de ces considérations dépasse le cadre de ce présent guide de sûreté. D'autres normes de sûreté donneront des conseils sur le processus d'ingénierie global des facteurs humains.

6.10. Les interfaces de l'opérateur avec la centrale se trouvent principalement dans la salle de commande principale, dans le centre de support technique, dans les salles de commande supplémentaires et dans le centre de contrôle d'urgence. Ces installations comportent des affichages de données liés à la sûreté, des commandes liées à la sûreté, des systèmes de surveillance des accidents, des indicateurs d'alarme et des systèmes d'exploitation des données historiques. Des recommandations sur la conception de ces installations et systèmes sont données dans cette section.

SALLE DE COMMANDE PRINCIPALE

6.11. L'emplacement principal pour les actions de commande liées à la sûreté est la salle de commande principale. Les exigences relatives à la conception prévoient (réf. [1], par. 6.71) la mise en œuvre d'une salle de commande d'où la centrale nucléaire peut être exploitée de manière sûre pour tous les états d'exploitation et d'où des mesures peuvent être prises pour maintenir la centrale dans un état sûr ou la ramener à un état sûr après l'apparition d'incidents d'exploitation prévus, d'accidents de dimensionnement et d'accidents graves. En outre, des mesures peuvent être prises à partir de la salle de commande pour limiter les conséquence des accidents graves.

6.12. Les exigences relatives à la conception prévoient (réf. [1], par. 6.73) que l'implantation des instruments et le mode de présentation des informations offrent au personnel de conduite une vue globale adéquate de l'état et du fonctionnement de la centrale. La conception de la salle de commande doit prendre en compte les facteurs ergonomiques.

6.13. Les principaux objectifs de la conception fonctionnelle d'une salle de commande sont de fournir à l'opérateur des informations précises, complètes, en temps opportun sur l'état des systèmes et équipements de la centrale pour tous les états d'exploitation et dans des conditions accidentelles de dimensionnement et d'optimiser les activités de l'opérateur relatives à la surveillance et au contrôle de la centrale. Les exigences relatives à l'isolement fonctionnel et à la séparation physique ainsi que les principes ergonomiques devraient être pris

en compte lors de la conception de la salle de commande principale qui est un centre où les éléments de contrôle-commande et d'instrumentation des systèmes de sûreté, des systèmes liés à la sûreté et des systèmes sans importance pour la sûreté convergent.

6.14. Pour la conception de la salle de commande, les facteurs ergonomiques comme la charge de travail, la possibilité d'erreur humaine, le temps de réponse de l'opérateur et la minimisation des efforts intellectuels et physiques de l'opérateur devraient être pris en compte afin de faciliter l'exécution des procédures de conduite spécifiées pour garantir la sûreté pour tous les états d'exploitation et à la suite de conditions accidentelles de dimensionnement. Il faudrait prendre les mesures nécessaires pour garantir des conditions de travail satisfaisantes, dont les conditions d'éclairage, de température et d'humidité et pour éviter des conditions dangereuses comme des niveaux de radioactivité inacceptables ou la présence de fumée ou substances toxiques dans l'atmosphère. Les affichages, indicateurs et commandes liés à la sûreté étant généralement utilisés dans toutes les conditions de fonctionnement de la centrale, la conception de la salle de commande devrait prendre en considération, et ce de manière équilibrée, toutes les conditions envisagées. Les actions automatiques des commandes liées à la sûreté devraient être employées le plus souvent possible afin de ne pas imposer une charge trop lourde à l'opérateur lorsqu'il accomplit les fonctions de sûreté. La prise en considération des facteurs humains a conduit à la spécification de plusieurs objectifs de conception dont les plus importants sont les suivants:

— la présentation des informations au moyen de dispositifs d'affichages et d'instrumentation devrait être harmonieusement intégrée afin d'optimiser la compréhension de l'état de la centrale pour l'opérateur et les activités nécessaires pour contrôler la centrale;
— lorsque le processus surveillé fait intervenir des affichages redondants ou différents pour contrôler les informations, les autres sources d'information devraient, dans la mesure du possible, être implantées et configurées de telle manière que l'opérateur puisse utiliser toutes les sources avec un minimum d'effort pour arriver à une conclusion, sans pour cela compromettre l'indépendance des sources d'information;
— les dispositifs d'affichage de la salle de contrôle devraient être disposés de telle manière que l'opérateur puisse facilement les consulter et établir avec précision l'état de n'importe quel système;
— les équipements de commande et leurs affichages fonctionnellement associés devraient dans la mesure du possible être implantés de manière à faciliter leur mise en route par l'opérateur;

— il faudrait veiller à la nécessité pour les opérateurs d'avoir une vision globale de l'état de la centrale et à la cohérence des informations présentées aux différents opérateurs présents dans la salle de commande;
— certains affichages peuvent présenter des paramètres provenant d'instruments de contrôle possédant différents niveaux de qualification (et donc de fiabilité); dans ces cas-là, la différence de niveau de qualification devrait être mise en évidence pour l'opérateur sur l'affichage.

SALLES DE COMMANDE SUPPLÉMENTAIRES

6.15. Outre la salle de commande principale, différents types de salles de commande supplémentaires et divers emplacements pour les commandes sont utilisés. Le détail de la nomenclature et de l'affectation des fonctions varie parmi les États Membres, mais les autres salles de commande et emplacements des commandes incluent:

— la salle de commande d'urgence,
— la zone de commande secondaire,
— le panneau d'arrêt de sûreté,
— les salles de commande supplémentaires, et
— les autres postes de contrôle-commande locaux.

D'autres renseignements sont fournis dans la réf. [4]. Des recommandations sur la conception sont donnés dans ce qui suit.

6.16. Les exigences relatives à la conception prévoient (réf. [1], par. 6.75) que suffisamment d'équipements CCI soient mis à disposition, de préférence dans un endroit unique physiquement et électriquement séparé de la salle de commande, afin que le réacteur puisse être placé et maintenu dans un état d'arrêt sûr, que la chaleur résiduelle puisse être évacuée et que les variables principales de la centrale puissent être surveillées dans le cas où l'on ne peut plus réaliser ces fonctions de sûreté à partir de la salle de commande. Ces instruments sont généralement situés dans une salle de commande supplémentaire.

6.17. Le dimensionnement de la centrale devrait définir les conditions dans lesquelles il n'est plus possible d'accomplir les fonctions de commande à partir de la salle de commande principale du fait de conditions hostiles, d'un incendie ou autres raisons pouvant nécessiter l'abandon de la salle de commande principale.

6.18. Des mesures appropriées devraient être prises pour transférer les commandes prioritaires dans un nouvel emplacement et isoler les équipements

présents dans la salle de commande principale chaque fois que cette dernière est abandonnée.

6.19. Le dimensionnement d'une centrale nucléaire est habituellement tel que l'indisponibilité de la salle de commande du fait d'un EIP est très peu fréquente. Il est donc inutile de faire l'hypothèse qu'un deuxième EIP se produira lorsque la salle de commande principale sera indisponible et que les fonctions de sûreté nécessaires seront accomplies à partir d'une salle de commande supplémentaire.

6.20. Si le dimensionnement exige de prendre en compte l'endommagement des équipements présents dans la salle de commande, les exigences relatives à l'indépendance devraient être appliquées aux circuits alimentant cette zone afin que les défaillances provoquées par l'EIP dans une zone (par exemple, courts-circuits, circuits ouverts et surtensions) n'empêchent pas l'exécution des tâches nécessaires dans une autre zone. En fonction de la nature de l'événement et de la conception de la centrale, il peut être nécessaire d'installer des lignes d'instrumentation, des voies logiques et autres équipements de sûreté redondants pour chaque zone. Lorsque des actionneurs de sûreté communs sont utilisés, la priorité des signaux de commande devrait être établie dans le dimensionnement.

6.21. La conception des salles de commande supplémentaires devrait comporter des mesures appropriées pour empêcher les accès et usages non autorisés.

6.22. La commande manuelle à partir d'une salle de commande supplémentaire devrait, normalement, être effectuée à l'aide d'actions simples comme actionner un interrupteur ou appuyer sur un bouton. Dans la mesure du possible, les affichages et les commandes devraient être similaires à ceux de la salle de commande principale.

6.23. La conception de la salle de commande principale et des salles de commande supplémentaires devrait être telle qu'aucun EIP puisse affecter simultanément la salle de commande principale et les salles de commande supplémentaires assez gravement pour que les fonctions de sûreté nécessaires ne puissent plus être remplies.

6.24. Il faudrait également veiller à ce que la priorité nécessaire pour déclencher une fonction spécifique de sûreté soit attribuée soit à la salle de commande principale soit à une salle supplémentaire.

6.25. Les parties applicables des autres sections du présent guide de sûreté devraient être prises en compte pour la conception des salles de commande supplémentaires et les différences d'objectif et d'utilisation entre les salles de commande supplémentaires et la salle de commande principale devraient être dûment prises en considération.

6.26. En fonction de la nature de l'EIP, la mise en place de voies d'instrumentation indépendantes de celles de la salle de commande principale devrait faire l'objet d'une étude. Il faudrait également prendre en compte les besoins particuliers en fonctions support du système de sûreté, le cas échéant.

6.27. Il faudrait également veiller avec soin à garantir qu'un chemin d'accès approprié soit prévu dans la conception pour permettre aux opérateurs abandonnant la salle de commande principale de se diriger en toute sécurité et facilement vers les salles de commande supplémentaires.

6.28. Un signalisation adéquate des dangers potentiels (comme la fumée) et des mesures de prévention (comme des masques à gaz) devraient être prévues tout le long du chemin d'accès allant de la salle de commande principale aux salles de commande supplémentaires.

6.29. Les salles de commande supplémentaires devraient être implantées et configurées de telle manière que les opérateurs puissent commencer leurs tâches dans le nouvel emplacement dans un délai acceptable.

6.30. Si l'analyse de la sûreté montre qu'une occupation à long terme se révèle nécessaire, l'habitabilité devrait être assurée, au moyen d'une ventilation par exemple. Il faudrait également prévoir des sièges, des moyens pour écrire, l'accès aux documents et suffisamment d'espace pour étaler les documents.

CENTRE TECHNIQUE DE CRISE

6.31. La salle de commande principale est, pour l'opérateur, le centre d'activation et d'information de la centrale pour les états d'exploitation et les conditions accidentelles de dimensionnement. Elle peut également être utilisée comme centre principal pour diriger les activités à l'extérieur du site en cas d'urgence pendant leur phase initiale. Cependant, les opérations d'intervention en cas d'urgence à l'extérieur du site ne devraient pas empêcher la capacité du personnel de la salle de commande à mettre en œuvre des procédures de gestion d'accident. En conséquence, des mesures devraient être prises pour

transférer les aspects non opérationnels de l'intervention en cas d'urgence, comme la direction des équipes ou les notifications et la coordination à l'extérieur du site, hors de la salle de commande dès que possible, et pour limiter l'accès à la salle de commande en cas d'urgence.

6.32. Les exigences relatives à la conception prévoient (réf. [1], par. 6.87) qu'un centre de contrôle d'urgence sur place, séparé de la salle de commande de la centrale, soit mis en place pour servir de lieu de réunion à l'équipe d'urgence qui opérera à partir de cet endroit en cas d'urgence. Les informations concernant les paramètres importants de la centrale et les conditions radiologiques dans la centrale et les environs immédiats devraient être fournies dans ce centre de contrôle d'urgence. La salle devrait mettre à disposition des moyens de communication avec la salle de commande, les salles de commande supplémentaires et les autres emplacements importants de la centrale ainsi qu'avec les organisations d'intervention en cas d'urgence sur place et à l'extérieur du site. Des mesures appropriées doivent être prises pour protéger les occupants pendant une période prolongée contre les risques résultant d'un accident grave.

6.33. Outre les dispositions locales relatives à la gestion d'un accident, certains États Membres ont trouvé qu'il était efficace d'avoir un centre de support d'urgence éloigné du site pour permettre la coordination des avis donnés par les experts. De même, des systèmes d'information et de communication appropriés devraient être mis en place pour les installations de ce type.

6.34. Des informations supplémentaires sur les centres techniques de crise sont données dans les réf. [4, 13].

DISPOSITIFS DE COMMANDE

6.35. Si les appareils importants pour la sûreté peuvent être commandés à partir de la salle de commande et à partir d'emplacements situés à l'extérieur de la salle de commande, le lieu réel de commande devrait être indiqué visuellement (alarmes, voyants lumineux testables, positions d'interrupteur manuel) dans chaque lieu de commande.

6.36. La salle de commande devrait comporter toutes les commandes nécessaires pour faire face aux conditions accidentelles pour lesquelles:

— l'exécution des commandes nécessaires à l'extérieur de la salle de commande peut être limitée par les conditions accidentelles, et
— les temps impartis pour faire face aux conditions accidentelles peuvent empêcher l'opérateur de quitter la salle de commande pour actionner les commandes ailleurs.

6.37. Des fonctions de service adéquates, comme l'éclairage et les installations de communication et de lutte contre l'incendie, devraient être mises en place pour permettre au personnel d'exploitation de la centrale d'interpréter les affichages de contrôle et de mettre en œuvre les actions de sûreté appropriées après un EIP.

6.38. Lors de la conception des dispositifs de commande, il faudrait prendre en compte les aspects n'ayant aucun rapport avec les systèmes CCI comme la radioprotection [12], l'habitabilité [8], la protection contre la foudre, la protection contre l'incendie [6], l'accessibilité et le contrôle d'accès, la protection contre les missiles [7, 8] et la résistance sismique [14], en fonction des EIP d'origine interne ou externe spécifiés pour la centrale.

6.39. Les communications orales entre la salle de commande principale, les salles de commande supplémentaires, les autres emplacements concernés de la centrale et les services d'urgence à l'extérieur du site sont importantes pour la sûreté, particulièrement dans des conditions d'incidents d'exploitation prévus ou d'accidents de dimensionnement. Ces communications devraient normalement être munies de deux liaisons de communication, de préférence diversifiées, et devraient être compatibles du point de vue électromagnétique avec les systèmes CCI (téléphones auto-alimentés, téléphones fonctionnant sur batteries, téléphones portables). Ces liaisons de communication devraient être acheminées de telle manière que les incendies, défaillances de circuits électriques ou autres EIP applicables ne puissent pas rendre inopérants les deux systèmes simultanément.

AFFICHAGES

6.40. Les affichages informent les opérateurs de la centrale de son état et de l'état des systèmes et équipements nécessaires pour surveiller, gérer et faire fonctionner les systèmes importants pour la sûreté et pour maintenir la centrale à l'intérieur des limites du dimensionnement. Les affichages sont utilisés pour accomplir une ou plusieurs des fonctions suivantes:

— informer les opérateurs de la centrale de l'état des systèmes et de l'état de sûreté de la centrale;

— informer les experts en sûreté sur place et à l'extérieur du site de l'état de sûreté de la centrale dans des conditions accidentelles; et
— fournir des informations sur l'évolution au cours du temps des variables de fonctionnement importantes pour la sûreté afin de procéder à des analyses immédiates ou ultérieures et pour présenter des comptes rendus à l'organisation d'exploitation ainsi qu'aux autorités extérieures.

6.41. Les modifications de l'état des systèmes de sûreté devraient être signalées par alarme et l'état devrait être indiqué dans la salle de commande.

6.42. En fonctionnement normal, les opérateurs surveillent en continu l'état de la centrale à l'aide des tableaux de signalisation et alarmes ou des écrans de visualisation se trouvant dans la salle de commande principale. Des alarmes ou autres dispositifs indiquent les écarts par rapport au fonctionnement normal. Lorsque ceux-ci se produisent, les opérateurs devraient posséder les informations nécessaires pour:

— identifier les actions initiées par les systèmes automatiques;
— analyser la cause de la perturbation;
— suivre le comportement de la centrale; et
— effectuer toute intervention manuelle nécessaire.

6.43. Les dispositifs d'affichage devraient couvrir les variables appropriées, conformément aux hypothèses de l'analyse de la sûreté et aux informations dont l'opérateur a besoin pour les états d'exploitation et les conditions accidentelles de dimensionnement. L'exactitude et la gamme de variation des affichages devraient être cohérentes avec les hypothèses de l'analyse de sûreté.

6.44. Lorsque des dispositifs d'affichage redondants sont utilisés pour satisfaire aux exigences de fiabilité, ils devraient être fonctionnellement isolés et séparés physiquement afin de garantir qu'une défaillance unique de ce système n'entraînera pas une perte complète des informations relatives à une variable surveillée; en utilisant, par exemple, deux claviers pour les écrans de visualisation multiples.

6.45. Si la défaillance d'un seul circuit d'affichage peut éventuellement rendre les informations ambiguës (par exemple, une défaillance unique entraînant une discordance entre deux affichages redondants), l'opérateur peut être conduit à faire échouer ou rater l'exécution d'une fonction de sûreté nécessaire. Pour éviter cela, des moyens supplémentaires devraient être mis en place pour

permettre à l'opérateur de résoudre ces problèmes d'informations contradictoires. Ceci peut se faire, par exemple, en installant un troisième circuit d'information ou en affichant une autre variable liée par une relation connue aux circuits d'affichage concernés et permettant l'identification du circuit défectueux. Un circuit d'affichage unique possédant un mode de défaillance clairement identifiable peut convenir lorsque le temps moyen de détection et de réparation ou de remplacement est inférieur au temps d'indisponibilité tolérable.

6.46. Lorsqu'il est indispensable de savoir comment évolue une variable pour déterminer l'action appropriée de l'opérateur, un moyen d'affichage de cette évolution devrait être fourni.

6.47. Si une partie d'un système important pour la sûreté a été mise volontairement hors service en utilisant un dispositif prévu à cet effet dans la conception, cette condition devrait être automatiquement affichée dans la salle de commande. Si une partie d'un système important pour la sûreté a été mise hors service par un moyen administratif, ceci devrait être clairement indiqué dans la salle de commande.

SURVEILLANCE DES CONDITIONS ACCIDENTELLES

6.48. Un affichage fiable, facilement accessible et compréhensible des informations sur l'état de la centrale et des évolutions de ses paramètres essentiels devrait être mis en place pour garantir que l'opérateur peut efficacement faire face aux conditions accidentelles et que le personnel support venu en aide est convenablement informé. Des recommandations concernant la conception des systèmes et installations de surveillance des accidents sont données ci-après.

6.49. Des dispositifs d'affichage des informations destinés à la surveillance des conditions accidentelles dans la centrale devraient être installés dans la salle de commande principale et, si nécessaire, dans les salles de commande supplémentaires.

6.50. La décision concernant les informations à afficher devrait prendre en compte le fait que l'opérateur a besoin de:

— reconnaître un écart par rapport aux conditions normales;
— identifier l'accident particulier et, si possible, son événement initiateur;

— vérifier que les fonctions de sûreté nécessaires sont assurées;
— suivre le déroulement de l'événement ou de l'accident;
— déterminer le moment où l'évolution des conditions justifie que les autorités prennent des mesures d'urgence à l'extérieur de la centrale;
— résoudre les problèmes d'informations contradictoires qui peuvent résulter de la redondance des circuits d'affichage.

6.51. Pour permettre de déterminer si les fonctions de sûreté nécessaires sont mises en œuvre, les appareils de surveillance des conditions accidentelles devraient être conçus de façon à permettre à l'opérateur de confirmer que:

— le réacteur est arrêté et le restera;
— la chaleur résiduelle est évacuée et continuera à être évacuée du cœur par d'autres composants importants pour la sûreté vers la source froide finale;
— toute barrière conçue pour éviter les rejets radioactifs dans l'environnement est en place et le restera.

6.52. Les paramètres de la centrale à surveiller pour cette confirmation devraient être ceux appropriés à la conception et au site du réacteur.

6.53. Les équipements de surveillance des conditions accidentelles devraient être capables de fonctionner dans l'environnement présent après l'accident lorsque nécessaire et pendant la période nécessaire. Les plages de mesure des paramètres clés sélectionnés devraient être étendues aux valeurs qui peuvent être atteintes lors d'événements pouvant mettre à l'épreuve les barrières contre le rejet de matières radioactives émanant du combustible, du système caloporteur ou du confinement, ou pouvant entraîner un rejet de matières radioactives en dehors d'une ou plusieurs de ces barrières.

6.54. Les affichages utilisés pour la surveillance après accident devraient être distincts des autres affichages.

6.55. Lorsque des données historiques sont nécessaires pour l'analyse de l'accident ou les mesures d'urgence, une possibilité d'enregistrement et de récupération des données appropriées devrait être fournie.

6.56. La centrale devrait être équipée d'installations permettant de communiquer les données adéquates aux installations d'urgence spécifiées dans la réf. [13] sans perturber excessivement les activités de la salle de commande qui sont exécutées en cas d'urgence.

SYSTÈMES D'ALARME

6.57. Les systèmes d'alarme, visuels et sonores, sont utilisés pour attirer l'attention des opérateurs sur la nécessité d'intervenir sur le fonctionnement de la centrale en déclenchant, par exemple, les fonctions des systèmes de sûreté ou les actions de maintenance ou de commande de la centrale afin de garantir que l'état de la centrale reste dans les limites prévues du dimensionnement. Les recommandations suivantes concernent l'utilisation des alarmes dans le cas des systèmes importants pour la sûreté.

6.58. Des alarmes visuelles ou sonores devraient être installées aux endroits appropriés et activées au moment opportun, en fonction des besoins fondamentaux dictés par les actions des opérateurs.

6.59. Lors de la conception des systèmes d'alarme, il faudrait veiller soigneusement à garantir que les opérateurs puissent réellement distinguer les informations essentielles, particulièrement lors d'incidents de fonctionnement prévus et lors de conditions accidentelles qui peuvent activer un grand nombre d'alarmes. Diverses techniques existent pour atteindre cet objectif; ce sont, par exemple, le regroupement, la fixation de priorités et le conditionnement des alarmes ainsi que la différenciation sonore ou visuelle pour faire la distinction entre des alarmes de différents types et différentes priorités.

6.60. L'application des techniques permettant d'éviter de submerger l'opérateur d'informations d'alarmes ne devrait pas conduire à la suppression des informations nécessaires à l'identification de l'emplacement et des conséquences potentielles du défaut de fonctionnement.

6.61. L'opérateur devrait avoir à sa disposition des moyens lui permettant d'acquitter les alarmes, individuellement ou en groupes, en temps voulu.

6.62. Les signaux d'alarme sonores sont couramment utilisés pour attirer l'attention de l'opérateur sur de nouvelles conditions d'alarme. Des moyens d'arrêter les signaux sonores devraient être mis à disposition afin d'éviter une surcharge auditive et de faciliter la perception des nouvelles alarmes qui pourraient se déclencher ultérieurement. Si les alarmes sonores sont arrêtées, les indications visuelles des conditions d'alarme devraient persister jusqu'à ce que les états défectueux en cause aient été supprimés, afin de ne pas oublier ces conditions. Des moyens visuels (changement de couleur ou passage d'un signal clignotant à un signal fixe) devraient être utilisés pour faire la distinction entre les conditions d'alarme qui ont été perçues et auxquelles on

a répondu et celles qui ne l'ont pas encore été. Lorsque l'état de la centrale redevient normal, l'indication d'alarme devrait persister jusqu'à sa réinitialisation par l'opérateur, afin que les informations concernant l'alarme soient conservées.

SYSTÈME D'ENREGISTREMENT DES DONNÉES HISTORIQUES

6.63. Il faudrait fournir la possibilité d'enregistrer, de stocker et de récupérer les données des processus importants de la centrale qui enregistrent les données de fonctionnement et l'historique du comportement de la centrale. Ces systèmes destinés aux données historiques prennent généralement en charge les éléments suivants:

— informations supplémentaires pour les équipes d'opérateurs (donnant les évolutions et tendances à court et long terme);
— informations générales d'exploitation pour la direction de la centrale;
— diagnostic et analyse à court et long terme du fonctionnement normal et des accidents.

6.64. Traditionnellement, des systèmes de copie papier (impression des données sur papier) ont été utilisés pour ces fonctions. Toutefois, l'utilisation de systèmes programmés devrait être envisagée car elle facilite le stockage, la récupération et le traitement des grands volumes de données qui sont généralement mis en jeu. Généralement, avec les systèmes programmés, des imprimantes bien situées devraient être mises à disposition des utilisateurs pour leur permettre d'imprimer des copies papier.

6.65. Les terminaux permettant d'accéder aux informations historiques devraient être placés dans la salle de commande principale et ses environs, suivant le cas. La présence de terminaux distants, bien placés, destinés au personnel du support technique, est utile et devrait également être envisagée. Lors de la décision concernant l'emplacement des terminaux et la conception des interfaces homme–machine servant à accéder aux données historiques, il faudrait tenir compte des besoins, des tâches et des capacités des utilisateurs.

7. PROCESSUS DE CONCEPTION DES SYSTÈMES CCI IMPORTANTS POUR LA SÛRETÉ

7.1. L'ingénierie d'une centrale nucléaire est une activité complexe faisant intervenir de nombreuses disciplines techniques. L'obtention d'informations exactes, en temps opportun pour le projet, est nécessaire pour chaque discipline afin de garantir un développement adéquat de la conception. Dans le cas des systèmes importants pour la sûreté, un processus de développement structuré incorporant des méthodes prudentes et une bonne pratique technique devrait être utilisé pour garantir que les exigences relatives à la conception [1] sont correctement appliquées. Le non-respect de ce principe du fait d'un processus mal organisé ou mal géré pourrait compromettre la sûreté nucléaire.

ASSURANCE DE LA QUALITÉ

7.2. Pour atteindre les niveaux de qualité requis, il est important de s'assurer que les systèmes CCI importants pour la sûreté sont conçus, fabriqués, qualifiés, inspectés, installés, exploités, testés et maintenus conformément à un programme d'assurance de la qualité élaboré par le concepteur, le fabricant ou l'installateur et approuvé par l'organisme compétent. Ce programme devrait se conformer aux Code et guides de sûreté correspondants (réf. [3], guides de sûreté Q3 et Q10).

7.3. Le programme d'assurance de la qualité devrait inclure toutes les activités nécessaires (1) pour vérifier l'adéquation de la conception des systèmes de sûreté et (2) pour garantir que les systèmes de sûreté se conforment à toutes les normes et exigences applicables.

PLANIFICATION DE PROJET

7.4. Pour garantir la livraison en temps opportun et commercialement viable des éléments de la conception, des techniques de gestion de projet et de planification de projet devraient être utilisées. Pour les activités de planification du projet utilisées pour amener un projet à son terme, les exigences de sûreté des systèmes en cours de conception devraient être prises en compte. Un temps suffisant devrait être imparti, dans le calendrier général du projet, à la présentation des documents de conception des systèmes importants pour la sûreté à l'organisme de réglementation.

CONTRÔLE DES MODIFICATIONS ET GESTION DE LA CONFIGURATION

7.5. Tout au long du processus de conception, de la conception à l'exploitation, pour chaque itération, il faudrait exercer un contrôle sur toute modification proposée, afin de gérer la configuration de la conception. Le processus servant à apporter une modification à la conception devrait être documenté et une approbation écrite devrait être demandée et obtenue afin de garantir que la modification proposée a été dûment étudiée et que son impact peut être évalué par des personnes indépendantes du concepteur. Dans les premières phases de la conception, de nombreuses itérations peuvent être nécessaires pour déterminer la conception requise, et souvent la méthode de gestion des modifications devient moins formelle. Dans ce cas, des examens périodiques de la conception devraient être effectués afin de garantir que le personnel concerné qui n'appartient pas à l'équipe de conception est mis au courant de l'avancement de la conception et d'obtenir la confirmation que les exigences de sûreté continuent à être respectées. Cependant, lorsqu'un engagement sur une conception spécifique a été pris, une procédure formelle de contrôle des modifications de la conception devrait être établie.

INTÉGRATION DES FACTEURS HUMAINS

7.6. Étant donné l'importance et l'étendue du rôle des opérateurs et autres employés de la centrale en ce qui concerne l'exploitation et l'utilisation des systèmes CCI importants pour la sûreté (et pour la centrale dans son ensemble), des processus de traitement des facteurs humains devraient être intégrés dans le processus global de conception.

7.7. Les techniques applicables aux facteurs humains incluent l'analyse fonctionnelle, l'analyse des tâches et l'analyse de la charge de travail. Elles sont utilisées pour assigner et répartir les fonctions entre les individus et les machines et pour concevoir l'interface homme–machine. Des recommandations sur l'ingénierie des facteurs humains existent, en particulier sur l'anthropométrie, l'erreur humaine, la conception des interfaces utilisateur et divers sujets connexes. Pour tirer profit de ces connaissances, il faudrait systématiquement tenir compte des facteurs humains (voir également la section 6).

7.8. Les principes de conception ou les exigences applicables aux facteurs humains devraient être observés pour garantir la compatibilité avec les utilisateurs, la compréhensibilité et l'efficacité de l'interface homme–machine.

Le processus de conception des systèmes devrait incorporer le retour d'expérience du groupe d'utilisateurs et les mesures appropriées de vérification et de validation de l'interface homme–machine. Le programme d'ingénierie des facteurs humains (comme précisé dans la section 6) devrait être inclus dans le plan global de réalisation du projet. Les analyses et conclusions concernant les facteurs humains devraient être systématiquement documentées au cours de la conception technique et respecter les directives et les références techniques applicables aux facteurs humains.

7.9. L'évaluation des choix de conception de l'interface homme–machine est conseillée et devrait démarrer dès le début de la conception, en utilisant au départ des maquettes et des techniques de visualisation informatique. Au cours des dernières phases de la conception, une simulation pleine échelle de la salle de commande devrait être utilisée pour valider sa conception.

7.10. La conception devrait prendre en compte la possibilité d'erreurs humaines, que ce soit des omissions ou des erreurs commises par les utilisateurs du système. Pour minimiser la probabilité de conséquences préjudiciables graves résultant d'erreurs des utilisateurs, l'interface homme–machine devrait, dans la mesure du possible, être structurée au niveau conception de telle manière que de simples erreurs d'opérateur n'aient aucune conséquence et puissent être détectées et corrigées. Les situations où la probabilité d'une erreur humaine est relativement importante et peut entraîner de graves conséquences devraient être évitées grâce à une structure du système ou une conception de l'interface utilisateur appropriées ou par le recours à une automatisation.

DESCRIPTION DU PROCESSUS DE CONCEPTION

7.11. Le développement de systèmes importants pour la sûreté devrait être un processus contrôlé étape par étape. Dans cette optique, le processus de développement est organisé sous forme d'un ensemble ordonné de phases distinctes. Chaque phase utilise les informations obtenues lors des phases précédentes et fournit les informations d'entrée pour les phases suivantes. Il faut noter que le développement de systèmes importants pour la sûreté est par nature un processus itératif. Au fur et à mesure de la progression de la conception, les défauts et omissions intervenus lors des étapes antérieures apparaissent et nécessitent des itérations. Une caractéristique essentielle de cette méthode est que les résultats obtenus lors de chaque phase de développement sont vérifiés par rapport aux exigences de la phase précédente,

afin d'établir le bien-fondé de la conception. À certaines phases du développement, une validation est effectuée pour confirmer que le résultat obtenu (le produit de cette phase spécifique) est conforme aux exigences fonctionnelles et autres exigences et qu'il n'existe aucun comportement non souhaité. La vérification et la validation devraient être effectuées par des équipes indépendantes des concepteurs et des développeurs.

7.12. Les phases types d'un processus de développement systématique et un bref résumé du processus décrit dans le présent guide de sûreté sont présentés dans la fig. 4. Les cadres incluent les activités de développement à effectuer et les flèches indiquent l'ordre prévu et le flux d'informations principales. La figure 5 illustre les relations de la vérification et de la validation avec les exigences et les différentes phases de la conception et de la mise en œuvre. Le choix d'activités de développement particulières et leur ordre sur cette figure et dans le présent guide de sûreté ne sont pas destinés à imposer une méthode particulière de développement, d'autres variantes pouvant aussi être capables de satisfaire aux recommandations concernant les principes et les attributs.

7.13. La conception globale d'une centrale nucléaire commence par la conception des systèmes et composants mécaniques et fonctionnels de la centrale. Ensuite, la conception des systèmes CCI devrait être développée en fonction des résultats des analyses (déterministes et/ou probabilistes) de sûreté des événements de dimensionnement sélectionnés (voir section 3). Le processus de conception devrait comporter un processus systématique pour établir la liste des événements de référence sélectionnés, car des omissions peuvent entraîner une mauvaise spécification des besoins en ce qui concerne les mesures de sûreté et donc conduire à un système non sûr.

7.14. Les exigences relatives au système de sûreté sont établies en fonction du résultat de ces analyses. Les spécialistes de sûreté nucléaire et autres disciplines techniques, suivant le cas, devraient participer à la définition des exigences relatives au système de sûreté. Habituellement, il est nécessaire d'apporter des modifications à la conception initiale et de créer une nouvelle conception, puis de procéder à nouveau à une analyse de sûreté. Après quelques itérations, on obtient une configuration des systèmes CCI, des systèmes fonctionnels et mécaniques qui satisfait à toutes les exigences de sûreté nucléaire en vigueur.

7.15. Une fois que le développement de la conception a atteint un stade où l'on sait comment satisfaire aux exigences et comment les systèmes et composants principaux de la centrale seront configurés, la documentation de conception est généralement émise sous forme de spécifications pour l'approvisionnement.

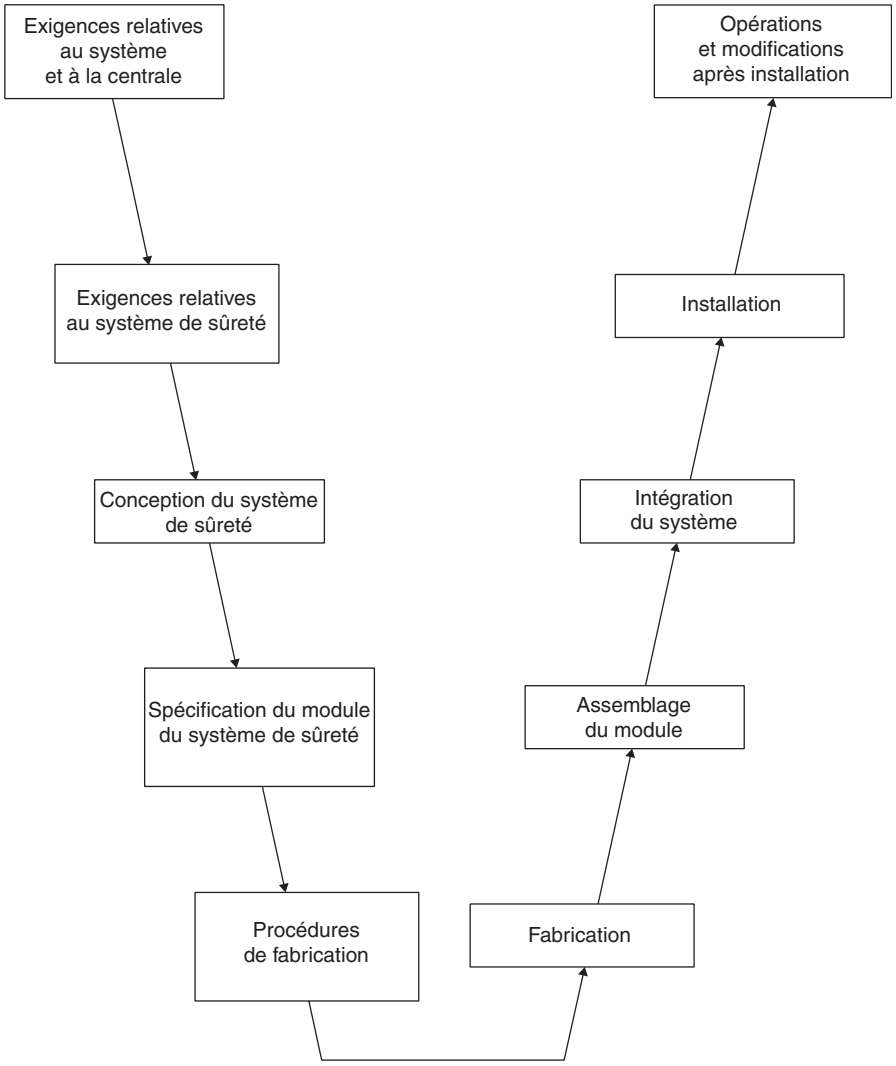

FIG. 4. Développement d'un système CCI important pour la sûreté.

Lors de la négociation des contrats pour les systèmes et les équipements de la centrale, le concepteur devrait établir un moyen de communication qui garantira que la mise en œuvre proposée par les fournisseurs pourra prouver qu'elle répond aux besoins du système. Les modalités réelles de vérification et de validation devraient être établies par le concepteur et les fournisseurs.

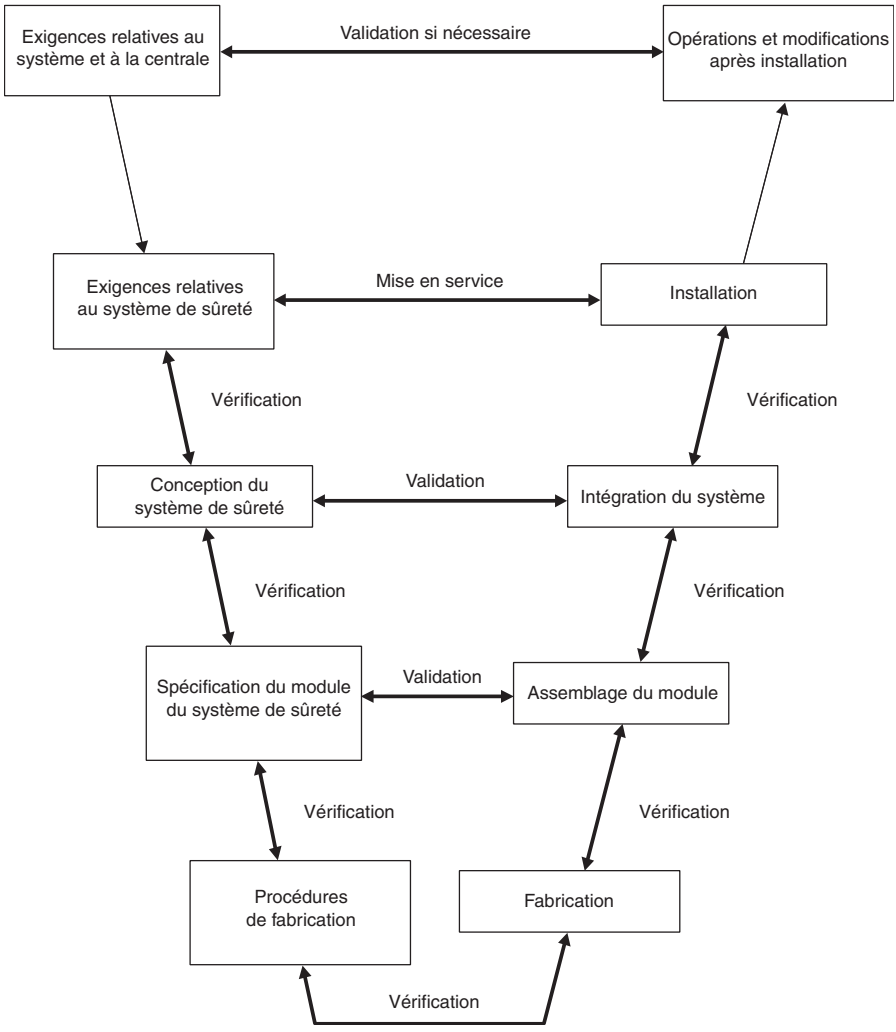

FIG. 5. Processus de vérification, validation et mise en service.

7.16. Une fois déterminées les exigences relatives au système CCI de sûreté, leur concepteur définit comment chaque exigence sera respectée en définissant les exigences de conception du système CCI de sûreté. Si un système programmé est proposé, le concepteur devrait définir les exigences relatives au système numérique support et décider de l'architecture des systèmes et des fonctions à accomplir. De même, l'affectation des fonctions à

l'homme ou à la machine devrait également être décidée. À ce stade de la conception, on saura pour quelles parties de la conception des techniques seront utilisables immédiatement et seront fiables et quelles parties nécessiteront un effort spécifique de développement. Lorsqu'un développement est nécessaire et nécessite d'être basé sur des prototypes, d'autres modèles de processus de conception peuvent se révéler plus efficaces (modèle en spirale par exemple).

7.17. Au fur et à mesure que la conception des équipements CCI est mise en œuvre et que les modules sont livrés, ces modules devraient subir une série de vérifications et de tests pour prouver que les modules ou les sous-ensembles fonctionnent comme prévu. Ceci est illustré dans la fig. 5. Souvent, à ce stade, les tests de qualification des équipements commencent au niveau du module ou du sous-ensemble et les essais de type ou les essais génériques peuvent être effectués sur les appareils qui seront utilisés dans de multiples applications. Les modules individuels sont ensuite intégrés dans les sous-systèmes pour remplir les fonctions exigées par le concepteur. D'autres tests, spécifiques à la configuration des équipements, devraient être effectués pour prouver que les modules fonctionnent ensemble dans leurs sous-systèmes correspondants. Les sous-systèmes sont ensuite combinés ou intégrés pour permettre l'exécution d'une série de 'recettes usine' sur le système dans les installations du fournisseur. Ces tests devraient prouver que la fonctionnalité du système exigée par le concepteur a été correctement mise en œuvre.

7.18. Lorsque le concepteur est satisfait du comportement du système dans les installations du fournisseur, les appareils sont acheminés jusqu'au site et installés. L'expédition ou l'installation elle-même peut affecter les performances des appareils et, de ce fait, des tests complets devraient être effectués après installation. Ces tests d'installation et ces 'tests de clôture', en plus de réitérer certains des tests finaux d'acceptation en usine, devraient garantir que le système complet est testé tel qu'il est prévu de fonctionner en pratique; par exemple, les systèmes redondants multiples devraient être testés en les faisant fonctionner ensemble plutôt que d'utiliser des signaux simulés. Dans le cas d'un système nécessitant de longues opérations de câblage, il n'est souvent pas possible de terminer le câblage avant l'exécution des tests de clôture. Dans ces cas-là, pour être prudent, les tests devraient être effectués après qu'une sélection représentative de tous les différents types de branchement sur le système a été faite. De cette manière, tout problème générique avec les interfaces sera facilement identifié et pourra être efficacement résolu. Les tests finaux devraient être effectués avec un système entièrement câblé. À ce stade, le système peut être mis en service et prouver qu'il fonctionne comme prévu. Les

systèmes CCI devraient, dans la mesure du possible, être mis en service et fonctionner avant que d'autres activités de mise en service, exigeant le fonctionnement du système CCI, soient menées.

MISES À NIVEAU ET MISES EN CONFORMITÉ

7.19. Pour garantir que les centrales nucléaires continuent à fournir une énergie fiable et satisfont aux normes de sûreté en vigueur, les systèmes CCI devraient être périodiquement modernisés. L'industrie nucléaire s'est trouvée confrontée à des problèmes d'approvisionnement de pièces de rechange pour des systèmes CCI analogiques dont le matériel avait été conçu et fabriqué il y a 20–30 ans. Le vieillissement physique des équipements combiné au manque de pièces de rechange a accru les taux de défaillance et les coûts de fonctionnement et de maintenance. De plus, un certain nombre de fournisseurs ont réduit leur assistance pour les systèmes analogiques et, dans certains cas, le fournisseur d'origine n'est plus en activité. Du fait des améliorations considérables de la fiabilité de l'électronique numérique ces dernières années, de nombreuses installations nucléaires ont décidé de remplacer les anciens systèmes analogiques CCI par des systèmes programmés.

7.20. Les avancées de la technologie numérique donnent ces autres éléments de motivation pour les mises à niveau:

— possibilité d'exécution de fonctions plus complexes;
— obtention d'une plus grande précision;
— compilation et utilisation d'un plus gros volume et d'une plus grande variété d'informations;
— possibilité de rendre l'interface utilisateur plus flexible;
— il est plus facile pour le système de détecter et de traiter les défaillances internes prévues;
— possibilité d'apporter des modifications fonctionnelles sans modification matérielle ou même accès physique;
— possibilité d'utiliser des processeurs normalisés de fiabilité connue dans de nombreuses applications.

7.21. Lorsqu'un système CCI programmé fait partie d'une amélioration ou d'une mise à niveau, sa fonction en ce qui concerne la sûreté de la centrale nucléaire devrait être prise en considération. Le classement de sûreté d'un système CCI devrait être établi selon les critères donnés dans la section 2. Les exigences

concernant la fiabilité, la qualification et l'assurance de la qualité du système et les autres exigences seront définies en fonction du classement de sûreté.

7.22. Pour des raisons de commodité, en premier lieu, une spécification du système existant complétée par une spécification des exigences relatives au nouveau système ou au système modifié devraient être rédigée. La documentation technique du système analogique existant peut être incomplète et manquer de précision. La mise en œuvre d'une 'rétroingénierie' pour rétablir les exigences et les spécifications de conception en partant de la mise en œuvre de la conception peut être nécessaire.

7.23. Les avantages que procurent les modifications de l'interface opérateur et/ou des stratégies de contrôle-commande devraient être comparés avec les coûts potentiels. Les améliorations apportées à l'interface opérateur peuvent nécessiter une modification complète des panneaux de commande et un recyclage des opérateurs et du personnel de maintenance. De plus, les opérateurs de la salle de commande devraient être consultés avant la sélection d'une interface opérateur et ils devraient également fournir le retour d'expérience à l'équipe de conception lors des différentes phases du processus de développement.

7.24. Des informations détaillées sur les mises à niveau des systèmes CCI sont fournies dans les références [15, 16].

ANALYSES EXIGÉES POUR LES SYSTÈMES DE SÛRETÉ

Analyses de défaillance

7.25. Des analyses devraient être effectuées à des stades appropriés du processus de conception des systèmes de sûreté pour vérifier que la combinaison des sous-systèmes principaux (le système de protection, les systèmes de commande de sûreté et les fonctions support des systèmes de sûreté) peut satisfaire, à tout moment, aux recommandations du présent guide de sûreté concernant les défaillances uniques (voir section 4) et les défaillances de cause commune ainsi que toutes les autres exigences relatives à la fiabilité des systèmes de sûreté. Elles devraient inclure des analyses de mode de défaillance pour confirmer les affirmations faites sur la conception à position de repli sécurisée. Ces analyses devraient être documentées.

Évaluation des dispositions de test

7.26. Une évaluation de la conception finale devrait être faite pour vérifier l'adéquation des dispositions prises pour le test du système de protection, des systèmes de commande de sûreté et des fonctions support du système de sûreté. Les résultats de cette évaluation devraient être documentés; les domaines de la conception qui sont sensibles à la défaillance des équipements ou à l'erreur humaine de quelque manière que ce soit lors du test du système ou du test des équipements devraient être identifiés dans les documents.

Analyse de fiabilité

7.27. Dans un État Membre où il a été décidé d'employer des exigences chiffrées pour la fiabilité des systèmes de sûreté ou des éléments de ces derniers, une analyse de fiabilité quantitative appropriée devrait être effectuée et utiliser des taux de défaillance des composants et des temps moyens de réparation démontrables, afin de:

— tenir compte des défaillances aléatoires des appareils;
— tenir compte des défaillances de cause commune, y compris les erreurs humaines;
— établir l'importance relative vis-à-vis de la fiabilité des différentes parties des systèmes de sûreté;
— établir les intervalles de test initiaux cohérents avec les taux de défaillance des composants applicables et avec les exigences de fiabilité;
— confirmer au cours de l'exploitation de la centrale que les informations obtenues en fonctionnement sur les taux de défaillance sont cohérentes avec les hypothèses faites et que les objectifs de fiabilité sont atteints;
— définir les actions à mener si les taux de défaillance dépassent les taux de défaillance de conception ou ne correspondent plus; par exemple, réduction ou augmentation de l'intervalle de test, ou remplacement des composants qui empêchent d'atteindre les objectifs de fiabilité.

7.28. Les résultats de cette analyse devraient être documentés ainsi que les résultats des tests périodiques, des évaluations de la fiabilité en service et de toute action correctrice prise.

ÉVALUATION PROBABILISTE DE SÛRETÉ

7.29. Les connaissances acquises grâce aux évaluations probabilistes de sûreté (EPS) devraient être prises en compte dans la conception avec comme objectif de garantir qu'aucune caractéristique spécifique ne contribue de manière disproportionnée ou incertaine au risque global. Des informations détaillées sur les EPS sont fournies dans les réf. [17–20].

HYPOTHÈSES FAITES DANS LES ANALYSES

7.30. Les hypothèses faites dans les analyses nécessaires à la vérification de la conception devraient être consignées dans les documents de ces analyses. Chaque hypothèse devrait être mentionnée et justifiée.

DOCUMENTATION RELATIVE AU SYSTÈME CCI

7.31. Le but de la documentation sur le système CCI est: (1) de procurer le moyen de communiquer les informations entre les différentes phases et les différentes parties impliquées dans le processus de conception; (2) de fournir un enregistrement montrant que les exigences ont été correctement interprétées et respectées pour le système installé; (3) de communiquer les informations liées à la conception et essentielles pour l'exploitation aux opérateurs de la centrale; et (4) de fournir une base pour la maintenance de la centrale et pour les futures révisions éventuelles de la conception.

7.32. Dans le cas d'un système CCI important pour la sûreté, un nombre important de documents sont élaborés lors des nombreuses activités associées au processus de conception. Pour garantir que la signification de ces documents est bien saisie, ils devraient être regroupés en fonction de leurs rôles dans le processus de conception.

7.33. Les documents primaires sont les documents qui font partie intégrante du processus de conception et qui constituent les documents d'entrée et de sortie de chacune des phases. Une faute dans ces documents peut conduire directement à un défaut dans le système lui-même. Les documents primaires incluent normalement les documents de dimensionnement servant à l'analyse de sûreté de la centrale, les documents regroupant les exigences relatives aux systèmes de sûreté, les diagrammes logiques et les plans de l'ouvrage tel que réalisé.

7.34. Les documents secondaires sont des documents qui sont associés au processus de conception et qui sont utilisés par le concepteur pour préparer les documents d'entrée et de sortie. Une faute dans ces documents ne conduira pas directement à un défaut dans le système, mais ils peuvent masquer la présence d'un défaut du fait d'une mauvaise communication des informations, et suivre une indication erronée du document pourrait introduire un défaut dans le système. Généralement, les documents secondaires définissent et consignent les activités associées au processus de conception, comme les activités de vérification et de validation entre les phases. Les enregistrements de vérification et de validation sont utilisés pour déterminer la nécessité d'une modification des documents des phases correspondantes lorsque des fautes sont trouvées.

7.35. D'autres documents dans les programmes d'assurance de la qualité, la planification de projet et la qualification des équipements viennent étayer le processus de conception. Ces documents justificatifs contribuent aux décisions organisationnelles, logistiques et stratégiques à prendre pour le processus de conception, qui peuvent avoir un effet indirect sur la conception.

7.36. La conception d'un système CCI important pour la sûreté devrait être complètement documentée au moment où elle est terminée. La documentation devrait être compréhensible, complète, vérifiable et permettre la traçabilité afin de prouver que le système répond aux exigences de fonctionnalité et de sûreté de fonctionnement. Une documentation adéquate facilitera la modification ou la modernisation future du système.

7.37. Au moment de l'achèvement de la conception du système CCI, la documentation de conception finale devrait inclure la liste des documents correspondants de conception, vérification de la conception et validation de la conception, et devrait contenir des références spécifiques à ces documents.

7.38. La documentation du système CCI devrait être tenue à jour et toute modification du système devrait être répercutée dans la documentation. Toutes les évolutions des documents relatifs au système CCI devraient se faire dans le cadre d'un contrôle de la configuration.

Codes et normes

7.39. La liste des guides, codes et normes qui s'appliquent à la conception d'un système CCI important pour la sûreté ainsi que les indicateurs de conformité associés devraient faire l'objet d'un accord au début du projet et devraient être

documentés et communiqués à l'organisme responsable du projet au cours du projet.

Documentation relative au dimensionnement

7.40. Le dimensionnement final devrait être documenté. Ceci devrait inclure au minimum l'identification et la documentation sur:

— les états d'exploitation de la centrale où le système doit être exploité;
— les EIP, avec une identification des actions de protection et de sûreté correspondantes des systèmes CCI, accompagnés des conditions initiales de l'EIP et des limites admissibles des conditions de la centrale pour chaque événement de ce type;
— les variables ou les combinaisons de variables qui doivent être surveillées pour commander chaque action protectrice, soit manuellement soit automatiquement (ou les deux);
— les plages et les vitesses de variation de ces variables ou combinaisons de variables qui devraient être prises en charge par les systèmes CCI importants pour la sûreté;
— les valeurs extrêmes de déclenchement des systèmes de sûreté de chacune de ces variables pour chaque mode de fonctionnement applicable de la centrale;
— les contraintes imposées au système de contrôle-commande en ce qui concerne les valeurs admissibles pour les variables de fonctionnement et autres paramètres importants.

7.41. Les points critiques (en ce qui concerne le temps ou les conditions de la centrale) qui régissent les actions du système après l'apparition d'un événement pris en compte à la conception devraient être documentés et inclure:

— le moment ou les conditions de la centrale pour lesquelles les fonctions de sûreté doivent être initiées;
— le moment ou les conditions de la centrale pour lesquelles le contrôle automatique des fonctions de sûreté doit être mis en œuvre;
— le moment ou les conditions de la centrale pour lesquelles l'on considère que la fonction de sûreté a rempli correctement sa mission;
— le moment ou les conditions de la centrale pour lesquelles le retour d'un système de sûreté à son état normal d'attente peut être effectué.

7.42. Les méthodes à utiliser pour déterminer que la fiabilité de la conception d'un système de sûreté convient pour chaque fonction du système de sûreté et

tout objectif qualitatif ou quantitatif de fiabilité qui peut être imposé à la conception du système devraient être consignés dans un document.

7.43. Toutes les contraintes liées à la bande passante (comme les cadences de scrutation et les vitesses de transmission des données) influant sur la conception du système devraient être documentées.

7.44. Pour chaque action de protection identifiée dont la réalisation peut être commandée manuellement dès le début ou après l'initiation, les éléments suivants devraient être consignés dans les documents:

— le moment ou les conditions de la centrale pour lesquelles la commande manuelle est autorisée;
— la justification de l'autorisation de déclenchement, ou du contrôle après déclenchement, à l'aide de moyens manuels exclusivement;
— la plage des conditions environnementales imposées à l'opérateur lors des états d'exploitation de la centrale et des conditions accidentelles dans lesquelles les opérations manuelles doivent être effectuées;
— les variables, comme mentionné précédemment, qui doivent être affichées afin que l'opérateur puisse les prendre en compte pour décider d'une action manuelle.

7.45. La plage des conditions transitoires et stabilisées (comme la tension et la fréquence) des fonctions support du système de sûreté devrait être identifiée et documentée pour les états d'exploitation et les conditions accidentelles de la centrale où les systèmes importants pour la sûreté doivent fonctionner.

7.46. La plage des conditions environnementales transitoires et stabilisées (comme les conditions de rayonnement, température, humidité, pression et vibration) dans lesquelles les systèmes importants pour la sûreté doivent fonctionner devrait être documentée pour les états d'exploitation et les conditions accidentelles de la centrale ainsi que pour les événements externes.

7.47. Les conditions pouvant potentiellement dégrader les fonctions des systèmes de sûreté et pour lesquelles des dispositions ont été prises pour conserver la capacité à remplir les fonctions de sûreté (par exemple, impact de missile, rupture d'une conduite, incendie, arrêt de la ventilation, mise en route intempestive des systèmes d'extinction des incendies, erreur de l'opérateur, défaillance dans des systèmes de classe de sûreté différente) devraient être documentées.

7.48. Les conditions de la centrale pour lesquelles le bipasse des actions de sûreté est autorisé devraient être identifiées. Les moyens servant à activer ces bipasses autorisés, accompagnés des indicateurs essentiels, devraient également être décrits.

7.49. Les procédures de spécification et de conception technique qui doivent être respectées pour les systèmes et les composants devraient être documentées.

Documents concernant la conception des systèmes CCI

7.50. La conception des systèmes CCI importants pour la sûreté devrait être documentée. Ces documents devraient comporter, au minimum, les informations suivantes:

Fonction

7.51. Chaque système CCI devrait être classé, comme spécifié dans la section 2.

7.52. Le dimensionnement de chaque système devrait être documenté et inclure ses fonctions liées à la sûreté, les interfaces avec les autres systèmes ainsi que les EIP et les conditions de la centrale auxquels s'appliquent les fonctions liées à la sûreté.

7.53. Les fonctions remplies par chaque voie CCI devraient être documentées. Cette documentation inclut les documents relatifs aux indicateurs, aux caractéristiques des alarmes et des commandes, et, le cas échéant, aux marges de stabilité.

7.54. Pour les actions de protection, une description précise et claire des conditions de la centrale et des indicateurs de ces conditions, qui définissent l'achèvement des actions de protection, devrait être consignée dans les documents.

Performances

7.55. La description de la plage, de l'exactitude et du temps de réponse du système global et de chaque voie devrait être fournie.

7.56. Des documents prouvant la qualification, les performances fonctionnelles et toute autre exigence spécifique du système et de ses composants devraient être fournis.

7.57. La liste des équipements présents dans le système CCI important pour la sûreté dont les performances peuvent ne pas satisfaire aux exigences du système pendant toute la durée de vie utile de la centrale, comportant les critères déterminant la fin de vie utile des équipements et leur durée de vie prévue, devrait faire partie de la documentation.

7.58. Pour les systèmes de sûreté (c'est-à-dire, le système de protection, le système de commande de sûreté et les fonctions support du système de sûreté), il faudrait indiquer le temps maximum imparti et le temps prévu pour accomplir les fonctions de sûreté nécessaires.

7.59. La description des analyses du système de sûreté identifiées dans les par. 7.25–7.28 devrait être faite et comporter des références aux documents de conception correspondants.

Qualification

7.60. Il faudrait indiquer les conditions environnementales dans lesquelles chaque composant doit fonctionner, y compris les conditions normales, les incidents de fonctionnement prévus et les conditions accidentelles de dimensionnement.

7.61. L' (ou les) alimentation(s) électrique(s) qui servira (serviront) à faire fonctionner chaque système dans des conditions normales, lors d'incidents d'exploitation prévus et dans des conditions accidentelles de dimensionnement devrai(en)t être identifiée(s).

7.62. Les documents relatifs à la vérification des exigences de qualification de chaque composant ou système devraient être fournis.

Test et maintenance

7.63. Un calendrier de test, d'inspection et de maintenance périodique, destiné à garantir la disponibilité nécessaire des appareils, devrait être spécifié.

7.64. Les exigences se rapportant au test, à la maintenance et à l'inspection devraient être spécifiées et accompagnées des défaillances, risques ou dégradations pouvant résulter de ces activités.

Fonctionnement

7.65. Les principes de fonctionnement du système pour tous les états d'exploitation devraient être décrits. La description devrait spécifier les signaux correspondants et les actions automatiques nécessaires ou les actions que l'opérateur doit mettre en œuvre.

7.66. Les notices d'exploitation et de maintenance devraient être fournies.

Procédures et instructions

7.67. Les instructions d'exploitation, de mise en service et de maintenance se rapportant au système devraient être référencées.

Pièces de rechange

7.68. Les spécifications techniques d'achat devraient être disponibles pour chaque composant.

7.69. Pour maintenir les bases de conception dans l'avenir, les critères et les raisons de sélection des pièces de rechange devraient être documentés.

7.70. Les exigences relatives à la documentation de l'assurance de la qualité énoncées dans les normes de sûreté de l'AIEA concernant l'assurance de la qualité devraient être respectées. (Pour plus d'informations, se reporter à la réf. [3], guides de sûreté Q3 et Q10).

Organisation de la documentation

7.71. La documentation devrait respecter une structure semblable à celle indiquée ci-dessous:

— les fonctions fournies par le système et sa conception fonctionnelle;
— les caractéristiques de la conception du système;
— les installations de test, de diagnostic et de maintenance du système et leur fonctionnement;
— la documentation des résultats de test;
— la qualification des équipements;
— le processus de conception et les exigences de qualité suivies pour la conception;
— les stratégies de maintenance;

— les stratégies de mise en service;
— les méthodes de vérification et de validation de la conception;
— l'exploitation du système;
— les programmes de maintenance, surveillance et test périodique;
— la fourniture des pièces et/ou composants de rechange.

Documentation relative au système CCI de sûreté

7.72. Lorsque la conception du système CCI de sûreté est terminée, les performances fonctionnelles prévues et la fiabilité du système devraient être documentées. Ces documents devraient comporter, au minimum, les informations suivantes:

— Une brève description du dimensionnement, les raisons ayant conduit aux modifications de conception comprenant les données issues de l'examen de l'expérience d'exploitation (le cas échéant), la conception fonctionnelle du système et les éléments ayant motivé ce choix spécifique pour la conception.
— Une description complète du système, qui devrait inclure les informations concernant toutes les variables surveillées (variables de fonctionnement, signaux opérateur) et toutes les variables contrôlées (sorties vers les actionneurs et les indicateurs) pour tous les modes de fonctionnement du système. Cette description devrait également inclure les méthodes d'affichage des données (par exemple, câblées ou informatisées).
— Les détails relatifs à toute dépendance des caractéristiques de fonctionnement des systèmes en interface, des systèmes de commande de sûreté, des autres systèmes liés à la sûreté ou des systèmes support de sûreté, y compris l'alimentation électrique.
— Les variables ou combinaisons de variables et les méthodes de combinaison utilisées qui doivent être surveillées pour décider des actions protectrices à mettre en œuvre. Les informations à fournir devraient inclure le nombre minimum et les emplacements des capteurs nécessaires pour surveiller convenablement toutes les variables importantes pour la sûreté, y compris celles qui ont une dépendance spatiale (c'est-à-dire dont la valeur mesurée varie en fonction de la position dans une zone particulière, comme par exemple le flux de neutrons). Les plages calculées et les vitesses de variation des variables ou des combinaisons de variables mentionnées précédemment devraient être spécifiées.
— Le nombre de voies CCI, leurs fonctions et leur logique d'entrée–sortie, ainsi que les informations sur les caractéristiques des indicateurs, alarmes et commandes, y compris les marges de sûreté, résultats et stabilité.

— La description du système devrait inclure les emplacements (par exemple, coordonnées x,y,z sur le plan de la centrale, numéro de salle ou numéro de la zone) des capteurs, armoires, coffrets, panneaux, commandes opérateur ou affichages opérateur ainsi que ceux des installations de réglage manuel et de test du système.
— Les EIP, accompagnés des actions correspondantes de protection et de sûreté.
— Les variables, ou combinaisons de variables, qui doivent être surveillées pour mettre en œuvre des actions protectrices pour chaque événement pris en compte à la conception.
— Les seuils pour chaque variable listée, pour chaque mode de fonctionnement applicable de la centrale, incluant toutes les conditions de bipasse pour l'exploitation et la maintenance et la tolérance d'erreur d'étalonnage des instruments. La marge entre les paramètres du système de sûreté et le niveau adopté pour signaler l'apparition de conditions dangereuses devrait être identifiée et accompagnée des informations appropriées pour l'interprétation.
— Les temps de réponse maximums autorisés pour les systèmes de sûreté nécessaires pour accomplir toutes les actions de protection et de sûreté.
— Les critères de fiabilité pour chaque action de protection.
— Les conditions qui, une fois atteintes, définissent l'achèvement d'une action de protection.
— Les seuils nominaux du système de sûreté pour chaque variable ou combinaison de variables.
— La plage, la durée de vie et l'exactitude prévue de chaque élément des équipements du système de sûreté.
— Les analyses de conception identifiées dans les par. 7.25–7.28.
— La documentation attestant les exigences de qualification et de performances fonctionnelles ainsi que toute autre exigence spécifique relative aux équipements du système de sûreté.
— La liste des équipements du système de sûreté dont les performances peuvent ne pas satisfaire aux exigences fonctionnelles du système pendant toute la vie utile de la centrale. Les critères servant à déterminer la fin de vie des appareils et la durée de vie prévue devraient être précisés.
— La liste des codes et normes applicables à la conception du système de sûreté.
— Les conditions de la centrale pour lesquelles le bipasse des actions de sûreté identifiées est autorisé (pour les conditions d'autorisation applicables, voir par. 5.36–5.38).

RÉFÉRENCES

[1] AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE, Sûreté des centrales nucléaires : conception, collection Normes de sûreté n° NS-R-1, AIEA, Vienne (à paraître).

[2] AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE, Logiciels destinés aux systèmes programmés importants pour la sûreté des centrales nucléaires, collection Normes de sûreté n° NS-G-1.1, AIEA, Vienne (2004).

[3] AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE, L'assurance de la qualité pour la sûreté des centrales nucléaires et autres installations nucléaires, code et guides de sûreté Q1–Q14, collection Sécurité n° 50-C/SG-Q, AIEA, Vienne (1999).

[4] INTERNATIONAL ATOMIC ENERGY AGENCY, Modern Instrumentation and Control for Nuclear Power Plants: A Guidebook, Technical Reports Series No. 387, IAEA, Vienna (1999).

[5] INTERNATIONAL ATOMIC ENERGY AGENCY, Application of the Single Failure Criterion, Safety Series No. 50-P-1, IAEA, Vienna (1990).

[6] AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE, Protection contre l'incendie dans les centrales nucléaires, collection Sécurité n° 50-SG-D2 (Rev. 1), AIEA, Vienne (1997).

[7] AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE, Protection des centrales nucléaires contre les projectiles d'origine interne et leurs effets secondaires, collection Sécurité n° 50-SG-D4, AIEA, Vienne (1981).

[8] AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE, Agressions externes dues aux activités humaines et conception des centrales nucléaires, collection Sécurité n° 50-SG-D5 (Rev. 1), AIEA, Vienne (1997).

[9] AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE, Source froide ultime et systèmes de transport de la chaleur directement associés pour les centrales nucléaires, collection Sécurité n° 50-SG-D6, AIEA, Vienne (1982).

[10] INTERNATIONAL ATOMIC ENERGY AGENCY, Equipment Qualification in Operational Nuclear Power Plants: Upgrading, Preserving and Reviewing, Safety Reports Series No. 3, IAEA, Vienna (1998).

[11] AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE, Systèmes d'énergie de secours dans les centrales nucléaires, collection Sécurité n° 50-SG-D7 (Rev. 1), AIEA, Vienne (1993).

[12] AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE, Conception de la protection radiologqique dans les centrales nucléaires, collection Sécurité n° 50-SG-D9, AIEA, Vienne (1987).

[13] INTERNATIONAL ATOMIC ENERGY AGENCY, Preparedness and Response for a Nuclear or Radiological Emergency, Safety Standards Series No. GS-R-2, IAEA, Vienna (2002).

[14] AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE, Conception et homologation des constituants des centrales nucléaires du point de vue sismique, collection Sécurité n° 50-SG-D15, AIEA, Vienne (1997).

[15] INTERNATIONAL ATOMIC ENERGY AGENCY, Modernization of Instrumentation and Control in Nuclear Power Plants, IAEA-TECDOC-1016, IAEA, Vienna (1998).
[16] INTERNATIONAL ATOMIC ENERGY AGENCY, Specifications of Requirements for Upgrades Using Digital Instrumentation and Control Systems, IAEA-TECDOC-1066, IAEA, Vienna (1999).
[17] INTERNATIONAL ATOMIC ENERGY AGENCY, Treatment of External Hazards in Probabilistic Safety Assessment for Nuclear Power Plants, Safety Series No. 50-P-7, IAEA, Vienna (1995).
[18] INTERNATIONAL ATOMIC ENERGY AGENCY, Procedures for Conducting Probabilistic Safety Assessments of Nuclear Power Plants (Level 2): Accident Progression, Containment Analysis and Estimation of Accident Source Terms, Safety Series No. 50-P-8, IAEA, Vienna (1995).
[19] INTERNATIONAL ATOMIC ENERGY AGENCY, Human Reliability Analysis in Probabilistic Safety Assessment for Nuclear Power Plants, Safety Series No. 50-P-10, IAEA, Vienna (1995).
[20] INTERNATIONAL ATOMIC ENERGY AGENCY, Procedures for Conducting Probabilistic Safety Assessments of Nuclear Power Plants (Level 3): Off-Site Consequences and Estimation of Risks to the Public, Safety Series No. 50-P-12, IAEA, Vienna (1996).

GLOSSAIRE

Les définitions suivantes s'appliquent aux fins de la présente publication.

accident de dimensionnement. Conditions accidentelles pour lesquelles une centrale nucléaire est conçue en fonction de critères de conception établis et pour lesquelles l'endommagement du cœur et le rejet de matières radioactives sont maintenus dans des limites autorisées.

action de protection. Génération des actions protectrices nécessaires pour garantir que l'action de protection exigée par un événement initiateur postulé est accomplie.

action de sûreté. Action unique mise en œuvre par un actionneur de sûreté[4].

actionneur. Composant qui commande directement l'énergie motrice pour les équipements actionnés. Les actionneurs incluent par exemple les disjoncteurs et les relais qui commandent la distribution et l'utilisation de l'alimentation électrique et les commandes de vannes contrôlant les fluides hydrauliques ou pneumatiques.

action protectrice. Action du système de protection commandant le fonctionnement d'un actionneur de sûreté spécifique.

appareils commandés. Composant comme une pompe ou une vanne actionné par un dispositif moteur.

assurance de la qualité. Mesures programmées et systématiques nécessaires pour fournir une confiance appropriée qu'un élément, processus ou service satisfera aux exigences de qualité, par exemple celles spécifiées dans l'autorisation d'exploitation.

bipasse. Mécanisme servant à inhiber, volontairement mais provisoirement, le fonctionnement d'un circuit ou d'un système en, par exemple, court-circuitant les contacts d'un relais.

coïncidence. Une caractéristique de conception du système de protection qui fait que deux ou plusieurs signaux se recouvrant ou simultanés provenant de plusieurs voies sont nécessaires pour que la logique produise un signal déclenchant une action protectrice.

composant. Élément discret d'un système. Ce sont par exemple les fils, les transistors, les circuits intégrés, les moteurs, les relais, les solénoïdes, les conduites, les garnitures, les pompes, les réservoirs et les vannes.

---

[4] Par exemple, insertion d'une barre de contrôle, fermeture des vannes du confinement ou mise en route des pompes d'injection de sécurité.

conditions accidentelles. Écarts par rapport au fonctionnement normal plus graves que les incidents de fonctionnement prévus, incluant les accidents de dimensionnement et les accidents graves.

contrôle qualité. Partie de l'assurance de la qualité destinée à vérifier que les structures, systèmes et composants correspondent aux exigences prédéfinies.

cycle de vie du système. Tous les stades par lesquels passe un système, depuis sa conception jusqu'à sa mise au rebut finale.

défaillance de cause commune. Défaillance de deux ou plusieurs structures, systèmes ou composants due à un événement ou une cause spécifique unique.

défaillance unique. Défaillance résultant de l'incapacité d'un composant à remplir sa ou ses fonctions de sûreté prévues et toute défaillance consécutive qui en résulte.

disponibilité. Proportion de temps pendant lequel un système est capable de remplir sa tâche prévue.

dispositif moteur. Composant tel qu'un moteur, une commande par électro-aimant ou une commande pneumatique qui convertit une énergie en action lorsqu'il est commandé par un actionneur.

dispositifs support du système de sûreté. Ensemble d'équipements qui fournissent des services, comme le refroidissement, la lubrification et l'approvisionnement en énergie, demandés par le système de protection et les systèmes actionneurs de sûreté[5].

diversité. Présence de deux ou plus de deux systèmes ou composants redondants pour effectuer une fonction définie, les différents systèmes ou composants ayant des attributs différents de façon à réduire la possibilité d'une défaillance d'origine commune.

élément important pour la sûreté. Élément qui fait partie d'un groupe de sûreté et/ou dont le dysfonctionnement ou la panne peut conduire à une exposition aux rayonnements du personnel sur le site ou des personnes du public.

équipement actionné. Ensemble composé de dispositifs moteurs et d'équipements commandés utilisé pour accomplir une ou plusieurs actions de sûreté.

---

[5] À la suite d'un événement initiateur postulé, certains dispositifs support du système de sûreté peuvent être déclenchés par le système de protection et d'autres peuvent être déclenchés par les systèmes de commande de sûreté; d'autres dispositifs support du système de sûreté nécessaires peuvent ne pas avoir besoin d'être déclenchés s'ils fonctionnent au moment où se produit l'événement initiateur postulé.

états d'exploitation. États définis lors d'un fonctionnement normal et lors d'incidents d'exploitation prévus.

événement initiateur postulé Événement identifié au cours de la conception comme étant capable de conduire à des incidents de fonctionnement prévus ou à des conditions accidentelles.

fiabilité. Probabilité pour un système de satisfaire aux exigences minimales de performance lorsqu'il sera appelé à le faire.

fonction de sûreté. Mission spécifique qui doit être accomplie pour la sûreté.

fonctionnement normal. Fonctionnement à l'intérieur de limites et de conditions d'exploitation spécifiées.

groupe de sûreté. Assemblage d'équipements désignés pour exécuter toutes les actions nécessaires dans le cas d'un événement initiateur postulé afin de garantir que les limites spécifiées dans le dimensionnement pour les incidents de fonctionnement prévus et les accidents de dimensionnement ne sont pas dépassées.

incidents d'exploitation prévus. Processus d'exploitation s'écartant du fonctionnement normal et censé se produire au moins une fois au cours de la durée d'exploitation d'une installation mais qui, grâce à des dispositions de conception appropriées, ne cause aucun dommage important aux éléments importants pour la sûreté ou ne conduit pas à des conditions accidentelles.

inhibition d'entretien. Bipasse d'un équipement du système de sûreté lors d'un entretien, d'un test ou d'une réparation.

inhibition d'exploitation. Bipasse de certaines actions de protection lorsqu'elles ne sont pas nécessaires au cours d'un mode spécifique de fonctionnement de la centrale.

isolement fonctionnel. Prévention des influences dues au mode de fonctionnement ou à une défaillance d'un circuit ou d'un système sur un autre.

limites de sûreté. Limites des paramètres de fonctionnement à l'intérieur desquelles il a été prouvé qu'une installation agréée est sûre.

logique. Génération d'un signal de sortie tout ou rien approprié à partir d'un certain nombre de signaux d'entrée tout ou rien en fonction de règles prédéterminées, ou équipement servant à générer ce signal.

mission de sûreté. Détection d'une ou de plusieurs variables représentatives d'un événement initiateur postulé, traitement du signal, déclenchement et exécution des actions de sûreté nécessaires pour éviter que les limites spécifiées dans le dimensionnement soient dépassées et déclenchement et exécution de certains services fournis par les dispositifs auxiliaires du système de sûreté.

multiplexage. Transmission et réception de deux ou plusieurs signaux ou messages le long d'un canal de transmission de données unique, à l'aide

par exemple de techniques de répartition dans le temps, répartition en fréquence ou codage des impulsions.

redondance. La mise en place de structures de remplacement (identiques ou différentes), systèmes ou composants, afin qu'un élément quelconque puisse remplir la fonction requise indépendamment de l'état de fonctionnement ou de défaillance d'un autre élément.

séparation physique. Séparation obtenue grâce à l'implantation (distance, orientation), à des barrières appropriées ou une combinaison de ces éléments.

sûreté de fonctionnement. Terme général décrivant la fiabilité globale d'un système, c'est-à-dire le degré de confiance que l'on peut raisonnablement accorder à ce système. La fiabilité, la disponibilité et la sûreté sont des attributs de la sûreté de fonctionnement.

sûreté nucléaire. L'obtention de conditions correctes de fonctionnement, de prévention des accidents ou de limitation des conséquences d'un accident, entraînant la protection des travailleurs, du public et de l'environnement contre des risques exagérés de rayonnement.

système d'instrumentation et de contrôle-commande (CCI) lié à la sûreté. Système CCI important pour la sûreté qui ne fait pas partie d'un système de sûreté.

système de commande de sûreté. Ensemble d'équipements déclenchés par le système de protection pour accomplir les actions de sûreté nécessaires.

système de protection. Système qui surveille le fonctionnement d'un réacteur et qui, lorsqu'il détecte une anomalie, déclenche automatiquement des actions pour éviter une condition non sûre ou potentiellement non sûre.

système de sûreté. Système important pour la sûreté, mis en place pour garantir un arrêt sûr du réacteur ou l'évacuation de la chaleur résiduelle du cœur du réacteur ou pour limiter les conséquences des incidents de fonctionnement prévus et des accidents de dimensionnement.

temps de réponse. Temps mis par un composant à atteindre un état de sortie donné à compter du moment où il reçoit un signal lui imposant de prendre cet état de sortie.

validation. Processus visant à déterminer si un produit ou un service est capable de remplir sa fonction prévue de manière satisfaisante. Par exemple, dans le cas d'un système tel qu'un système CCI, le processus qui sert à confirmer que la totalité du système (matériel et logiciel) se conforme à toutes les exigences (fonctionnelles et autres) et ne présente pas de comportement non prévu.

vérification. Processus visant à déterminer si la qualité ou les performances d'un produit ou d'un service sont conformes à celles indiquées, voulues ou nécessaires. Par exemple, pour un processus de développement, le fait de

s'assurer qu'une phase particulière du processus de développement satisfait aux exigences qui lui sont imposées par la phase précédente.

voie. Ensemble de composants interconnectés qui, au sein d'un système, déclenche une sortie unique. Un circuit perd son identité lorsque des signaux de sortie uniques sont combinés avec des signaux provenant d'autres circuits, par exemple d'un circuit de surveillance ou d'un circuit de déclenchement de sûreté.

PERSONNES AYANT COLLABORÉ À LA RÉDACTION ET À L'EXAMEN

Anani, N.	Énergie atomique du Canada limitée (Canada)
Bock, H.W.	Siemens (Allemagne)
Duong, M.	Agence internationale de l'énergie atomique
Faya, A.	Énergie atomique du Canada limitée (Canada)
Hughes, P.J.	Service d'inspection des installations nucléaires (Royaume-Uni)
Johnson, G.L.	Laboratoire national Lawrence de Livermore (États-Unis d'Amérique)
MacBeth, M.	Énergie atomique du Canada limitée (Canada)
Pachner, J.	Agence internationale de l'énergie atomique
Pauksens, J.	Énergie atomique du Canada limitée (Canada)
Rollinger, F.	Institut de protection et de sûreté nucléaire (France)

ORGANES D'APPROBATION DES NORMES DE SÛRETÉ

Comité des normes de sûreté nucléaire

Allemagne: Wendling, R.D.; *Argentine:* Sajaroff, P.; *Belgique:* Govaerts, P. (Président); *Brésil:* Salati de Almeida, I.P.; *Canada:* Malek, I.; *Chine:* Zhao, Y.; *Espagne:* Mellado, I.; *États-Unis d'Amérique:* Murphy, J.; *Fédération de Russie:* Baklushin, R.P.; *France:* Saint Raymond, P.; *Inde:* Venkat Raj, V.; *Italie:* Del Nero, G.; *Japon:* Hirano, M.; *Mexique:* Delgado Guardado, J.L.; *Pakistan:* Hashimi, J.A.; *Pays-Bas:* de Munk, P.; *République de Corée:* Lee, J.-I.; *Royaume-Uni:* Hall, A.; *Suède:* Jende, E.; *Suisse:* Aberli, W.; *Ukraine:* Mikolaichuk, O.; *Agence de l'OCDE pour l'énergie nucléaire:* Royen, J.; *AIEA:* Hughes, P. (coordonnateur); *Commission européenne:* Gómez-Gómez, J.A.; *Organisation internationale de normalisation:* d'Ardenne, W.

Commission des normes de sûreté

Allemagne: Renneberg, W., Wendling, R.D.; *Argentine:* D'Amato, E.; *Brésil:* Caubit da Silva, A.; *Canada:* Bishop, A., Duncan, R.M.; *Chine:* Zhao, C.; *Espagne:* Martin Marquínez, A.; *États-Unis d'Amérique:* Travers, W.D.; *Fédération de Russie:* Vishnevskiy, Y.G.; *France:* Lacoste, A.-C., Gauvain, J.; *Inde:* Sukhatme, S.P.; *Japon:* Suda, N.; *République de Corée:* Kim,S.-J.; *Royaume-Uni:* Williams, L.G. (président), Pape, R.; *Suède:* Holm, L.-E.; *Suisse:* Jeschki, W.; *Ukraine:* Smyshlayaev, O.Y.; *Agence de l'OCDE pour l'énergie nucléaire:* Shimomura,K.; *AIEA:* Karbassioun, A. (coordonnateur); *Commission internationale de protection radiologique:* Clarke, R.H.

ISBN 92–0–201305–5
ISSN 1020–5829