RAPPORT TECHNIQUE

TECHNICAL REPORT

CEI
IEC
TR 61838

Première édition
First edition
2001-02

Centrales nucléaires – Fonctions d'instrumentation et de contrôle-commande importants pour la sûreté – Utilisation des évaluations probabilistes de sûreté pour le classement

Nuclear power plants – Instrumentation and control functions important for safety– Use of probabilistic safety assessment for the classification

Numéro de référence
Reference number
CEI/IEC/TR 61838:2001

Numérotation des publications

Depuis le 1er janvier 1997, les publications de la CEI sont numérotées à partir de 60000. Ainsi, la CEI 34-1 devient la CEI 60034-1.

Editions consolidées

Les versions consolidées de certaines publications de la CEI incorporant les amendements sont disponibles. Par exemple, les numéros d'édition 1.0, 1.1 et 1.2 indiquent respectivement la publication de base, la publication de base incorporant l'amendement 1, et la publication de base incorporant les amendements 1 et 2.

Informations supplémentaires sur les publications de la CEI

Le contenu technique des publications de la CEI est constamment revu par la CEI afin qu'il reflète l'état actuel de la technique. Des renseignements relatifs à cette publication, y compris sa validité, sont disponibles dans le Catalogue des publications de la CEI (voir ci-dessous) en plus des nouvelles éditions, amendements et corrigenda. Des informations sur les sujets à l'étude et l'avancement des travaux entrepris par le comité d'études qui a élaboré cette publication, ainsi que la liste des publications parues, sont également disponibles par l'intermédiaire de:

- **Site web de la CEI (www.iec.ch)**
- **Catalogue des publications de la CEI**

  Le catalogue en ligne sur le site web de la CEI (www.iec.ch/catlg-f.htm) vous permet de faire des recherches en utilisant de nombreux critères, comprenant des recherches textuelles, par comité d'études ou date de publication. Des informations en ligne sont également disponibles sur les nouvelles publications, les publications remplacées ou retirées, ainsi que sur les corrigenda.
- **IEC Just Published**

  Ce résumé des dernières publications parues (www.iec.ch/JP.htm) est aussi disponible par courrier électronique. Veuillez prendre contact avec le Service client (voir ci-dessous) pour plus d'informations.
- **Service clients**

  Si vous avez des questions au sujet de cette publication ou avez besoin de renseignements supplémentaires, prenez contact avec le Service clients:

  Email: custserv@iec.ch
  Tél: +41 22 919 02 11
  Fax: +41 22 919 03 00

Publication numbering

As from 1 January 1997 all IEC publications are issued with a designation in the 60000 series. For example, IEC 34-1 is now referred to as IEC 60034-1.

Consolidated editions

The IEC is now publishing consolidated versions of its publications. For example, edition numbers 1.0, 1.1 and 1.2 refer, respectively, to the base publication, the base publication incorporating amendment 1 and the base publication incorporating amendments 1 and 2.

Further information on IEC publications

The technical content of IEC publications is kept under constant review by the IEC, thus ensuring that the content reflects current technology. Information relating to this publication, including its validity, is available in the IEC Catalogue of publications (see below) in addition to new editions, amendments and corrigenda. Information on the subjects under consideration and work in progress undertaken by the technical committee which has prepared this publication, as well as the list of publications issued, is also available from the following:

- **IEC Web Site (www.iec.ch)**
- **Catalogue of IEC publications**

  The on-line catalogue on the IEC web site (www.iec.ch/catlg-e.htm) enables you to search by a variety of criteria including text searches, technical committees and date of publication. On-line information is also available on recently issued publications, withdrawn and replaced publications, as well as corrigenda.
- **IEC Just Published**

  This summary of recently issued publications (www.iec.ch/JP.htm) is also available by email. Please contact the Customer Service Centre (see below) for further information.
- **Customer Service Centre**

  If you have any questions regarding this publication or need further assistance, please contact the Customer Service Centre:

  Email: custserv@iec.ch
  Tel: +41 22 919 02 11
  Fax: +41 22 919 03 00

.

RAPPORT TECHNIQUE

TECHNICAL REPORT

CEI
IEC
TR 61838

Première édition
First edition
2001-02

Centrales nucléaires – Fonctions d'instrumentation et de contrôle-commande importants pour la sûreté – Utilisation des évaluations probabilistes de sûreté pour le classement

Nuclear power plants – Instrumentation and control functions important for safety– Use of probabilistic safety assessment for the classification

International Electrotechnical Commission 3, rue de Varembé Geneva, Switzerland
Telefax: +41 22 919 0300 e-mail: inmail@iec.ch IEC web site http://www.iec.ch

Commission Electrotechnique Internationale
International Electrotechnical Commission
Международная Электротехническая Комиссия

CODE PRIX
PRICE CODE W

Pour prix, voir catalogue en vigueur
For price, see current catalogue

SOMMAIRE

Pages

CONTENTS

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

CENTRALES NUCLÉAIRES – FONCTIONS D'INSTRUMENTATION ET DE CONTRÔLE-COMMANDE IMPORTANTS POUR LA SÛRETÉ – UTILISATION DES ÉVALUATIONS PROBABILISTES DE SÛRETÉ POUR LE CLASSEMENT

AVANT-PROPOS

1) La CEI (Commission Électrotechnique Internationale) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de la CEI). La CEI a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. A cet effet, la CEI, entre autres activités, publie des Normes internationales. Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec la CEI, participent également aux travaux. La CEI collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
2) Les décisions ou accords officiels de la CEI concernant les questions techniques représentent, dans la mesure du possible un accord international sur les sujets étudiés, étant donné que les Comités nationaux intéressés sont représentés dans chaque comité d'études.
3) Les documents produits se présentent sous la forme de recommandations internationales. Ils sont publiés comme normes, spécifications techniques, rapports techniques, ou guides et agréés comme tels par les Comités nationaux.
4) Dans le but d'encourager l'unification internationale, les Comités nationaux de la CEI s'engagent à appliquer de façon transparente, dans toute la mesure possible, les Normes internationales de la CEI dans leurs normes nationales et régionales. Toute divergence entre la norme de la CEI et la norme nationale ou régionale correspondante doit être indiquée en termes clairs dans cette dernière.
5) La CEI n'a fixé aucune procédure concernant le marquage comme indication d'approbation et sa responsabilité n'est pas engagée quand un matériel est déclaré conforme à l'une de ses normes.
6) L'attention est attirée sur le fait que certains des éléments du présent rapport technique peuvent faire l'objet de droits de propriété intellectuelle ou de droits analogues. La CEI ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de propriété et de ne pas avoir signalé leur existence.

La tâche principale des comités d'études de la CEI est l'élaboration des Normes internationales. Toutefois, un comité d'études peut proposer la publication d'un rapport technique lorsqu'il a réuni des données de nature différente de celles qui sont normalement publiées comme Normes internationales, cela pouvant comprendre, par exemple, des informations sur l'état de la technique.

La CEI 61838, qui est un rapport technique, a été établie par le sous-comité 45A: Instrumentation des réacteurs, du comité d'études 45 de la CEI: Instrumentation nucléaire.

Le texte de ce rapport technique est issu des documents suivants:

Projet d'enquête	Rapport de vote
45A/363/CDV	45A/388/RVC

Le rapport de vote indiqué dans le tableau ci-dessus donne toute information sur le vote ayant abouti à l'approbation de ce rapport technique.

Cette publication a été rédigée selon les Directives ISO/CEI, Partie 3.

Ce document, purement informatif, ne doit pas être considéré comme une Norme internationale.

Les annexes A et B sont données uniquement à titre d'information.

INTERNATIONAL ELECTROTECHNICAL COMMISSION

NUCLEAR POWER PLANTS – INSTRUMENTATION AND CONTROL FUNCTIONS IMPORTANT FOR SAFETY – USE OF PROBABILISTIC SAFETY ASSESSMENT FOR THE CLASSIFICATION

FOREWORD

1) The IEC (International Electrotechnical Commission) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of the IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, the IEC publishes International Standards. Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. The IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
2) The formal decisions or agreements of the IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested National Committees.
3) The documents produced have the form of recommendations for international use and are published in the form of standards, technical specifications, technical reports, or guides and they are accepted by the National Committees in that sense.
4) In order to promote international unification, IEC National Committees undertake to apply IEC International Standards transparently to the maximum extent possible in their national and regional standards. Any divergence between the IEC Standard and the corresponding national or regional standard shall be clearly indicated in the latter.
5) The IEC provides no marking procedure to indicate its approval and cannot be rendered responsible for any equipment declared to be in conformity with one of its standards.
6) Attention is drawn to the possibility that some of the elements of this technical report may be the subject of patent rights. The IEC shall not be held responsible for identifying any or all such patent rights.

The main task of IEC technical committees is to prepare International Standards. However, a technical committee may propose the publication of a technical report when it has collected data of a different kind from that which is normally published as an International Standard, for example "state of the art".

IEC 61838, which is a technical report, has been prepared by subcommittee 45A: Reactor instrumentation, of IEC technical committee 45: Nuclear instrumentation.

The text of this technical report is based on the following documents:

Enquiry draft	Report on voting
45A/363/CDV	45A/388/RVC

Full information on the voting for the approval of this technical report can be found in the report on voting indicated in the above table.

This publication has been drafted in accordance with the ISO/IEC Directives, Part 3.

This document, which is purely informative, is not to be regarded as an International Standard.

Annexes A and B are given for information only.

Le comité a décidé que le contenu de cette publication ne sera pas modifié avant 2006. A cette date, la publication sera

- reconduite;
- supprimée;
- remplacée par une édition révisée, ou
- amendée.

The committee has decided that the contents of this publication will remain unchanged until 2006. At this date, the publication will be:

- reconfirmed;
- withdrawn;
- replaced by a revised edition, or
- amended.

INTRODUCTION

La CEI 61226 «Centrales nucléaires – Systèmes d'instrumentation et de contrôle-commande importants pour la sûreté – classification» – a été publiée en 1993. La nécessité de classer les fonctions d'instrumentation et de contrôle-commande concernant les centrales nucléaires émane d'une recommandation de l'Agence Internationale de l'Energie Atomique (AIEA). La CEI 61226 insiste sur le fait que ce sont les **fonctions** qu'il faut classer à un stade précoce de la phase de conception afin que le degré d'importance au niveau de la sûreté de chaque fonction soit précisé. Au stade de la conception, les fonctions de contrôle-commande (CC) sont allouées à des systèmes d'instrumentation et de contrôle-commande spécifiques, dont chacun comprend normalement plusieurs types de matériels. Ces systèmes et matériels sont généralement attribués à des catégories d'importance de sûreté, mais ce sont les fonctions qui restent déterminantes pour la catégorisation.

Afin de pouvoir associer les systèmes et les matériels aux fonctions, le concept de FSE a été introduit dans la CEI 61226. Les FSE sont définis comme:

> Les fonctions et les systèmes et matériels associés. Les fonctions sont des actions qui sont effectuées dans un but ou pour atteindre un objectif. Les systèmes et matériels associés sont un assemblage de composants et les composants eux-mêmes qui sont employés pour remplir la fonction.

La CEI 61226 fournit une méthode de catégorisation des FSE basée sur des critères qualitatifs. Un grand nombre de ces critères sont courants dans l'industrie nucléaire dans la mesure où ils reconnaissent que la plus importante fonction de la sûreté nucléaire et la seule est de prévenir les accidents et d'en réduire les conséquences radiologiques. En conséquence, le classement des FSE au sens de la CEI 61226 est un processus déterministe qui ne prend pas en considération les techniques d'évaluation quantitative des risques .

Au cours des dix dernières années, les méthodes d'évaluation des risques, en particulier celles appliquées aux centrales nucléaires, se sont améliorées, bien que leur utilisation dans la conception des centrales nucléaires (ainsi qu'au niveau des demandes d'autorisation) soit très variable dans le monde. Dans certains pays, l'évaluation probabiliste des risques est considérée comme un élément essentiel du processus de conception et constitue l'acte final de sûreté; cela n'est pas le cas dans d'autres pays.

Pendant plusieurs années, il a été débattu de la manière dont une méthode de classement basée sur les risques pourrait être incorporée dans la CEI 61226. Comme indiqué précédemment, il existe des différences importantes dans l'utilisation des évaluations de risques dans le monde, ce qui engendre plusieurs problèmes pour la rédaction d'une Norme internationale, notamment:

a) Une méthode de classement basée sur les risques serait-elle acceptable en remplacement de l'approche déterministe? Si oui, quelles sont les exigences qu'il faut appliquer (en particulier concernant la norme relative à la modélisation et la validité des données)?

b) Si un classement basé sur l'évaluation des risques engendre des classements différents des FSE par rapport à l'approche déterministe, laquelle des deux approches devrait être prépondérante?

c) Les deux approches doivent-elles être utilisées ensemble afin d'en retirer un bénéfice maximal? L'approche déterministe est basée sur des principes de sûreté nucléaire solides et parfaitement éprouvés. Les résultats d'une méthode basée sur l'évaluation des risques pourraient engendrer le sous-classement de fonctions de CC spécifiques (en raison des caractéristiques de conception spécifiques à l'installation). Comment limiter ce sous-classement?

d) L'utilisation de l'évaluation des risques devrait-elle être rendue obligatoire en tenant compte de la robustesse de l'installation et des modifications de CC pendant toute la durée de vie? D'une manière similaire, des exigences devraient-elles être incluses pour l'utilisation de l'évaluation des risques dans les prises de décisions concernant la maintenance préventive?

INTRODUCTION

IEC 61226 "Nuclear power plants – Instrumentation and control systems important for safety – Classification" was published in 1993. The need to classify instrumentation and control functions on nuclear power plants originates from an International Atomic Energy Agency (IAEA) recommendation. IEC 61226 emphasizes that it is the **functions** which must be classified early in the design phase so that the degree of importance to safety of each function is determined. At the design stage, I&C functions are allocated to specific instrumentation and control systems each of which will normally comprise of several types of equipment. These systems and equipment are usually assigned to categories of safety significance, but it is the functions which determine the fundamental categorization.

In order to cater for this association of systems and equipment with functions, the concept of an FSE was introduced in IEC 61226. An FSE is defined as:

> Functions, and the associated systems and equipment. Functions are carried out for a purpose or to achieve a goal. The associated systems and equipment are the collection of components and the components themselves that are employed to achieve the functions.

IEC 61226 provides a categorization method for FSE based upon qualitative criteria. Many of the criteria are well-understood in the nuclear industry since they recognize that the single and most important nuclear safety function is to prevent accidents and mitigate against fission product releases. Consequently, the classification of FSE in IEC 61226 is a deterministic process and takes no account of quantitative risk assessment techniques.

During the last ten years, risk assessment methods, particularly applied to nuclear power plants, have matured although their use in NPP design (and licensing) varies greatly throughout the world. In some countries, a probabilistic risk assessment is seen as an essential element of the design process and of the final safety case; this is not the case in other countries.

For several years, how a risk based classification scheme could be incorporated into IEC 61226 has been the topic of discussion. As indicated above, there are significant differences in the use of risk assessments throughout the world, which leads to several problems when drafting an International Standard, namely:

a) Should a risk based classification scheme be acceptable in place of the deterministic approach? If so, what are the requirements (especially regarding the standard of modelling and the validity of data) that must be applied?

b) If a risk-based classification leads to different classifications of FSE compared to the deterministic approach, which should take precedence?

c) Should the two approaches be used together in order to gain the maximum benefit? The deterministic approach is based on sound, well-proven nuclear safety principles. Risk assessment results could lead to the classification of specific I&C functions being downgraded (because of plant-specific design features). Should this downgrading be limited in some way?

d) Should the use of risk assessments be mandated when considering the effectiveness of plant and I&C modifications throughout existence? Similarly, should requirements be included for the use of risk assessments in making decisions about preventive maintenance?

Après avoir abondamment débattu de ces questions, il a été convenu qu'un amendement de la CEI 61226 était prématurée. Cependant, afin de faire progresser le débat, le présent rapport technique présente un certain nombre d'approches pour l'utilisation de l'évaluation probabiliste des risques dans le classement des FSE.

Having discussed these issues extensively, it has been recommended that an amendment to IEC 61226 is premature at this time. In order to advance the debate, however, this Technical Report presents a number of different approaches to the use of probabilistic risk assessment in the classification of FSE.

CENTRALES NUCLÉAIRES – FONCTIONS D'INSTRUMENTATION ET DE CONTRÔLE-COMMANDE IMPORTANTS POUR LA SÛRETÉ – UTILISATION DES ÉVALUATIONS PROBABILISTES DE SÛRETÉ POUR LE CLASSEMENT

1 Domaine d'application

Le présent rapport technique fournit une étude de différentes méthodes permettant d'utiliser les résultats des évaluations probabilistes du risque afin d'établir des critères de classement basés sur l'évaluation du risque, dans le but de pouvoir classer les FSE dans les quatre catégories établies dans le cadre de la CEI 61226.

L'application des techniques d'évaluation des risques, conjointement avec l'approche d'évaluation des conséquences décrites dans la CEI 61226, est actuellement une décision des électriciens et/ou des organismes de réglementation au sein des Nations concernées. En l'absence d'une approche agréée sur le plan international, cette situation devrait perdurer. Néanmoins, le présent rapport technique a pour objet de susciter le débat sur ce sujet et d'encourager la convergence d'idées afin qu'une Norme Internationale CEI puisse être approuvée par tous.

Les principes de sûreté et l'utilité d'une approche de classement basée sur les risques ainsi qu'une description de quatre différentes approches sont présentés dans ce document.

Il est par ailleurs fait référence dans ce rapport à des documents CEI et AIEA qui traitent du même sujet.

Ce rapport fait également état des limites liées à l'utilisation des évaluations probabilistes de sûreté (EPS).

L'annexe A est un guide pour la modélisation de l'instrumentation et du contrôle-commande dans le cadre de l'évaluation probabiliste des risques.

2 Documents de référence

Publications AIEA

50-SG-D8:1985, *Systèmes d'instrumentation et de commande liés à la sûreté dans les centrales nucléaires*

INSAG 3: *Principes fondamentaux de sûreté pour les centrales nucléaires*

Publications CEI

CEI 60964:1989, *Conception des salles de commande des centrales nucléaires de puissance*

CEI 61226:1993, *Centrales nucléaires – Systèmes d'instrumentation et de contrôle-commande importants pour la sûreté – Classification*

NUCLEAR POWER PLANTS – INSTRUMENTATION AND CONTROL FUNCTIONS IMPORTANT FOR SAFETY – USE OF PROBABILISTIC SAFETY ASSESSMENT FOR THE CLASSIFICATION

1 Scope

This Technical Report provides a survey of some of the methods by which probabilistic risk assessment results can be used to establish "risk based" classification criteria, so as to allow FSEs to be placed within the four categories established within IEC 61226.

The application of risk based techniques, in conjunction with the consequence based classification approach given in IEC 61226, is currently decided by the utility and/or regulator within member Nations. In the absence of an internationally agreed approach, this should continue, but this Technical Report is intended to stimulate debate on this subject and encourage the convergence of views so that an IEC International Standard can be agreed.

The safety principles and the usefulness of a risk-based approach to classification are discussed and a description of four different approaches is presented.

In other respects, references are given in this report to IEC and IAEA documents which relate directly to the topic.

This report also discusses the limitations associated with the use of probabilistic safety assessment (PSA) techniques.

Guidance is given in annex A on modelling instrumentation and control functions for probabilistic risk assessment.

2 Reference documents

IAEA publications

50-SG-D8:1984, *Safety-related instrumentation and control systems for nuclear power plants*

INSAG 3: *Basic safety principles for nuclear power plants*

IEC publications

IEC 60964:1989, *Design for control rooms of nuclear power plants*

IEC 61226:1993, *Nuclear power plants – Instrumentation and control systems important for safety – Classification*

3 Définitions et abréviations

Pour les besoins du présent rapport technique, les définitions suivantes s'appliquent. Les définitions sont cohérentes avec celles d'autres codes ou normes CEI ou AIEA en vigueur, ou identiques à celles-ci (pour celles marquées d'un astérisque).

3.1 Définitions

3.1.1
diversité
existence de deux ou plusieurs façons ou moyens différents d'atteindre un objectif spécifié. La diversité est spécifiquement prévue comme une défense contre les défaillances de mode commun. Elle peut être réalisée en prévoyant des systèmes physiquement différents les uns des autres, ou par une diversité fonctionnelle, où des systèmes similaires assurent les objectifs spécifiés de façon différente, par des mesures prises au niveau développement, par exemple en séparant les équipes de conception des équipes de vérification et validation

NOTE Cette définition est plus large que celle utilisée par l'AIEA 50-C-D, qui est la suivante:

"Existence de composants ou de systèmes redondants prévus pour remplir une fonction déterminée, quand ces composants ou systèmes pris collectivement possèdent une ou plusieurs caractéristiques qui les différencient.

On peut donner, comme exemples de ces caractéristiques, des conditions de fonctionnement différentes, des tailles différentes de matériel, des fabricants différents, des principes de fonctionnement différents et des types de matériel utilisant des méthodes physiques différentes".

3.1.2
matériel*
partie(s) d'un système. Un matériel est un élément unique (et généralement amovible) ou une partie d'un système

[CEI 61226]

3.1.3
fonction*
but ou objectif spécifique à réaliser et qui peut être spécifié ou décrit sans référence aux moyens physiques nécessaires à sa réalisation

[CEI 61226]

3.1.4
fonctionnalité*
indication qualitative de la gamme ou du domaine des fonctions que peut exécuter un système ou un matériel. Un système capable d'accomplir nombre de fonctions complexes est dit avoir une «haute fonctionnalité», tandis qu'un système capable d'accomplir seulement quelques tâches simples est dit avoir une «fonctionnalité réduite»

[CEI 61226]

3.1.5
FSE du CC importants pour la sûreté
ceux-ci comprennent:

a) Les FSE de CC dont le défaut ou la défaillance pourrait entraîner pour le personnel du site ou le public une exposition inacceptable aux rayonnements;

b) Les FSE de CC qui empêchent les événements opérationnels prévus de provoquer une séquence significative;

c) Les FSE de CC qui réduisent les conséquences des pannes ou défaillances de structures, systèmes ou composants

[CEI 61226]

3 Definitions and abbreviations

For the purposes of this technical report, the following definitions apply. The definitions are consistent with, or identical to (if marked with an asterisk) those used in other IEC or IAEA codes and standards.

3.1 Definitions

3.1.1
diversity
the existence of two or more different ways or means of achieving a specified objective. Diversity is specifically provided as a defence against common mode failure. It may be achieved by providing systems that are different from each other, or by functional diversity, where similar systems achieve the specified objective by performing different functions, or by provision in the development process, for example by having separate design teams and verification and validation teams

NOTE This definition is wider than that used by the IAEA 50-C-D, which is as follows:

"The existence of redundant components or systems to perform an identified function, where such components or systems collectively incorporate one or more different attributes.

Examples of such attributes are: different operating conditions, different sizes of equipment, different manufacturers, different working principles and types of equipment that use different physical methods".

3.1.2
equipment*
one or more parts of a system. An item of equipment is a single definable (and usually removable) element or part of a system

[IEC 61226]

3.1.3
function*
a specific purpose or objective to be accomplished, that can be specified or described without reference to the physical means of achieving it

[IEC 61226]

3.1.4
functionality
a qualitative indication of the range or scope of the functions that a system or item of equipment can carry out. A system that can carry out many complex functions has a "high functionality"; a system that can only carry out a few simple functions has a "low functionality"

[IEC 61226]

3.1.5
I&C FSE important for safety*
the I&C FSE that comprise:

a) those I&C FSE whose malfunction or failure could lead to undue radiation exposure of the site personnel or members of the public;

b) those I&C FSE that prevent anticipated operational occurrences from leading to a significant sequence;

c) those I&C FSE that mitigate the consequences of malfunction or failure of structures, systems, or components

[IEC 61226]

3.1.6
sûreté de la centrale*
prévention de tout rejet radioactif imprévu ou incontrôlé susceptible d'être préjudiciable à la santé du personnel d'exploitation de la centrale ou du public

[CEI 61226]

3.1.7
sûreté nucléaire*
aptitude d'une centrale à éviter ou empêcher un accident nucléaire, c'est-à-dire une criticité incontrôlée dont l'importance serait susceptible de créer des dommages inacceptables

[CEI 61226]

3.1.8
en continu*
état d'un système qui remplit ses fonctions spécifiées comme l'exige la conception de la centrale

[CEI 61226]

3.1.9
performances*
efficacité avec laquelle une fonction prévue est exécutée (par exemple temps de réponse, précision, sensibilité aux modifications des paramètres)

[CEI 61226]

3.1.10
événements initiateurs hypothétiques (EIH)*
événements qui entraînent des incidents de fonctionnement et des situations accidentelles, leurs effets plausibles, causes de défaillances et leurs combinaisons plausibles

[CEI 61226]

3.1.11
redondance*
présence d'éléments ou systèmes (identiques ou différents) en nombre supérieur d'un minimum, de sorte que la perte de l'un d'entre eux ne cause pas la perte de la totalité de la fonction

[CEI 61226]

3.1.12
fonction de sûreté*
but particulier à atteindre aux fins de la sûreté

[CEI 61226]

3.1.13
système de sûreté*
système important pour la sûreté, prévu pour assurer, dans toutes conditions, l'arrêt sûr du réacteur et l'évacuation de chaleur du cœur, et/ou réduire les conséquences des événements initiateurs hypothétiques et des séquences significatives

[CEI 61226]

3.1.14
FSE de CC liés à la sûreté*
FSE de CC importants pour la sûreté qui ne font pas partie des systèmes de sûreté

[CEI 61226]

3.1.6
NPP safety*
the prevention of an unplanned or uncontrolled release of radioactive material that might injure the health of the NPP operating staff or the public

[IEC 61226]

3.1.7
nuclear safety*
the ability of an NPP to avoid or prevent a nuclear accident, that is an unplanned or uncontrolled criticality of magnitude that causes damage

[IEC 61226]

3.1.8
on-line*
the state of a system that is carrying out its specified functions as required by the NPP design

[IEC 61226]

3.1.9
performance
the effectiveness with which an intended function is performed (e.g. time response, accuracy, sensitivity to parameter changes)

[IEC 61226]

3.1.10
postulated initiating event (PIE)*
events that lead to anticipated operational occurences and accident conditions, their credible causal failure effects and their credible combinations

[IEC 61226]

3.1.11
redundancy*
provision of more than the minimum number of (identical or diverse) elements or systems, so that the loss of one does not result in the loss of the required function as a whole

[IEC 61226]

3.1.12
safety function*
a specific purpose that must be accomplished for safety

[IEC 61226]

3.1.13
safety system*
systems important for safety, provided to ensure, in any condition, the safe shutdown of the reactor and the heat removal from the core, and/or to limit the consequences of PIE and significant sequence

[IEC 61226]

3.1.14
safety related I&C FSE*
those I&C FSE important for safety that are not part of the safety systems

[IEC 61226]

3.1.15
séquence significative*
série ou ensemble d'événements crédibles susceptibles de provoquer des conséquences inacceptables comme par exemple:

- un dégagement radioactif inacceptable sur le site ou dans l'environnement. Il peut s'agir soit d'un dégagement massif, incontrôlé, à une fréquence d'occurrence située au-delà de la base de conception de la centrale, soit de dégagements à une fréquence d'occurrence située à l'intérieur de la base de conception, mais dépassant les limites spécifiées d'amplitude et/ou de fréquence;
- une détérioration de combustible inacceptable. Il peut s'agir d'une détérioration des gaines de combustible provoquant une augmentation inacceptable, de l'activité du réfrigérant primaire ou d'un endommagement du combustible de nature à compromettre son refroidissement

[CEI 61226]

3.1.16
critère de défaillance unique (CDU)*
ensemble de matériels qui répond au critère de défaillance unique s'il peut remplir son but malgré une défaillance unique, aléatoire qui est supposée survenir en un point quelconque de l'ensemble. Les défaillances résultant de la défaillance unique supposée sont considérées comme faisant partie intégrante de la défaillance unique

[CEI 61226]

3.1.17
sous-système*
division d'un système dotée elle-même des caractéristiques de ce système

[CEI 61226]

3.1.18
système*
groupement d'éléments connectés entre eux, constitué, dans un objectif donné, pour accomplir une fonction spécifiée

[CEI 61226]

Abréviations

DCC Défaillance de cause commune
CFD Conditions de fonctionnement de dimensionnement
CFCA Conditions de fonctionnement complémentaires et accident grave
FSE Fonction(s), systèmes et matériels associés qui la (les) mettent en oeuvre
AMDE Analyse des modes de défaillance et de leurs effets
CC Contrôle-commande
AIEA Agence internationale de l'énergie atomique
NPP Centrale nucléaire
EIH Evénement initiateur hypothétique
EPS Evaluations probabilistes de sûreté

3.1.15
significant sequence*
a credible series or set of events that would result in unacceptable consequences such as:

- unacceptable radioactive release at the site or to the wider environment. This might be either a massive, uncontrolled release at a frequency that is outside the NPP's design basis, or releases at a frequency that is within the design basis but exceed specified magnitude and/or frequency limits;
- unacceptable fuel damage. This might be damage to the fuel clad that leads to an unacceptable increase in the activity of the primary coolant, or structural damage to the fuel that impairs the ability to cool it

[IEC 61226]

3.1.16
single failure criterion*
an assembly of equipment satisfies the single failure criterion if it can meet its purpose despite a single random failure assumed to occur anywhere in the assembly. Consequential failures resulting from the assumed single failure are a part of the single failure

[IEC 61226]

3.1.17
sub-system*
a division of a system that in itself has the characteristics of a system

[IEC 61226]

3.1.18
system*
a set of interconnected elements constituted to achieve a given objective of carrying out a specified function

[IEC 61226]

Abbreviations

CCF Common cause failure
DBC Design basis conditions
DEC Design extension conditions
FSE Function(s) and the associated systems and equipment that implement it (them)
FMEA Failure modes and effects analysis
I&C Instrumentation and control
IAEA International atomic energy agency
NPP Nuclear power plant
PIE Postulated initiating event
PSA Probabilistic safety assessment

4 Limites d'utilisation des EPS

L'utilisation des techniques d'évaluation probabiliste des risques permet d'obtenir des informations qui peuvent conduire à des décisions plus avisées ainsi qu'à un usage plus rentable et plus efficace des ressources afin d'améliorer la sûreté des centrales nucléaires. L'utilisation des EPS dans la conception et comme support à l'exploitation des centrales nucléaires a cependant été limitée en raison de plusieurs facteurs:

- le développement et l'utilisation des techniques d'évaluation probabiliste des risques continuent à évoluer au sein des états membres et leur niveau d'acceptation dans le monde n'est pas cohérent;
- l'application des techniques d'évaluation probabiliste des risques en tant qu'outil de classement dans la conception d'une centrale nucléaire exige la réalisation d'EPS au stade précoce de la phase de conception. La réalisation d'une telle évaluation détaillée à ce stade n'est pas courante, d'une part en raison des modifications apportées à la conception et d'autre part en raison du manque de données quantitatives à ce premier stade.

Par ailleurs, même lorsque les EPS sont appliquées à une installation existante, l'analyse fait souvent l'objet de limites technologiques qui empêchent la réalisation de l'examen de cette installation en utilisant exclusivement les données probabilistes. Cela est dû au fait que les EPS peuvent ne pas être suffisamment précises et exhaustives. Ces limites résultent:

- des difficultés liées à la modélisation et à la quantification des défaillances de cause commune, des erreurs de logiciel et des erreurs humaines,
- du manque ou de l'indisponibilité d'informations spécifiques à l'installation,
- de l'exclusion des états opérationnels autres que l'état nominal,
- des limites dans la définition du niveau des EPS effectuées,
- de l'exclusion de certains événements initiateurs potentiels (par exemple incendies, inondations, séismes),
- d'une bonne connaissance des incertitudes.

Dans le cas d'une nouvelle installation, l'application des résultats des EPS aux systèmes et matériels de CC est en outre limitée par l'impossibilité, pour le concepteur, de définir en détail toutes les fonctions de CC requises.

Pour toutes ces raisons, l'utilisation des EPS, comme seule base pour la conception et le classement des fonctions de sûreté associées au CC, n'est pas réaliste. Malgré ces limites, les EPS sont de toute évidence précieuses lorsqu'elles sont utilisées conjointement avec l'approche qualitative basée sur le principe de la défense en profondeur qui reste la base de conception de la sûreté des centrales nucléaires (voir la CEI 61226). Lorsque les EPS sont utilisées pendant la phase initiale de conception des futures centrales nucléaires ou pour le réexamen de sûreté des installations existantes, il convient de les utiliser en tant que complément de la méthode qualitative, comme cela est décrit dans les articles qui suivent.

5 Utilisation des EPS: méthodes et résultats

5.1 Introduction

La conception d'une centrale nucléaire est principalement basée sur des exigences déterministes strictes et sur des principes de défense en profondeur bien connus et éprouvés. Toutefois, des études probabilistes peuvent être effectuées afin de déterminer, sous l'aspect quantitatif, l'importance relative des fonctions d'instrumentation et de contrôle-commande dans la sûreté globale de la centrale nucléaire.

4 Limitations regarding the use of PSA

The use of probabilistic safety assessment technology enables information to be obtained which can lead to improved risk-informed decisions and to more cost effective and efficient use of resources to improve the safety of NPPs. The use of PSA techniques in the design and in-service support of NPPs has been limited, however, because of several factors:

- the development and use of probabilistic safety assessment techniques continues to evolve within member nations and its level of acceptance is not consistent.
- the application of probabilistic safety assessment techniques as a classification tool in the design of a NPP requires a PSA to be carried out early in the design phase. The performance of such a detailed assessment at this point in time is not common practice, partly due to the changing plant design and partly due to the lack of quantitative data at this first stage.

Also, even when the PSA is applied to an existing design, there are often technical limitations in the analysis which prevent the design review being performed exclusively using probabilistic data as its basis. This is because the PSA might not be sufficiently accurate and exhaustive. These limitations include:

- the difficulties related to modelling and quantifying common cause failures, software errors, and human errors,
- the lack or the unavailability of plant specific information,
- the exclusion of operational states other than the full power state,
- the scope limitations of the level of the PSA performed,
- the exclusion of some potential initiating events (e.g. fire, flood, earthquake),
- the completeness of the uncertainty analysis.

In the case of a new design, the application of PSA results to I&C systems and equipment is further restricted by the inability of the designer to define in detail all the required I&C functions.

For these reasons, the use of PSA, as the sole basis for the development of the design and classification of its I&C safety functions cannot be achieved. Despite these limitations, PSA is clearly valuable when used in conjunction with the qualitative approach based upon the defence-in-depth principle which has been firmly established in the safety design basis of NPPs (see IEC 61226). When PSA is used during the design phase for future NPPs as well as during the review of existing designs, it should be used along with and as a complement to the qualitative method, as described in the following clauses.

5 The use of PSA: methods and results

5.1 Introduction

The design of an NPP is principally based upon stringent deterministic requirements and on the well-understood and well-proven defence-in-depth principles. However, probabilistic studies can be carried out to determine, in a quantitative format, the relative importance of the instrumentation and control functions in the overall safety of the NPP.

En fait, les études probabilistes de sûreté peuvent être utilisées dans deux différents domaines:

- comme support au processus de conception des nouvelles centrales nucléaires afin de déterminer le classement correct des fonctions de CC, en particulier pour éviter un sur-classement ou un sous-classement,
- comme vérification de la conception et identification des améliorations les plus efficaces qu'il convient d'apporter aux systèmes de CC. Cette utilisation des techniques probabilistes est particulièrement appropriée dans le cadre des réexamens de sûreté des centrales nucléaires existantes.

Ainsi, les évaluations probabilistes des risques peuvent être utilisées pour améliorer la conception des centrales nucléaires et concentrer les efforts sur les fonctions de CC les plus importantes en matière de sûreté.

Toutefois, nous devons noter que l'utilisation des EPS ne cesse d'évoluer et que leur niveau d'acceptation n'est pas cohérent au sein des états membres, même si les EPS sont utilisées dans certains pays dans le cadre des procédures d'autorisation.

5.2 Utilisation des EPS pour la conception des futures centrales nucléaires

5.2.1 Domaine d'application général

Les évaluations probabilistes de la sûreté peuvent être utilisées dans la phase de conception avec les buts suivants:

- identifier la fiabilité des équipements et systèmes requis pour faire face aux objectifs de sûreté;
- compléter l'approche qualitative dans l'évaluation de la fréquence des événements initiateurs;
- identifier les séquences de défaillances complexes à prendre en considération dans la phase de conception;
- comme support de la définition des spécifications techniques et des procédures d'urgence;
- confirmer la phase de conception.

Les EPS permettent habituellement l'évaluation de la fréquence d'endommagement du cœur, l'évaluation de la robustesse de l'enceinte de confinement et l'évaluation de la fréquence et de l'ampleur des rejets.

Au premier stade de la conception, des EPS simplifiées sont généralement utilisées pour l'évaluation du CC, en particulier dans le but d'examiner la suffisance des dispositions prises en termes de redondance ainsi que vis-à-vis des défaillances de cause commune pour des systèmes redondants simples ou des erreurs humaines. De plus, il est également important de connaître les incertitudes et de les prendre en considération dans l'évaluation des risques et dans le classement qui s'ensuit. En conséquence, il faut accorder une attention particulière aux points suivants:

- les études de sensibilité et l'évaluation des incertitudes dans la modélisation;
- la qualité de la fiabilité des bases de données qui sont utilisées pour servir de référence.

5.2.2 Méthodes

5.2.2.1 Objectifs probabilistes de sûreté

Il est recommandé que les objectifs probabilistes de sûreté pour les fonctions de CC soient compatibles avec ceux établis pour l'ensemble de la centrale nucléaire. Un exemple d'objectifs est celui indiqué dans le document AIEA INSAG 3:

In fact, probabilistic safety assessments may be used in two areas:

- to support the design process of new NPPs in order to determine the correct classification of the I&C functions, especially to avoid down or upgradings of classification;
- to verify the design and identify improvements to the I&C systems which will be most effective. This use of probabilistic techniques is particularly appropriate to the safety reviews of existing NPPs.

In this way, probabilistic safety assessments can be used to improve the design of NPPs and focus resources on the provision of I&C functions which have the greatest safety significance.

However, we have to note that the use of PSA continues to evolve within member nations and its level of acceptance is not consistent, even if PSA are used in some countries as part of the licensing process.

5.2 Use of PSA in the design of future NPPs

5.2.1 Overall scope

PSA may be used in the design phase with the following purposes:

- to identify the reliability of equipment and systems required to cope with safety targets;
- to complement the qualitative approach in assessing the frequency of initiating events;
- to identify the complex failure sequences to be considered in the design;
- to support the definition of technical specifications and emergency procedures;
- to achieve a balanced design.

Typically, PSA covers the assessment of the core damage frequency, the evaluation of the containment response and the estimation of release frequencies and magnitudes.

Simplified PSA methods for I&C assessment are normally used during the early stages of the design process, in particular to examine the adequacy of redundancy provisions and the need for safeguards against common cause failure of simple redundant systems and to guard against the impact of human errors. Moreover, it is usually important to know the uncertainties and take them into account in the safety assessment and in the subsequent classification. Therefore, particular attention must be given to the following points:

- sensitivity studies and the evaluation of the uncertainties in the modelling;
- the quality of the reliability data bases which are used to provide reference data.

5.2.2 Methods

5.2.2.1 Probabilistic safety targets

Probabilistic safety targets for the I&C functions should be consistent with those set for the overall NPP. An example of such targets is provided in IAEA INSAG 3 document as follows:

- le risque global d'endommagement du cœur doit être inférieur à 10^{-5} par année réacteur;
- le risque global de dépassement des rejets limites doit être inférieur à 10^{-6} par année réacteur;
- les séquences impliquant de très importants rejets avec une défaillance brutale du confinement doivent avoir une fréquence cumulée très inférieure à l'objectif précédent de 10^{-6} par année réacteur.

5.2.2.2 Evénements initiateurs

Les événements initiateurs qui seront pris en considération dans les études probabilistes sont principalement les événements utilisés pour justifier la conception d'un système élémentaire ou une fonction de CC spécifique.

En conséquence, le concepteur s'exprime très souvent en familles d'événements. Une famille d'événements est en fait un groupe d'événements élémentaires qui conduit au même événement principal. Cette répartition des événements élémentaires en familles d'événements peut varier d'une installation à l'autre mais il convient que la répartition choisie soit clairement définie au début de la conception.

5.2.2.3 Données de fiabilité

Pendant la phase de conception, il est habituel d'utiliser une base de données de fiabilité générique car peu, voire aucune donnée spécifique concernant l'installation n'est disponible à ce premier stade. Il est recommandé que ces données soient utilisées avec beaucoup de précaution dans la mesure où elles peuvent ne pas être validées pour l'application à l'environnement de la centrale nucléaire.

Il est possible d'utiliser des valeurs spécifiques, auquel cas il convient d'effectuer des études de sensibilité afin d'évaluer leur influence sur la conception au niveau des hypothèses et des données de base les plus critiques.

5.2.2.4 Défaillance de cause commune (DCC)

Les matériels de CC sont sujets à des défaillances de cause commune en raison de l'utilisation de composants et techniques identiques. Ces défaillances de cause commune peuvent être provoquées par une erreur de conception, de fabrication, d'exploitation et de maintenance ou par des contraintes environnementales communes.

Concernant les matériels constitués de composants dont l'absence de défaillances résultant d'erreurs de conception, de fabrication ou des contraintes environnementales peut être raisonnablement déterminée par un essai, une expérience ou une analyse; il convient que la probabilité de défaillance de cause commune soit quantifiée selon la modélisation du facteur β ou toute autre technique équivalente appropriée.

Concernant les matériels constitués de composants dont l'absence de défaillances résultant d'erreurs de conception, de fabrication ou des contraintes environnementales ne peut pas être déterminée par un essai, une expérience ou une analyse, la modélisation du facteur β n'est pas applicable. Les exemples correspondants concernent les composants électroniques programmables et informatiques.

La pratique courante pour la quantification de la fiabilité des systèmes redondants qui utilisent un logiciel pour réaliser les fonctions importantes de sûreté consiste à postuler, de manière qualitative, une défaillance par demande pour le système redondant correspondant.

- core damage cumulative frequency shall be lower than 10^{-5} per reactor year;
- cumulative frequency of exceeding the limiting release shall be lower than 10^{-6} per reactor year;
- sequences involving very large releases with gross failure of containment shall have a cumulative frequency well below the previous target of 10^{-6} per reactor year.

5.2.2.2 Initiating events

The initiating events that will be considered in the probabilistic studies are principally the events used to justify the design of a specific plant system or of a specific I&C function.

Accordingly, the designer speaks about a family of events. A family of events is in fact a group of elementary events which lead to the same main event. This arrangement of elementary events in families of events may differ from plant to plant but the arrangement selected should be clearly defined at the beginning of the design.

5.2.2.3 Reliability data

During the design phase, it is usual for a generic reliability data base to be used because little or no plant specific data is available. Such data should be used with caution since it may not be validated for the application on the environment of the NPP.

Point values may be used, in which case sensitivity studies should be carried out to evaluate the influence on the design of the critical assumptions and base data.

5.2.2.4 Common cause failure (CCF)

I&C equipment is subject to common cause failures through the use of identical components and techniques. These common cause failures can be caused by error in design, manufacturing, operation and maintenance processes as well as common environmental stresses.

For the case of equipment that consists of components whose freedom from failures caused by design/manufacturing errors and environmental stresses can be reasonably determined through test, experience or analysis; the probability of common cause failure should be quantified according to the β factor model or another appropriate technique.

For the case of equipment that consists of components whose freedom from failures caused by design/manufacturing errors and environmental stresses cannot be reasonably determined through test, experience or analysis, the β factor model is not applicable. Examples include programmable electronic equipment and computer-based equipment.

The present state of practice for the quantification of the reliability of redundant systems which employ software for the achievement of functions important to safety is to assume a failure per demand for the redundant system, based upon qualitative engineering judgement.

5.2.2.5 Fiabilité humaine

La fiabilité humaine ou la probabilité d'apparition d'une erreur humaine est une donnée importante dans les études de conception. En conséquence, il convient que l'évaluation de la probabilité d'erreurs humaines soit incluse dans les EPS. Il est recommandé que l'évaluation des erreurs humaines prenne en compte les éléments indépendants du temps (par exemple erreurs latentes) et ceux dépendants du temps (par exemple erreurs de diagnostic).

5.2.3 Analyse de l'installation et modélisation du CC dans les EPS

Il convient que le modèle soit constitué

- d'un ensemble d'événements initiateurs;
- d'arbres d'événements qui décrivent les séquences accidentelles en termes de progression d'un événement initiateur jusqu'à un état final, y compris les succès ou les échecs des systèmes ainsi que des actions de l'opérateur;
- d'arbres de défaillances ou des fonctions mathématiques équivalentes qui décrivent les défaillances des systèmes sous la forme de combinaisons d'événements élémentaires (défaillances des composants, erreurs humaines, etc.).

Les arbres d'événements et les arbres de défaillances peuvent être combinés afin d'identifier les combinaisons d'événements élémentaires spécifiques à chaque séquence accidentelle.

Une proposition de modélisation des fonctions d'instrumentation et de contrôle-commande à utiliser dans les EPS est donnée à l'annexe A.

5.3 Avantages de l'utilisation des EPS pour les centrales nucléaires existantes

Pour les centrales nucléaires existantes, les EPS sont largement utilisés lors des réexamens périodiques de la sûreté afin de

- mettre en évidence et hiérarchiser les séquences dominantes;
- aider à la décision concernant la mise en œuvre des modifications qu'il convient d'apporter aux systèmes de sûreté et aux matériels de CC correspondants;
- évaluer le niveau de sûreté global des installations.

Des priorités peuvent être attribuées aux améliorations possibles en fonction de la diminution des risques (probabilité et conséquences). Les EPS permettent également d'attribuer une attention particulière aux séquences qui peuvent conduire

- à la fusion du cœur à haute pression;
- à un contournement du confinement;
- aux autres séquences dominantes, telles que celles incluant des erreurs humaines ou des défaillances de matériels.

Les EPS constituent un outil très utile pour évaluer l'importance des fonctions de CC et estimer le bénéfice de modifications potentielles. Le concepteur peut ainsi utiliser les résultats des EPS avec ceux d'autres études déterministes afin de déterminer les améliorations optimales pour la sûreté. Cela permet d'avancer des arguments coût/bénéfice sur la base d'informations et d'analyses technologiques sûres.

5.2.2.5 Human reliability

Human reliability or the probability of occurrence of human error is an important design consideration. Therefore, the assessment of the probability of human error should be included in the PSA. On the human error assessment both time independent (e.g. latent errors) and time dependent (e.g. diagnosis errors) should be considered.

5.2.3 Plant analysis and modelling I&C in PSA

The plant model should consist of

- a set of initiating events;
- event trees that describe the accident sequences in terms of progression from an initiating event to a final state including the successes or failures of systems and operator actions;
- fault trees or the equivalent mathematical functions that describe the system failures as combinations of basic events (component failures, human errors, etc.).

Event trees and fault trees can be combined in order to identify the basic event combinations specific to each accident sequence.

A proposal of modelling instrumentation and control functions for use in PSAs is presented in annex A.

5.3 Benefits of the use of PSA for existing NPPs

For existing NPPs, PSA is widely used during the periodic safety reviews in order to

- highlight and to place in the dominant sequences a hierarchy;
- help decide whether to implement modifications to the safety and safety-related I&C systems and equipment;
- evaluate the global safety level of the plants.

The possible improvements can be prioritized according to the reduction of risk (probability and consequences). Also the PSA allows attention to be paid to sequences which can lead to

- high pressure core melt;
- containment by-pass;
- other dominant sequences, such as those including human errors or equipment failures.

PSA is a very useful tool to evaluate the importance of I&C functions and assess the benefit of potential modifications. So, the designer can use the results of PSA along with other deterministic studies in order to decide which improvements will give the greatest safety improvement. This allows cost-benefit arguments to take place based upon sound engineering information and analysis.

6 Utilisation des EPS pour le classement

6.1 Généralités

Comme présenté dans l'article 4, les évaluations quantitatives du risque peuvent être utilisées pour compléter l'approche déterministe du classement des fonctions de CC. Il est bien connu que le développement et l'utilisation des techniques d'évaluation du risque (souvent appelées évaluations probabilistes du risque ou évaluations probabilistes de sûreté) sont en évolution au sein des états membres et ne sont pas encore approuvés.

Les informations obtenues grâce à l'utilisation des EPS peuvent faciliter la prise efficace de décisions concernant les risques et permettre une utilisation plus efficace des ressources.

Il ne faut pas que les méthodes et la technologie des EPS remplacent l'approche de défense en profondeur, mais il convient au contraire qu'elles complètent les méthodes déterministes, en particulier lorsque les EPS sont reconnues et les données disponibles.

Pour des résultats optimaux, il est recommandé que les EPS soient utilisées pendant la phase de conception d'une centrale nucléaire et de son système de contrôle-commande afin de confirmer le classement correct des fonctions de CC requises.

Les EPS peuvent être utilisées pour les centrales nucléaires existantes afin de déterminer les parties du système de contrôle-commande qu'il convient de modifier ou d'améliorer dans le but d'accroître la sûreté, d'améliorer la conception et l'exploitation de la centrale nucléaire et du système de CC. Cela est en particulier approprié aux examens de la sûreté des centrales nucléaires existantes.

Cet article présente quatre différentes approches de l'utilisation des EPS. Cette liste de méthodes n'est pas exhaustive; en effet il existe de nombreux cas dans lesquels des techniques probabilistes peuvent faciliter les prises de décision pendant la conception d'une centrale nucléaire. Le présent rapport a pour objet de stimuler le débat sur l'utilisation optimale des techniques probabilistes pendant la phase de conception des systèmes d'instrumentation et de contrôle-commande d'une centrale nucléaire.

Les quatre approches sont les suivantes:

Approche 1, voir 6.2 – Approche basée sur le temps et l'état du réacteur

Cette approche a été introduite dans le document European Utility Requirements pour le classement des équipements, notamment de contrôle-commande.

Approche 2, voir 6.3 – Approche basée sur l'importance quantitative

Cette approche est basée entièrement sur une technique probabiliste pour déterminer la contribution de chaque fonction de CC dans les séquences de défaillance de la centrale. De cette manière, l'importance de chaque fonction de CC peut être quantitativement calculée. La technique a été utilisée dans une centrale aux Etats-Unis comme base de surveillance en service du risque.

Approche 3, voir 6.4 – Approche basée sur les conséquences et la mitigation

Cette approche a été utilisée au Canada pour la conception des centrales nucléaires CANDU.

Approche 4, voir 6.5 – Approche basée sur la défense en profondeur

Cette approche est axée sur l'utilisation des techniques probabilistes permettant de modifier le classement du CC déterminé au préalable par la méthode qualitative approuvée. Elle envisage la possibilité d'utiliser les techniques probabilistes dans le but de surclasser d'un niveau le CC afin de minimiser le risque de dépendance excessive des données probabilistes basées sur les fiabilités génériques des composants.

Cette approche n'a pas encore été appliquée à un classement des fonctions d'une centrale nucléaire.

6 The use of PSA for classification

6.1 General

As discussed in clause 4, quantitative risk assessment can be used to supplement the deterministic approach to classification of I&C functions. It is recognized that the development and use of risk assessment techniques (often termed probabilistic risk assessment or probabilistic safety assessment) are evolving within member nations and have not reached a consistent level of acceptance.

The information obtained from the use of PSA technology can lead to the improvement of risk-effective decision making and a more focused and efficient use of resources.

The use of PSA methods and technology must not replace the defence-in-depth approach but should be used to complement deterministic methods, especially where PSA methods are well-established and data is available.

For the most effective results, PSA should be used during the design phase of the NPP and its I&C system to confirm the correct classification of the required I&C functions.

PSA may be used on existing NPPs to determine those parts of the I&C system which should be modified or enhanced in order to improve the safety, design and operation of the plant and the I&C system. This is particularly appropriate to the safety reviews of existing plants.

This clause presents four different approaches to the use of PSA techniques. This list of methods is not claimed to be comprehensive; indeed, there will be many ways in which probabilistic techniques can improve the decision making during the design of a NPP. This report is intended to stimulate debate on the best use of probabilistic techniques during the design phase of the instrumentation and control systems of a NPP.

The four approaches are as follows:

Approach 1, see 6.2 – Time and reactor states based approach

This has been introduced in the European Utility Requirements document to be used for future NPP to decide how I&C functions should be classified.

Approach 2, see 6.3 – Quantitative importance based approach

This approach is based on a full probabilistic technique to determine the contribution of each I&C function to plant fault sequences. In this way, the importance of each I&C function can be quantitatively calculated. The technique has been used in the USA as the basis for on-line plant risk monitoring.

Approach 3, see 6.4 – Consequence – mitigation based approach

This approach has been used in Canada for the design of CANDU NPPs.

Approach 4, see 6.5 – Defence in depth based approach

This approach is aimed at the use of probabilistic techniques to modify I&C classifications that have been determined by the accepted qualitative method. It considers whether the probabilistic techniques should not be permitted to change the classifications by more than one level in order to minimize the risk of over reliance on probabilistic data which may be based on generic component reliability data.

The approach has not yet been applied to a classification of functions of NPPs.

6.2 Approche 1: approche basée sur le temps et l'état du réacteur

6.2.1 Utilisation des EPS conjointement avec une méthode déterministe fonctionnelle

Pour classer les fonctions, systèmes et équipements, le concepteur peut procéder en deux étapes:

- en premier lieu, définir et classer les fonctions de CC en utilisant une approche déterministe pour répondre aux objectifs de sûreté pour les CFD;
- en second lieu, utiliser les EPS pour confirmer et classer les systèmes et équipements nécessaires pour atteindre les objectifs de sûreté en termes de cibles de sûreté probabilistes; cette seconde étape concerne principalement les CFCA qui constituent un ensemble de séquences accidentelles étudié au-delà des conditions de fonctionnement de dimensionnement.

6.2.2 Classement des fonctions, systèmes et équipements

L'objectif de la catégorisation et du classement est d'établir une gradation rationnelle et justifiable dans les exigences appliquées aux fonctions, systèmes et équipements. Il faut que cette graduation soit cohérente avec la fonction de sûreté assurée sans exiger une qualification des matériels ou un niveau de qualité excessifs.

6.2.2.1 Première étape: mitigation des événements initiateurs hypothétiques

Pour atteindre les objectifs mentionnés précédemment, le processus de classement s'appuie sur deux paramètres:

- l'état physique du réacteur;
- le temps disponible pour déclencher les fonctions de sûreté.

Deux états physiques de la centrale sont considérés dans la définition des classes de sûreté afin de permettre la hiérarchisation des fonctions de sûreté et des exigences associées.

Ces états correspondent aux conditions d'arrêt et sont l'état contrôlé et l'état d'arrêt sûr.

Ils sont définis comme suit:

Etat contrôlé: cet état correspond à la fin du transitoire rapide. Dans cette situation, l'exploitation de la centrale est stabilisée avec

- la réactivité contrôlée[1)],
- la chaleur du cœur évacuée avec un inventaire stable du réfrigérant du coeur.

Etat d'arrêt sûr: il s'agit de l'état au cours duquel la décroissance de la puissance résiduelle est durablement assurée. Les paramètres physiques de l'installation sont dans l'état suivant:

- le cœur est sous-critique,
- les rejets sont maintenus dans les limites de la catégorie de la CFD considérée,
- la chaleur de décroissance est durablement assurée (par une chaîne de refroidissement fermée telle que le système d'injection de secours ou le système d'évacuation de chaleur du réacteur à l'arrêt).

[1)] Dans la pratique, le cœur est en général sous-critique, mais un retour à la criticité est accepté, uniquement pour quelques évènements et pendant un court délai.

6.2 Approach 1: time and reactor states based approach

6.2.1 Use of PSA in conjunction with a functional deterministic method

For the classification of functions, systems and equipment, the designer may proceed in two steps:

- firstly, define and classify I&C functions using a deterministic approach to meet the safety goals for each DBC;
- secondly, use the PSA to confirm and to classify the systems and equipment needed to achieve the safety goals in term of probabilistic safety targets; this second step primarily concerns the DEC, which are a specific set of accident sequences that are considered beyond the design basis conditions.

6.2.2 Classification of functions, systems and equipment

The objective of the safety categorization and classification is to establish a rational and defensible gradation in the requirements applied to functions, systems and equipment. The graded requirements must be consistent with the importance to safety of the functions, without requiring unduly high levels of quality and equipment qualification.

6.2.2.1 First step: mitigation of postulated initiating events

To achieve the objectives mentioned above, the classification process is based on two considerations:

- the physical state of the reactor;
- the time available to initiate safety functions.

Two physical states of the plant are considered in order to give a definition of the safety classes and to allow the introduction of a hierarchy within the safety functions and the associated requirements.

These states correspond to shutdown conditions and are the controlled state and the safe shutdown state.

They are defined as follows:

Controlled state: this state is the state which puts an end to the rapid transient. In this situation, the plant operation is stabilized with:

- reactivity under control[1)],
- core heat removed with a stable core coolant inventory.

Safe shutdown state: this is a state where residual power decay is durably ensured. Physical plant parameters are in the following situation:

- the core is subcritical,
- activity release is within the limits of the corresponding DBC,
- decay heat is durably ensured (by a closed cooling chain such as the safety injection system or the reactor heat removal system).

---

1) In practice, subcriticality in general but limited re-criticality is accepted for a few events and a short period of time.

Considérant ces deux états, les fonctions de sûreté nécessaires pour réduire les EIH sont classées en fonction du moment auquel elles interviennent. L'étude du déroulement type des EIH montre qu'il est possible de distinguer trois phases:

- la première, très brève, consiste en une rapide évolution des paramètres physiques du réacteur, et nécessite l'intervention des systèmes de sûreté automatiques pour parvenir à l'état contrôlé où tous les paramètres sont sous contrôle;
- la seconde est caractérisée par une lente évolution des paramètres d'état autorisant des interventions humaines; elle se termine par l'atteinte de l'arrêt sûr;
- la troisième correspond à la stabilisation de tous les paramètres du réacteur, à l'exception d'une légère diminution de la température des équipements utilisés pour évacuer la puissance résiduelle; en raison du faible niveau de puissance résiduelle, la défaillance d'un équipement provoquerait une très lente évolution des paramètres physiques; dans ces conditions, les délais disponibles pour des actions en local deviennent plus importants et autorisent des interventions lourdes.

Il est possible de classer les fonctions de sûreté selon qu'elles interviennent dans la première, la seconde ou la troisième phase. Il est ensuite possible d'attribuer des exigences graduelles à ces catégories dans la mesure où les facultés de récupération des moyens de mitigation permettant de stabiliser le réacteur s'améliorent nettement pendant la seconde phase et encore plus dans la troisième phase.

Du point de vue de la sûreté, il faut que l'état d'arrêt sûr soit maintenu sans limite de temps. Néanmoins, il est raisonnable d'accepter une certaine souplesse pour les FSE nécessaires pour maintenir l'arrêt sûr au-delà d'une certaine durée, car le délai est suffisant pour rétablir les systèmes internes ou prendre des dispositions supplémentaires externes. Il est donc proposé d'assouplir les exigences appliquées aux FSE nécessaires pour maintenir l'arrêt sûr après 24 h (3^{e} phase) et d'accepter l'utilisation de FSE non classés après 72 h, cela reposant sur la possibilité de mise en exploitation de moyens additionnels durant cette période.

Cette approche conduit à la définition suivante des catégories de fonctions de CC:

- catégorie A: tous les FSE de sûreté nécessaires après un EIH pour atteindre l'état contrôlé;
- catégorie B: tous les FSE de sûreté (non déjà classés A) nécessaires à partir de l'état contrôlé pour atteindre l'état d'arrêt sûr et le maintenir jusqu'à 24 heures après l'événement initiateur;
- catégorie C: toutes les fonctions de sûreté supplémentaires nécessaires pour maintenir l'arrêt sûr au-delà de 24 h et jusqu'à 72 h après l'événement initiateur; après ce délai, l'utilisation de systèmes non classés est admise (si l'arrêt sûr est atteint).

Cela est représenté schématiquement en 6.2.2.3. La base du classement est déterministe et les catégories A et B sont définies pour les FSE nécessaires pour l'atteinte de l'état d'arrêt sûr en cas de EIH pour les conditions de fonctionnement de dimensionnement.

6.2.2.2 Seconde étape: base probabiliste pour la mitigation des CFCA et la prévention des événements

Le processus de classement peut être complété en utilisant les résultats des EPS dans le but de satisfaire aux objectifs probabilistes de sûreté. Il convient d'utiliser les EPS pour définir la liste des séquences complexes qui requièrent la conception de systèmes supplémentaires ou modifiés ou la mise en œuvre de procédures opérationnelles nouvelles/modifiées. Les FSE de sûreté nécessaires pour atteindre et maintenir un état final dans les séquences complexes sont également affectés à la catégorie C, en fonction des résultats des EPS, s'ils sont critiques pour atteindre les objectifs de sûreté probabilistes globaux.

Considering these two states, the safety functions required to mitigate against the PIEs are classified according to the point in time at which their operation is required. The analysis of the typical PIE evolutions shows that it is possible to distinguish three different time periods:

- the first one, very short, consists of a rapid evolution of the physical parameters of the reactor; it requires the intervention of automatic safety systems to achieve the controlled state where all the parameters are under control;
- the second one is characterized by a slow evolution of the plant parameters, thus allowing human actions to be taken; it ends in the achievement of the safe shutdown;
- the third one corresponds to the stabilization of all the plant parameters, apart from a slight decrease in the temperature of the equipment used to remove the residual heat; because of the low level of residual heat, the failure of an equipment would result in a very slow evolution of the physical parameters; in these conditions, the time available for local actions is extended and allows for external interventions.

It is possible to classify the safety functions according to whether the functions are required to operate in the first, second or third time period. These categories can then be allocated progressive requirements as the facilities and means to stabilize the plant clearly improve during the second time period and become much easier to provide during the third phase.

From a safety point of view, the safety shutdown state must be maintained with no maximum time limit. Nevertheless, it is reasonable to accept a certain flexibility for the FSE necessary to maintain the safe shutdown after a certain time period because of the time allowed to restore (or recover) internal systems or to provide additional and external facilities. It is thus proposed to relax the requirements applied to FSE necessary to maintain safe shutdown after 24 h (3rd phase) and to accept the use of non classified FSE after 72 h, on the basis that additional facilities can be put into operation within this period.

This approach leads to the following definition of categories for I&C functions:

- category A: all safety FSE which are needed after a PIE to reach the controlled state;
- category B: all safety FSE (not already classified A) needed after achievement of the controlled state to reach the safe shutdown and to maintain it until 24 h after the initiating event;
- category C: all additional safety functions needed to maintain the safe shutdown from 24 h until 72 h after the initiating event; after this limit, non-classified systems can be used (if safe shutdown is reached).

This is shown diagrammatically in 6.2.2.3. The basis of the classification is deterministic and categories A and B are defined for FSE needed to achieve safe shutdown in case of DBC.

6.2.2.2 Second step: probabilistic basis for mitigation of DEC and prevention of events

The classification process can be completed by using the results of a PSA with the aim of achieving the probabilistic safety targets. The PSA should be used to define the list of complex sequences that require additional or modified systems to be designed or new/amended operating procedures to be implemented. The safety FSE needed to reach and maintain a final state in complex sequences are also assigned to the category C, according to the PSA results, if they are critical to meet the overall probabilistic safety targets.

L'état final dans les séquences complexes est défini comme suit:

- le cœur est sous-critique;
- les activités rejetées sont dans la limite de la catégorie des EIH les moins fréquents;
- la chaleur résiduelle est évacuée.

Il faut que les FSE de sûreté qui ne sont pas déjà classés et qui sont requis pour remplir l'objectif d'une probabilité d'endommagement du cœur de 10^{-5} par an soient, en général, affectés à la catégorie C. Cette catégorie peut également comprendre les fonctions qui ont un effet indirect sur la sûreté, telles que la gestion des déchets et le contrôle des accès.

Il convient que les séquences importantes, impliquant la mise en œuvre de mesures supplémentaires soient déterminées en utilisant les méthodes probabilistes sur la base de leur contribution aux objectifs probabilistes de fusion du cœur ou de rejets. Une liste des séquences complexes qu'il convient de prendre en considération dans le cadre des CFCA est proposée comme liste préliminaire, sur la base du retour d'expérience des EPS:

- transitoire incidentel sans arrêt d'urgence du réacteur;
- perte totale de l'eau alimentaire;
- accident de perte de réfrigérant primaire par petite brèche et par perte de l'injection de sécurité moyenne pression;
- accident de perte de réfrigérant primaire par petite brèche et par perte de l'injection de sécurité basse pression;
- perte totale des alimentations électriques;
- perte totale de la chaîne de refroidissement;
- ruptures multiples de tubes de générateur de vapeur;
- ruptures simultanées d'une tuyauterie principale de vapeur et de tubes de générateur de vapeur;
- rupture de tube de générateur de vapeur avec une soupape de décharge du générateur de vapeur affecté bloquée en position ouverte.

6.2.2.3 Schéma simplifié

Le tableau 1 présente un schéma simplifié de l'enchaînement des différents FSE de contrôle-commande après un EIH.

Tableau 1 – Classement des FSE de CC

	FSE de CC à utiliser pour l'analyse de la sûreté			
Etat des réacteurs	**Evénements initiateurs**	**Etat contrôlé**		**Etat d'arrêt sûr**
Echelle dans le temps		24 h		72 h
Conditions de fonctionnement de dimensionnement	Catégorie A	Catégorie B	Catégorie C	Non classés
CFCA		Catégorie C		Non classés
Agressions internes		Catégorie C		Non classés

The final state in complex sequences is defined as follows:

- the core is subcritical;
- activity releases are within the limit of the less frequent PIE category;
- decay heat is being removed.

Safety FSE, which are not already classified and which are required to comply with the core damage cumulative frequency of 10^{-5} per year must in general be assigned to category C. This category can also be used to collect functions which have an indirect effect on safety, such as waste management systems and access control systems.

The significant sequences, where additional measures are to be implemented should be determined using probabilistic methods, on the basis of the dominance of their contribution to the cumulated frequency targets for core melting or for exceeding limiting release. A list of complex sequences that should be considered in DEC is proposed as a preliminary list, based on the PSA experience:

- anticipated transient without scram;
- total loss of feedwater;
- small break loss of coolant accident and loss of medium head safety injection;
- small break loss of coolant accident and loss of low head safety injection;
- station black out;
- total loss of the cooling chain;
- multiple steam generator tube ruptures;
- steam line break and simultaneous steam generator tube ruptures;
- steam generator tube rupture with a stuck open main relief train in the affected steam generator.

6.2.2.3 Simplified scheme

The table 1 gives a simplified scheme of the hierarchy of use of the different classified I&C FSE after a PIE.

Table 1 – Classification of I&C FSE

	I&C FSE to be used in the safety analysis			
State of reactor	**Initiating event**	**Controlled state**	**Safe shutdown state**	
Timescale		24 h	72 h	
DBC	Category A	Category B	Category C	Non classified
DEC	Category C			Non classified
Internal hazards	Category C			Non classified

6.2.3 Exigences techniques associées

Certaines exigences techniques générales doivent être appliquées à la conception des fonctions de CC dans chacune des catégories ci-dessus. Par exemple

- la prise en compte du critère de défaillance unique;
- la nécessité d'une alimentation électrique de secours;
- la nécessité d'une séparation physique entre les voies fonctionnelles d'un système;
- la nécessité d'une mise en marche automatique.

Celles-ci sont résumées de façon générale dans le tableau 2.

Tableau 2 – Exigences fonctionnelles

Catégorie	A	B	C
Critère de défaillance unique	OUI	OUI [1)]	NON [2)]
Alimentation électrique de secours	OUI	OUI	NON [3)]
Séparation physique	OUI	OUI [1)]	NON
Mise en marche automatique	Jusqu'à 30 min	Jusqu'à 30 min	NON [4)]

[1)] Utilisation possible de la diversification fonctionnelle avec des critères appropriés pour cette diversification.

[2)] La redondance peut être exigée dans le cas d'un équipement inaccessible ou, si nécessaire, pour atteindre les objectifs probabilistes, ou pour certaines agressions.

[3)] Oui pour les fonctions qui requièrent une alimentation électrique de haute fiabilité dans les conditions applicables.

[4)] Il peut exister des exceptions pour certaines CFCA.

Il faut que d'autres exigences relatives aux systèmes soient également appliquées, comme cela est illustré au tableau 3.

Tableau 3 – Exigences relatives à l'équipement

Catégorie	A	B	C
Code de calcul	OUI	OUI	OUI [1)]
Assurance qualité	OUI	OUI	OUI
Essais périodiques	OUI	OUI	OUI
Base de données pour la fiabilité	OUI	OUI	SI UTILISÉE DANS LES EPS
Qualification	OUI	OUI	SI NÉCESSAIRE
Qualification sismique	OUI	OUI	NON

[1)] Un code de calcul est requis, mais pas nécessairement un code nucléaire.

6.2.4 Utilisation complémentaire des EPS lors du processus itératif de conception

Comme cela est indiqué en 6.2.1, les EPS sont utilisées dans la phase de conception pour compléter les méthodes déterministes. Cette pratique permet de réaliser une conception bien équilibrée et optimisée et apporte une garantie raisonnable que la conception sera conforme aux objectifs de sûreté globaux de la centrale.

6.2.3 Associated technical requirements

There are certain general technical requirements which shall be applied to the design of I&C functions in each of the above categories. For example:

- the need to consider the single failure criterion;
- the need for emergency electrical supply;
- the need for physical separation between functional trains in a system;
- the need for automatic actuation.

These are summarized in their most general application in table 2.

Table 2 – Functional requirements

Category	A	B	C
Single failure criterion	YES	YES [1)]	NO [2)]
Emergency electrical supply	YES	YES	NO [3)]
Physical separation	YES	YES [1)]	NO
Automatic actuation	Until 30 min	Until 30 min	NO [4)]

[1)] Possible use of functional diversification with appropriate criteria for that diversification.

[2)] Redundancy may be required for the case of equipment which is inaccessible or, if required, to meet probabilistic targets, or for certain hazards.

[3)] Yes for those functions which require electrical supply of high reliability in the relevant conditions.

[4)] For certain DEC, there may be exceptions.

Further requirements on the systems design must also be applied as illustrated in the table 3.

Table 3 – Equipment requirements

Category	A	B	C
Design code	YES	YES	YES [1)]
Quality assurance	YES	YES	YES
Periodic tests	YES	YES	YES
Data base for reliability	YES	YES	IF USED IN PSA
Qualification	YES	YES	IF NECESSARY
Seismic qualification	YES	YES	NO

[1)] A design code is required but not necessarily a nuclear code.

6.2.4 Complementary use of PSA alongside the iterative design process

As it is stated in 6.2.1, PSA is used in the design phase to supplement the deterministic methods. This practice enables a well-balanced and optimized design to be achieved and provides a reasonable assurance that the design will comply with the overall plant safety objectives.

Elles peuvent être effectuées pendant la phase de conception des nouvelles centrales nucléaires ainsi que pour les examens de sûreté des centrales existantes. Plusieurs EPS peuvent être nécessaires pour optimiser totalement la conception, chacune étant effectuée à un niveau différent. Par exemple:

- une première évaluation préliminaire au stade précoce de la conception afin de vérifier approximativement que les objectifs probabilistes de sûreté peuvent être atteints;
- une évaluation plus fine pendant la conception détaillée afin de déterminer les séquences complexes qui nécessitent la mise en oeuvre de mesures supplémentaires;
- une dernière, au stade de la conception, afin d'effectuer une vérification finale de la conception globale.

Ensuite, pendant la durée de vie de la centrale, il convient d'effectuer une EPS pour chaque examen de sûreté afin de confirmer que les objectifs probabilistes de sûreté sont toujours respectés.

6.3 Approche 2: approche basée sur l'importance quantitative

L'importance pour la sûreté des fonctions d'instrumentation et de contrôle-commande peut être estimée en prenant en compte les conséquences de leurs défaillances, tel que le non-fonctionnement lorsqu'il est requis ou un fonctionnement intempestif. Les EIH servant de base à la conception de la centrale nucléaire peuvent être utilisés comme point de départ de l'évaluation. Il convient que cette évaluation inclue l'analyse de toutes les séquences prépondérantes d'événements, afin d'identifier les fonctions importantes à effectuer par le CC.

Cette prise en compte des fonctions effectuées par les FSE du CC peut être utilisée pour affecter chaque FSE à l'une des catégories définies dans la CEI 61226, à savoir la catégorie A, B, C ou le non-classement. Une affectation en «non classée» est faite si le FSE n'est pas important pour la sûreté.

Les FSE de CC liés aux systèmes de sûreté, tels que définis dans le Guide de la sûreté 50-SG-D8 de l'AIEA, doivent en général être affectés à la catégorie A. Les FSE de CC définis dans ce guide comme étant liés à la sûreté sont généralement affectés à la catégorie B ou C (et occasionnellement à la catégorie A).

6.3.1 Critères d'affectation quantitatifs

Afin de pouvoir établir l'importance de la sûreté de chaque fonction de CC, il faut déterminer un ensemble de critères. Un exemple de ces critères est présenté ci-après, sur la base d'un travail qui a été effectué aux Etats-Unis. La technique est basée sur une analyse quantitative de la contribution au risque en utilisant la théorie de l'ensemble des coupes pour parvenir à une approche mathématique cohérente. Dans certains cas, une fonction peut être affectée à plusieurs catégories en raison de sa contribution à plusieurs séquences d'événements. Dans ce cas, l'affectation finale de ces fonctions doit être la catégorie applicable la plus élevée.

6.3.2 Critères quantitatifs

6.3.2.1 Expressions quantitatives du risque pour les centrales nucléaires

Lorsqu'une évaluation quantitative du risque est effectuée sur une centrale nucléaire, une ou plusieurs des expressions suivantes du risque peuvent être développées en fonction du niveau de l'EPS réalisée:

- fréquence de la fusion du cœur (ou de l'endommagement du cœur) (EPS de niveau 1);
- fréquence des rejets radiologiques et termes sources associés (EPS de niveau 2);
- effets sur la santé, mesurés en terme de possibilités latentes et/ou aiguës (EPS de niveau 3).

It can be carried out during the design phase of new nuclear power plants as well as during the safety reviews of current plants. Several PSA may be necessary in order to fully optimize the design, with each PSA being carried out at a different level. For example:

- a first preliminary one early in the design to check roughly that the probabilistic safety targets can be met;
- a more detailed one during the detailed design to determine the complex sequences that require additional measures;
- a last one, at the design stage to make a final check of the overall design.

Then, during the lifetime of the plant, PSA should be performed for each safety review to confirm that the probabilistic safety objectives are always met.

6.3 Approach 2: quantitative importance based approach

Instrumentation and control functions can be assessed for their importance to safety by considering the consequences of their malfunction, such as failure to operate when required to do so, or spurious operation. PIEs within the NPP's design basis can be used as the starting point for the assessment. This assessment should include the analysis of all significant sequences of events, in order to identify the important functions required to be performed by the I&C.

This consideration of functions performed by the I&C functions, systems and equipment can be used to assign each of the FSE to one of the categories defined in IEC 61226, that is category A, B, C or unclassified. An unclassified assignment is made if the FSE is not significant to safety.

I&C FSE falling within the boundary of the safety system as defined in IAEA Safety Guide 50-SG-D8 are generally to be assigned to category A. I&C FSE defined as safety related in that guide are generally assigned to category B or C (and occasionally category A).

6.3.1 Quantitative assignment criteria

In order to be able to establish the safety significance of every I&C function, a set of criteria must be determined. An example of these criteria is given below, based on work which has been carried out in the USA. The technique is based on a quantitative analysis of the contribution to risk using the cut set theory to give a consistent mathematical approach. In some cases, a function may be assigned to more than one category due to its contribution in several event sequences. In this case, the final assignment of such functions should be to the highest applicable category.

6.3.2 Quantitative criteria

6.3.2.1 Quantitative risk expressions for NPPs

When a quantitative risk assessment is performed, on a NPP one or more of the following risk expressions may be developed depending upon the level of the PSA performed:

- core melt (or core damage) frequency (level 1 PSA);
- radiological release frequency and associated source terms (level 2 PSA);
- health effects measured in terms of latent and/or fatalities (level 3 PSA).

En général, et comme minimum de base pour une EPS de niveau 1, une expression booléenne de l'endommagement du cœur est générée en termes d'union booléenne de toutes les séquences accidentelles des arbres d'événements menant à un endommagement du cœur[2]. Cette expression est généralement construite comme l'union booléenne de toutes les coupes minimales qui contribuent, au-delà d'un certain seuil minimal, à une ou plusieurs séquences accidentelles significatives. Autrement dit, l'endommagement du cœur peut être exprimé en termes de fréquences d'occurrence de tous les EIH. Les probabilités de chacune des séquences potentielles résultant d'un EIH individuel ou fréquence d'endommagement du cœur C(t) est la somme des fréquences pour lesquelles les événements initiateurs causent des dommages au cœur.

$$C(t) = \sum_{i=1}^{n_i} \Pr\left\{\begin{matrix}\text{Les FSE sont dans un état critique} \\ \text{lorsque l' événement se produit}\end{matrix}\right\} C_{f,i}(t)$$

$$C(t) = \sum_{i=1}^{n_i} \Pr\{U_i\, E_{i,k}\} C_{f,i}(t) \qquad (1)$$

où

Pr est la probabilité;

$E_{i,k}$ est l'événement de la coupe minimale «k» sachant que l'EIH «i» se produit;

U_i est l'union booléenne des coupes minimales contenant l'EIH «i»;

n_i est le nombre d'EIH;

$C_{f,i}(t)$ est la fréquence d'occurrence de l'EIH «i».

L'expression ci-dessus peut être évaluée, à condition que

- les FSE soient raisonnablement fiables (à savoir que la probabilité qu'au moins deux coupes minimales surviennent simultanément soit faible);
- les événements individuels composant les coupes minimales (à savoir les événements de base) puissent être considérés comme indépendants;
- la probabilité conditionnelle de défaillance par unité de temps «λ» soit une approximation suffisamment précise pour la fréquence de défaillance.

Dans ce cas, l'expression (1) devient:

$$C(t) = \sum_{i=1}^{n_i} \left\{ \sum_{\substack{j \\ i \in k_i}} \prod_{\substack{l \in K_j \\ i \in K_j \\ i=1}} q_i \right\} \lambda_i \qquad (2)$$

[2] La fréquence d'endommagement du cœur est choisie comme un exemple de mesure du risque pour laquelle l'importance des contributions à la sûreté peut être déterminée pour les FSE. Cependant, l'approche utilisant l'importance pour l'évaluation de la sûreté est générale et peut être employée d'une manière similaire pour toute fréquence d'occurrence d'événement sommet (comme les fréquences de rejet et l'effet sur la santé qui peuvent être exprimées sous la forme d'une union booléenne de coupes minimales associées).

In general, as a minimum for a level 1 PSA, a Boolean expression for core damage is generated in terms of the Boolean union of all the accident sequences on the event trees leading to core damage[2]. This expression is usually constructed for the Boolean union of all the minimum cut sets which contribute beyond some minimal level to one or more significant accident sequence. In other words, core damage can be expressed in terms of the frequency of occurrences of all the PIEs. The probabilities of each of the potential sequences resulting from an individual PIE or core damage frequency C(t) is the sum of the frequencies at which initiating events cause damage to the core.

$$C(t) = \sum_{i=1}^{n_i} \Pr\left\{\begin{matrix}\text{FSE are in a critical state} \\ \text{when the initiating event occurs}\end{matrix}\right\} C_{f,i}(t)$$

$$C(t) = \sum_{i=1}^{n_i} \Pr\{U_i E_{i,k}\} C_{f,i}(t) \qquad (1)$$

where

Pr is the probability;

$E_{i,k}$ is the event that minimal cut set “k” containing PIE “i” recurs;

U_i is the Boolean union of the minimal cut sets containing PIE “i”;

n_i is the number of PIEs;

$C_{f,i}(t)$ is the failure frequency of PIE “i”.

The above expression can be evaluated provided that

- the FSEs are reasonably reliable (i.e. the probability of two or more minimal cut sets occurring simultaneously is small);
- the individual events making up the cut sets (i.e. basic events) can be considered to be independent;
- the conditional probability of failure per unit time "λ" is a satisfactorily accurate approximation for the failure frequency.

In this case, expression (1) becomes:

$$C(t) = \sum_{i=1}^{n_i} \left\{ \sum_{\substack{j \\ i \in k_i}} \prod_{\substack{l \in K_j \\ i \in K_j \\ i=1}} q_i \right\} \lambda_i \qquad (2)$$

---

[2] Core damage frequency is chosen as the example risk measure for which importance to safety contributions can be determined for the FSE. However, the importance approach to safety evaluation is a general one and can be employed in a similar fashion for any top event occurrence frequency (such as release frequencies and health effect which can be expressed as a Boolean union of underlying minimal cut sets).

où

j est le domaine d'indice pour les coupes minimales;

K_j est la j° coupe minimale;

$\in$ signifie «appartient à»;

q est la probabilité de l'événement;

l est le domaine d'indice des événements concernés;

$\lambda_i \cong C_{f,i}(t)$;

i est le domaine d'indice pour les EIH;

n_i est le nombre d'EIH dans toutes les coupes minimales.

NOTE Il convient de noter que le terme entre parenthèses dans l'expression (2) est une approximation de premier ordre pour l'indisponibilité due à l'état critique des FSE associés à l'EIH «i». Ce terme est la somme des probabilités des coupes minimales contenant l'EIH «i». L'expression (2) est généralement suffisamment exacte pour la plupart des calculs de risque et peut par conséquent être utilisée pour établir l'importance de la contribution des coupes minimales à la fréquence globale d'endommagement du cœur.

6.3.2.2 Importance pour l'évaluation de la sûreté

Si l'approche précédente est utilisée, l'importance pour la sûreté des FSE peut alors être déterminée en termes de fonctions de pondération qui évaluent la contribution de chacun des événements de base (et par conséquent les conditions de défaillances potentielles des FSE correspondants qui les composent) à la fréquence globale d'endommagement du cœur. Le développement d'une expression d'importance pour une fonction, et/ou les systèmes et équipements associés par lesquels elle est mise en œuvre, implique trois étapes:

a) l'établissement d'un nouvel événement sommet d'endommagement du cœur qui est l'union booléenne des coupes minimales contenant l'EIH ou l'événement concerné;

b) l'utilisation de l'expression (1) pour calculer la fréquence d'occurrence de ce nouvel événement sommet (pour les expressions de l'importance des EIH, un seul événement est utilisé comme événement initiateur pour le nouvel événement sommet);

c) diviser la fréquence d'occurrence résultante par la fréquence d'endommagement du coeur.

Exprimée mathématiquement, l'importance pour la sûreté des événements de base (ou des FSE dont ils sont constitués) pondérée par la fréquence d'endommagement du cœur est:

$$IEC = \frac{\text{Fréquence de l'union booléenne des coupes minimales contenant les événements intéressants}}{\text{Fréquence d'occurrence de l'événement sommet, C(t)}}$$

En conséquence, l'importance pour la sûreté est donnée simplement par la contribution relative des coupes minimales (contenant l'EIH ou l'événement concerné) à la fréquence totale d'endommagement du cœur. Dans de nombreux cas d'évaluation du risque, C(t) peut être pris comme une constante ou peut être représenté comme une constante selon le degré d'exactitude nécessaire pour établir un ordre raisonnable d'importance. Dans ce modèle de classement, il convient de noter que le numérateur est une fonction linéaire de la fréquence de défaillance des EIH. Pour les événements concernés, le numérateur est une fonction linéaire de l'indisponibilité de ces événements. Sur le plan conceptuel, l'importance des événements concernés (ou pivots) est une mesure constituante de l'importance dans la mesure où les événements ne provoquent pas l'occurrence de l'événement sommet (ici l'endommagement du cœur).

where

j is the domain of index for the minimal cut sets;

K_j is the jth minimal cut set;

$\in$ means “belongs to”;

q is the event probability;

l is the domain of index of PIE;

$\lambda_i \cong C_{f,i}(t)$

i is the domain of index for PIEs;

n_i is the number of PIEs in all of the minimal cut sets.

NOTE That the parenthetical term in expression (2) is a first order approximation for the critical state unavailability of the FSEs associated with PIE “i”. This term is the sum of the minimal cut set probabilities containing the PIE “i”. Expression (2) is generally accurate enough for most risk calculation and can therefore be used for establishing the importance of minimal cut set contribution to the overall frequency of core damage.

6.3.2.2 Importance to safety evaluation

If the above approach is employed, then the importance to safety of FSEs can be determined in terms of weighting functions which assess the contribution of each of the basic events (and thereby the postulated failure conditions of the corresponding FSEs of which they are constructed) to the overall frequency of core damage. The development of an importance expression for a function, and/or the associated systems and items of equipment by which it is implemented, involves three steps:

a) the formation of a new core damage top event that is the Boolean union of the minimal cut sets containing either the PIE or enabling event;

b) the use of expression (1) to compute the frequency of occurrence of this new top event (for PIE importance expressions, only one event can function as an initiating event for the new top event);

c) divide the resulting frequency of occurrence by the core damage frequency.

Stated mathematically, the importance to safety for basic events (or the FSEs of which they are constructed) as weighted to the core damage frequency is:

$$\text{ICD} = \frac{\text{Frequency of the Boolean union of the minimal cut sets containing the events of interest}}{\text{Top event occurrence frequency, C(t)}}$$

Therefore the importance to safety is simply given by the fractional contribution of the minimal cut sets (containing either the PIE or the enabling event) to the total core damage frequency. In many cases, in a risk assessment, C(t) can be taken to be a constant to the degree of accuracy necessary to establish reasonable importance rankings. In this ranking scheme, it should be noted that the numerator is a linear function of the failure frequency for PIEs. For enabling events, the numerator is a linear function of the enabling event unavailability. Conceptually, enabling (or pivotal) event importance is a contributing measure of importance since enabling events do not cause the occurrence of the top event (in this case core damage).

6.3.3 Affectation à une catégorie

Sur la base des importances dérivées de l'analyse précédente, les FSE d'instrumentation et de contrôle-commande peuvent être affectés aux catégories de classement conformément à une échelle d'importance. Il s'avère qu'une échelle logarithmique est la plus appropriée (bien que d'autres échelles puissent être utilisées). Par exemple, il convient que

- un FSE de CC soit affecté à la catégorie A si son importance calculée est $1,0 > I \geq 0,01$;
- un FSE de CC soit affecté à la catégorie B si son importance calculée est $0,01 > I \geq 0,001$;
- un FSE de CC soit affecté à la catégorie C si son importance calculée est $0,001 > I \geq 0,0001$.

6.3.4 Procédure de classement

En utilisant la méthode décrite dans les paragraphes précédents de 6.3, les fonctions de CC peuvent être classées selon leur importance. La majorité des phases de conception d'une centrale nucléaire incluent des cycles itératifs pendant l'étude des options de conception. Pendant ces cycles, les exigences en matière de CC sont progressivement affinées et les fonctions individuelles deviennent plus ou moins importantes pour la sûreté. Cette procédure est décrite ci-après.

6.3.4.1 Identification de la base de conception

L'une des entrées principales du processus de classement des FSE est la nature de la centrale nucléaire et le type de réacteur (par exemple PWR, BWR ou autre type de réacteur), les EIH associés et les principaux critères de conception sur la redondance des systèmes et équipements mécaniques et électriques. Une autre entrée principale est l'identification des principaux FSE de mitigation ainsi que leurs FSE supports, pour chaque EIH.

L'affectation des FSE aux catégories dépend de leur rôle en matière de prévention ou de mitigation des EIH. Le processus de classement exige de tenir compte du rôle des FSE dans la prévention et la mitigation des EIH dans tous les modes de fonctionnement et états de la centrale (par exemple démarrage, fonctionnement normal, rechargement), dans la mesure où les FSE peuvent jouer un rôle important uniquement dans certains modes de fonctionnement et, également des EIH, tels que les catastrophes naturelles (par exemple perturbations sismiques, inondations, vents extrêmes, foudre) et les dangers (par exemple incendies, inondations internes, missiles, rejets radioactifs de la centrale nucléaire adjacente).

6.3.4.2 Identification et classement des FSE

A un stade précoce de la conception d'une centrale nucléaire, il faut identifier les fonctions ayant un rôle de sûreté. Il est recommandé que le processus d'identification de ces fonctions et d'affectation aux FSE de CC ou aux opérateurs humains soit effectué conformément à la CEI 60964. Suite à cette identification initiale des FSE, il convient d'affecter une catégorie à chaque FSE.

Il ne sera pas possible d'identifier en détail tous les FSE à un stade précoce du processus de conception, dans la mesure où les caractéristiques de la centrale nucléaire n'auront pas encore été complètement définies. Il faut, en conséquence, que le processus d'identification et de classement des FSE continue d'une manière itérative pendant toute la phase de conception. Lorsque l'affectation initiale des FSE à une catégorie est incertaine, il convient d'ajouter une note explicative au classement. Il convient que les fonctions effectuées par chaque système de CC soient analysées afin d'identifier les sous-FSE au sein des FSE et d'affecter la catégorie appropriée à chaque sous FSE.

Dans la mesure où les FSE individuels peuvent être impliqués dans la mise en œuvre de plusieurs aspects des spécifications, le processus d'affectation peut engendrer l'affectation des FSE à plusieurs catégories. En cas d'affectations multiples, il convient que l'affectation finale de chaque FSE et de tous les sous-FSE soit la catégorie applicable la plus élevée.

6.3.3 Category assignment

Based upon the importances derived from the above analysis, instrumentation and control FSE can be assigned to classification categories in accordance to a scale of importance. A logarithmic scale has been found to be most appropriate (although other scales could be used). For example,

- an I&C FSE should be assigned to category A if its calculated importance is $1,0 > I \geq 0,01$;
- an I&C FSE should be assigned to category B if its calculated importance is $0,01 > I \geq 0,001$;
- an I&C FSE should be assigned to category C if its calculated importance is $0,001 > I \geq 0,0001$.

6.3.4 Classification procedure

Using the method described in the preceding subclauses of 6.3, I&C functions can be classified according to their importance. Most NPP design phases contain iterative cycles while plant design options are studied. During these cycles, the I&C requirements are progressively refined and individual functions become more or less important to safety. This procedure is described below.

6.3.4.1 Identification of design basis

A main input to the FSE categorization process is the nature of the NPP and the reactor type (e.g. PWR, BWR or other reactor type), the associated PIEs, and the major design criteria on redundancy of mechanical and electrical systems and equipment. Another main input is the identification of the major mitigating FSEs, and their supporting FSEs, for each PIE.

The assignment of FSE to categories depends upon their role in preventing or mitigating PIEs. The categorization process requires consideration of the role of the FSE in preventing and mitigating PIEs in all operating modes and plant conditions (e.g. start-up, normal operation, refuelling), as an FSE may have a significant role in some operating modes only, and also following PIEs such as natural events (e.g. seismic disturbance, flood, extreme wind, lightening) and hazards (e.g. fire, internal flood, missiles, radioactive release from adjacent NPP).

6.3.4.2 Identification and categorization of FSE

At an early stage in the design of the NPP, functions with a safety role must be identified. The process of identifying these functions and assigning them to the I&C FSE or to the human operators should be performed according to IEC 60964. Following this initial identification of FSE, a category should be assigned for each FSE.

It will not be possible to identify in detail all the FSE at an early stage in the design process, as the characteristics of the NPP will not then have been defined fully. The process of identification and categorization of the FSE must therefore continue iteratively throughout the design phase. Where an initial assignment of a FSE to a category is uncertain, then an explanatory note should be added to the categorization. The functions performed by each I&C system should be reviewed, to identify the sub-FSE within the FSE and to assign the appropriate category to each sub-FSE.

Since individual FSE may be involved in the implementation of several aspects of the requirements specification, the assignment process may result in some FSE being assigned to several categories. In the case of multiple assignment, the final assignment of each FSE and all sub-FSE should be to the highest applicable category.

Dans la mesure où les exigences en matière de redondance, diversité et autres aspects techniques des FSE sont déterminés d'une manière plus précise, par exemple au fur et à mesure que l'analyse de la sûreté progresse et que les procédures opérationnelles sont développées, la liste de classement est affinée et revue afin d'aboutir à une liste finale. Il convient que cette liste soit incluse dans la documentation requise pour obtenir et conserver la licence d'exploitation de la centrale nucléaire.

6.3.5 Détermination des exigences

Les exigences techniques et de qualité spécifiques aux FSE qui ont été affectés aux catégories A, B et C en utilisant l'approche probabiliste susmentionnée sont présentées dans la CEI 61226.

6.4 Approche 3: approche basée sur les conséquences et la mitigation

6.4.1 Historique de l'approche probabiliste

Au Canada, la conception des centrales nucléaires CANDU est basée sur une approche probabiliste ou des objectifs probabilistes, depuis les premières centrales prototypes conçues dans les années 50 et 60 jusqu'à la dernière conception CANDU. L'objectif probabiliste pour les premières centrales CANDU était exprimé en termes de fréquence inférieure à 10^{-5} événement par an pour un accident sérieux. Avec une fréquence de défaillance de un en trois ans supposée pour la défaillance des systèmes en fonctionnement normal conçus selon les normes industrielles de l'époque, les principaux systèmes de mitigation assurant la prévention des rejets (arrêt, refroidissement de secours du cœur) et ceux qui contiennent les produits de fission (confinement) devaient chacun avoir une «défiabilité» d'environ un jour par an, ce qui représente une indisponibilité de 3×10^{-3}.

6.4.2 Objectif probabiliste actuel

Les considérations précédentes sont devenues la base des objectifs actuels de fiabilité de 10^{-3} pour l'indisponibilité des principaux systèmes de mitigation (soient deux systèmes d'arrêt, le système de refroidissement de secours du cœur et le système de confinement), ce qui est une exigence réglementaire. Cela signifie que les principaux systèmes de mitigation empêcheraient un rejet majeur avec l'objectif d'une fréquence d'environ 10^{-6} événement par an (à savoir deux systèmes de mitigation ayant une indisponibilité de 10^{-3} chacun), ce qui devient dans la pratique un objectif de conception. C'est la base de l'objectif actuel des évaluations probabilistes de sûreté, avec l'application d'une autre marge d'analyse de 10^{-7} événement par an pour la perte des systèmes importants pour la sûreté engendrant un rejet supérieur aux limites de dose réglementaires pour les événements individuels.

Pour la plage de fréquences de 10^{-1} à 10^{-6} événement par an, un certain nombre de limites de dose réglementaire est appliqué pour caractériser la conséquence, la limite augmentant au fur et à mesure que la fréquence de l'événement diminue. Il convient de noter que les limites de dose réglementaire sont liées aux événements initiateurs dans une plage de fréquences particulière estimée, et non pas directement à la plage de fréquences.

6.4.3 Classement des systèmes importants pour la sûreté

Les systèmes et composants requis pour assurer des fonctions «de protection» (ou de mitigation) pour garantir l'objectif probabiliste décrit ci-dessus sont classés comme systèmes importants pour la sûreté. Différents types de systèmes de mitigation peuvent avoir différents objectifs d'indisponibilité, selon leur fonction de sûreté.

As the redundancy, diversity and other technical requirements of the FSE are determined more exactly, for example as the safety analysis progresses and the operating procedures are developed, the categorization list is refined and revised, to derive a final list. This list should be included in the documentation that is required to obtain and maintain the NPP operating license.

6.3.5 Determination of requirements

The specific technical and quality requirements for FSEs that have been assigned to categories A, B, and C using the probabilistic approach presented above are given in IEC 61226.

6.4 Approach 3: consequence – mitigation based approach

6.4.1 Historical probabilistic approach

In Canada, the design of the CANDU nuclear power plants has had a probabilistic basis, or risk target approach, from the early prototype plants designed in the 1950's and 1960's through to the latest CANDU design. The risk target for the earliest CANDU plants was expressed as a frequency of less than 10^{-5} events per year for a serious accident. With a failure frequency of one in three years assumed for failure of normally operating systems designed to normal industrial standards at that time, the major mitigating systems that prevented release from the fuel (shutdown, emergency core cooling) and those which contained the fission products (containment), were each required to have an "unreliability" of about one day per year which is an unavailability of 3×10^{-3}.

6.4.2 Current probabilistic target

The considerations outlined above became the basis for the current reliability targets of 10^{-3} for the unavailability of the major mitigating systems (defined as two shutdown systems, the emergency core cooling system, and the containment system), which is a regulatory requirement. This means that the major mitigating systems would prevent a major release with a frequency of about 10^{-6} events per year (i.e. two mitigating systems having an unavailability of 10^{-3} each), which becomes in practice a target for the design. This is the basis for the current probabilistic safety assessment target, with a further analysis margin applied, of 10^{-7} events per year for loss of safety related systems leading to a release exceeding the regulatory dose targets, for individual events.

For the frequency range from 10^{-1} to 10^{-6} events per year, a number of regulatory dose limits are applied to characterize the consequence, with the limit becoming larger as the frequency of the event becomes smaller. It should be noted that the regulatory dose limits are associated with initiating events within a particular estimated frequency range, and not directly to the frequency range.

6.4.3 Safety related system classification

The systems and components needed to perform "protective" (or mitigating) functions to satisfy the probabilistic target described above are classified as safety related systems. Different types of mitigating systems may have different unavailability targets, depending on their safety function.

Les systèmes les plus importants sont ceux qui doivent effectuer des fonctions de sûreté dans un court délai pour éviter les conséquences graves et sont appelés «systèmes de sûreté spéciaux». Ils sont constitués de deux systèmes d'arrêt, du système de refroidissement de secours du cœur et du système de confinement. Des exigences de conception très strictes sont applicables à ces systèmes, y compris un ensemble détaillé d'exigences de conception définies par l'organisme réglementaire, l' «Atomic Energy Control Board». Les objectifs d'indisponibilité de 10^{-3} pour chacun des systèmes de sûreté spéciaux sont inclus dans ces exigences.

Les systèmes qui assurent des fonctions support essentielles aux systèmes de sûreté spéciaux (par exemple la puissance électrique et l'eau de refroidissement pour les échangeurs et pompes de refroidissement de secours du cœur) font également l'objet d'une exigence d'indisponibilité spécifiée, issue de l'objectif d'indisponibilité des systèmes de sûreté spéciaux. Cette exigence dicte le niveau de redondance, la diversité, la protection contre les événements de cause commune (par exemple incendies, inondations, tremblements de terre, etc.) à prévoir dans la conception du système. Les exigences applicables aux autres systèmes qui effectuent une fonction de sûreté de mitigation à plus long terme sont définies d'une manière similaire, sur la base de la redondance de la fonction effectuée, en tenant compte de l'évaluation probabiliste de sûreté.

En reconnaissant que l'événement initiateur peut également jouer un rôle dans l'atteinte de l'objectif probabiliste global, les systèmes de fonctionnement normal dont la défaillance pourrait engendrer un rejet supérieur aux limites réglementaires (en l'absence d'une autre action de mitigation) sont également classés comme systèmes importants pour la sûreté. Ces systèmes peuvent n'avoir aucune fonction de mitigation et incluent les systèmes qui effectuent des fonctions de sûreté pour maintenir la centrale dans un état normal (par exemple arrêt normal, contrôle de la réactivité, refroidissement du combustible, surveillance de la centrale). Ce classement signale aux concepteurs de ces systèmes que le système joue un rôle dans l'atteinte des objectifs de dose pour la centrale et que pour y parvenir des exigences de conception particulières peuvent être applicables. Dans la mesure où le fonctionnement continu de ces systèmes empêche l'apparition d'un accident, il est dit qu'ils effectuent une fonction de sûreté «préventive». Le rôle spécifique attribué à chaque système est identifié dans la documentation des règles de conception de sûreté, issue des analyses de sûreté traditionnelles et des évaluations probabilistes de sûreté. La fréquence de défaillance de ces systèmes est déterminée par l'analyse des arbres de défaillance, en général sans spécification d'objectif d'indisponibilité particulier pour la conception. La défaillance de l'un de ces systèmes importants pour la sûreté devient l'événement initiateur d'une séquence accidentelle.

Pour résumer l'approche ci-dessus, les types de systèmes importants pour la sûreté prévus dans une centrale CANDU sont, par ordre d'importance de sûreté,

a) les systèmes de sûreté spéciaux, avec un objectif d'indisponibilité donné de 10^{-3};

b) les systèmes support de sûreté, avec un objectif d'indisponibilité déterminé à partir de ce qui précède;

c) les autres systèmes importants pour la sûreté ayant une fonction de «protection» ou de mitigation, avec un objectif d'indisponibilité basé sur les EPS;

d) les autres systèmes importants pour la sûreté ayant une fonction de sûreté «préventive», ayant ou non un objectif d'indisponibilité donné (les systèmes de contrôle et de surveillance en continu utilisés pour connaître l'état de ces systèmes sont un autre sous-ensemble de cette catégorie. Ils ne sont cependant pas classés comme importants pour la sûreté, dans la mesure où ils ne jouent pas un rôle direct dans la fonction de sûreté définie).

Les exigences de conception sont définies sur une base propre au système afin de garantir les fonctions de sûreté définies pour chaque système et d'atteindre les objectifs de fiabilité identifiés pour les systèmes individuels. Les exigences les plus strictes sont appliquées aux systèmes de sûreté spéciaux qui ont les objectifs d'indisponibilité les plus élevés et effectuent une fonction de sûreté importante dans un délai court.

The most important systems are those which must perform immediate safety functions to avoid serious consequences, and are called “special safety systems”. They consist of two shutdown systems, the emergency core cooling system, and the containment system. These systems have very stringent design requirements associated with them, including a detailed set of design requirements defined by the regulatory agency, the Atomic Energy Control Board. Included in these requirements are the unavailability targets of 10^{-3} for each of the special safety systems.

Systems which provide essential support services to the special safety systems are called safety support systems (e.g. electrical power and cooling water to the emergency core cooling heat exchangers and pumps), and also have a specified unavailability requirement derived from the special safety system unavailability target. This requirement dictates the degree of redundancy, diversity, protection from common cause events (e.g. fires, floods, earthquakes, etc.), provided in the system design. Requirements for other systems which provide a mitigating safety function in the longer term are defined in a similar fashion, based on the redundancy of the function provided, with input from the PSA.

In recognition of the fact that the initiating event can also play a role in meeting the overall probabilistic target, normally operating systems whose failure could lead to a release exceeding regulatory limits (in the absence of further mitigating action) are also classified as safety related systems. These systems may have no mitigating function, and include the systems that perform safety functions to maintain the plant in a normal condition (e.g. normal shutdown, reactivity control, fuel cooling, plant monitoring). This classification signals to the designers of these systems that the system has a role in meeting the dose targets for the plant, and that special design requirements to achieve this may be applicable. Since the continued operation of these systems prevents the occurrence of an accident, they are said to perform a preventative safety function. The specific role credited for each system is identified in safety design documentation, derived from traditional safety analyses and from the probabilistic safety assessment. The failure rate of these systems is determined by fault tree analysis, generally with no specific unavailability target being specified for the design. The failure of one of these safety related systems becomes the initiating event for an accident sequence.

To summarize the above approach, the types of safety related systems provided in a CANDU plant are, in order of importance or safety significance,

a) special safety systems, having a defined unavailability target of 10^{-3};

b) safety support systems, having a defined unavailability target derived from the above;

c) other safety related systems having a protective or mitigating safety function, with an unavailability target based on PSA;

d) other safety related systems having a preventative safety function, which may or may not have a defined unavailability target (a further subset of this category are the testing and monitoring systems used to determine the condition of these systems on an ongoing basis, but these are not classified as being safety related, as they do not play a direct role in the defined safety function).

Design requirements are defined on an individual system basis to support the defined safety function(s) for each system, and to satisfy the reliability targets identified for the individual systems. The most stringent requirements are applied to the special safety systems, which have the most demanding unavailability targets and perform an immediate and significant safety function.

6.4.4 Application des exigences de conception

Dans le passé, on pensait que des ensembles normalisés d'exigences de conception pourraient être développés sur la base de «l'importance pour la sûreté» d'un système de sûreté et que l'objectif de fiabilité déterminé pour le système pourrait d'une certaine manière être utilisé pour choisir un ensemble approprié d'exigences. Cependant, cela s'est, jusqu'à présent, avéré impossible pour les centrales CANDU, hormis dans très peu de cas isolés, comme cela est indiqué ci-après. Au lieu de cela, les exigences de conception de chaque système important pour la sûreté sont développées sur la base de l'importance pour la sûreté du type de système (décrits ci-dessus), du jugement et de l'expérience des concepteurs et spécialistes de sûreté, et des résultats des analyses de sûreté et EPS. Les objectifs de fiabilité des EPS (à savoir l'indisponibilité) sont utilisés pour développer des exigences spécifiques en matière de redondance, diversité et protection contre les événements de cause commune.

Un récent exemple de l'utilisation des critères probabilistes dans la sélection des exigences de conception basées sur le concept de l'importance pour la sûreté et les objectifs probabilistes se situe dans le domaine de la conception des logiciels informatiques. Dans cette application, les étapes suivantes sont respectées:

a) la fonction de sûreté du système pour lequel le logiciel est requis est définie, sur la base du type de système, comme cela est indiqué en 6.4.3;

b) «l'importance pour la sûreté» du système est définie comme «élevée», «moyenne» ou «faible», sur la base de la fonction de sûreté et l'indisponibilité requise pour le système (en utilisant l'exigence réglementaire applicable aux systèmes de sûreté spéciaux, ou l'exigence issue des EPS pour la fréquence des événements initiateurs ou l'indisponibilité du système de mitigation);

c) l'impact de la défaillance du logiciel sur la fonction de sûreté est défini; à savoir, le type I provoquerait la défaillance de la fonction de sûreté, le type II provoquerait une dégradation de la capacité du système (par exemple redondance, surveillance, contrôle) mais non la défaillance de la fonction de sûreté requise, et le type III n'affecterait pas la fonction de sûreté du système;

d) une matrice relative à l'importance pour la sûreté et à l'impact de la défaillance du logiciel est utilisée pour sélectionner l'un des quatre différents niveaux d'exigences de conception du logiciel.

Dans cette application, le niveau le plus élevé des exigences relatives au logiciel est appliqué aux systèmes les plus importants pour la sûreté (systèmes de sûreté spéciaux), ou à d'autres systèmes importants pour la sûreté (tels que les systèmes de prévention) ayant une très faible fréquence de défaillance (fréquence des événements initiateurs), lorsque la défaillance du logiciel provoquerait directement la défaillance de la fonction de sûreté requise. Le niveau le plus faible de l'exigence relative au logiciel (par exemple exigences commerciales standards) serait appliqué au logiciel qui n'a aucun effet sur la fonction de sûreté du système, même pour un système important pour la sûreté. Des niveaux d'exigences de conception plus sévères peuvent être appliquées au logiciel sur la base de la perte économique potentielle découlant d'une défaillance du logiciel.

6.4.5 Conclusions de l'approche 3

Ce qui précède montre que les critères probabilistes peuvent et devraient être utilisés dans la sélection des exigences de conception des systèmes importants pour la sûreté. Cependant, il faut, pour le développement de ces exigences qui est un processus très complexe, tenir compte des exigences réglementaires, de l'objectif probabiliste global pour la centrale, de la fonction de sûreté spécifique du système, des objectifs de fiabilité pour le système et le composant particulier, du nombre de systèmes effectuant la fonction de sûreté et de l'impact de l'instrumentation ou du logiciel sur la fonction de sûreté. En raison du nombre de variables impliquées dans ce processus, il serait très difficile de développer un processus normalisé pour parvenir à un ensemble prédéfini d'exigences de conception qui seraient applicables au niveau de la conception du composant. Cependant, l'expérience dans la conception de la centrale CANDU montre que les résultats des analyses probabilistes peuvent être systématiquement et effectivement incorporés dans le processus de conception globale d'une centrale.

6.4.4 Application of design requirements

In the past, it was felt that standardized sets of design requirements could be developed based on the safety importance of a safety related system, and that the reliability target set for the system could somehow be used to select the appropriate set of design requirements. However, this has so far been found to be impractical for CANDU plants, except in a very few isolated cases, as described below. Instead, design requirements for each safety related system are developed based on the general safety significance of types of systems (described above), the judgement and experience of the designers and safety analysts, and the results of safety analysis and PSA. The PSA reliability targets (i.e. unavailability) are used to develop specific requirements for redundancy, diversity, and protection from common cause events.

One recent example of the use of probabilistic criteria in the selection of design requirements based on the concept of safety significance and probabilistic targets is in the area of computer software design. In this application, the following steps are followed:

a) the safety function of the system for which the software is required is defined, based on the system type as outlined in 6.4.3;

b) the safety significance of the system is defined as “high”, “medium”, or “low”, based on the safety function and the required unavailability of the system (using the regulatory requirement for special safety systems, or the PSA derived requirement for the initiating event frequency or the mitigating system unavailability);

c) the impact of the failure of the software on the safety function of the system is defined; that is, type I would cause failure of the safety function, type II would cause a degradation of the system capability (e.g. redundancy, monitoring, testing) but not failure of the required safety function, and type III would have no effect on the safety function of the system;

d) a matrix of the safety significance and the impact of software failure is used to select one of four different levels of software design requirements.

In this application, the highest level of software requirements are applied to the most important safety related systems (special safety systems), or to other safety related systems (such as preventative systems) having a very low credited failure rate (initiating event frequency), where failure of the software would directly cause failure of the required safety function. The lowest level of software requirement (e.g. standard commercial requirements) would be applied to software that has no effect on the safety function of the system, even though the system is safety related. Higher levels of the software design requirements may be applied to software based on the potential economic loss that could occur due to software failure.

6.4.5 Conclusions from approach 3

The above shows that probabilistic criteria can and should be used in the selection of design requirements for safety related systems. However, the development of the design requirements is a very complex process, which must take into consideration regulatory requirements, the overall probabilistic target for the plant, the particular safety function of the system, the reliability targets for the system and the particular component, the number of systems performing the safety function, and the impact of the instrumentation or software on the safety function. Due to the number of variables involved in this process, it would be very difficult to develop a standardized process to come up with a predetermined set of design requirements that would be applicable at the component design level. However, the experience in CANDU plant design does indicate that the results of probabilistic analyses can be systematically and effectively incorporated in the overall plant design process.

6.5 Approche 4: approche basée sur la défense en profondeur

6.5.1 Introduction

L'objectif d'une méthode de classement efficace est de pouvoir établir des exigences générales applicables aux FSE. Ces exigences contribuent alors à l'assurance que les FSE donnés seront disponibles pour effectuer la fonction spécifiée pendant une durée précise avant, pendant ou après un EIH. La CEI 61226 tient uniquement compte de la fonction effectuée, sans considérer la fiabilité requise de cette fonction ou l'existence éventuelle d'autres fonctions qui permettent de compenser la perte d'une fonction donnée. Une méthode de classement qui tient compte des facteurs quantitatifs permettra de positionner plus correctement les FSE vis-à-vis de l'importance pour la sûreté.

La méthode de classement présentée dans ce paragraphe considère trois facteurs, à savoir: la défense en profondeur, la fiabilité et le temps.

Défense en profondeur: le concept de défense en profondeur est basé sur la philosophie de l'AIEA en matière de sûreté. Bien que le concept AIEA de défense en profondeur possède cinq échelons, seuls trois d'entre eux sont pris en considération pour l'équipement de CC, les autres étant associés aux plans d'évacuation, etc. Les échelons qui seront utilisés ici sont «prévention, achèvement, et mitigation».

Fiabilité: il est possible d'établir un objectif de fiabilité pour chaque FSE. Dans ce cas, il convient de prendre en compte les conséquences de la perte de la fonction. De plus, la prise en compte de l'existence d'autres caractéristiques pouvant mitiger la perte de la fonction peut réduire l'objectif de fiabilité d'un FSE donné. L'objectif peut être déterminé par des EPS. Pour certaines fonctions, il peut ne pas être pratique de déterminer un objectif chiffré. En conséquence, les objectifs sont divisés en trois niveaux. Il est recommandé que les limites entre ces niveaux soient déterminées par le concepteur du système; ils peuvent varier d'un pays à l'autre, voire même entre les centrales d'un même pays. Les éléments suivants sont donnés à titre indicatif et peuvent être utilisés comme lignes directrices.

Elevé	probabilité de défaillance sur demande < 10^{-4}
Moyenne	probabilité de défaillance sur demande de 10^{-4} à 10^{-2}
Faible	probabilité de défaillance sur demande > 10^{-2}

Pour les fonctions continues, il convient que la défaillance sur demande soit remplacée par la défaillance par unité de temps. Par ailleurs, pour certaines fonctions de sûreté, il est nécessaire d'avoir une fiabilité très élevée, de l'ordre de 10^{-6} défaillance par demande. Pour parvenir à une fiabilité aussi élevée, il est en général nécessaire de prévoir plusieurs fonctions diversifiées. Chacune de ces fonctions aura un objectif de fiabilité élevé et l'indépendance entre elles sera évaluée pour assurer le respect de l'objectif de fiabilité très élevé. La fiabilité n'inclut pas uniquement les éléments quantitatifs tels que la redondance, la fréquence de défaillance et l'intervalle des essais, mais également les éléments qualitatifs qui apportent une garantie du nombre quantitatif évalué. Ces éléments qualitatifs incluent l'indépendance et l'étendue de la vérification de la conception, la qualification du personnel impliqué dans la conception et la maintenance des FSE, la perfection des programmes d'assurance qualité des organisations impliquées dans les FSE, etc.

Temps: Le temps est également un facteur important dans la fiabilité d'une fonction. Pour des actions à court terme pour lesquelles l'intervention des ressources humaines n'est pas possible, un degré de fiabilité plus élevé des fonctions automatiques est nécessaire. Pour les actions à moyen terme, pour lesquelles l'opérateur humain, s'il possède les moyens adéquats, peut prendre des mesures planifiées à partir des stations de contrôle-commande de fonctionnement normal, une dépendance plus faible des fonctions automatiques peut être considérée. Enfin, les actions à long terme, qui prévoient la planification et l'exécution d'actions alternatives en cas d'indisponibilité ou de non-efficacité des actions planifiées, conduiront à une fiabilité minimale des FSE considérés. Le temps n'est pas nécessairement mesuré à partir du début d'un événement. Par exemple, une action minutée avec précision peut être requise plusieurs heures ou jours après l'événement initiateur. Cependant, lorsque cette action est nécessaire, il n'existe aucune chance de se remettre de sa défaillance. Cela peut placer le temps d'action requis dans la gamme la plus courte.

6.5 Approach 4: defence-in-depth based approach

6.5.1 Introduction

The purpose of an effective classification scheme is to allow general requirements to be established for FSE. These requirements then contribute to the assurance that the given FSE will be available to perform its specified function for a specified period of time before, during or after a PIE. IEC 61226 only considers the function performed without regard to the required reliability of that function or the potential existence of other functions to offset the loss of a given function. A classification scheme that considers quantitative factors will allow the FSE to be more correctly placed in its relative place of importance to safety.

The classification scheme presented in this subclause considers three factors, namely defence in depth, reliability and time.

Defence-in-depth: defence-in-depth has a basis in IAEA safety philosophy. While the IAEA concept of defence-in-depth has five echelons, only three echelons are considered for the I&C equipment, the others being associated with evacuation plans, etc. The echelons that will be used here are “prevention, termination and mitigation”.

Reliability: it is possible to establish a reliability target for every FSE. In doing this, the consequences of the loss of the function should be taken into consideration. Also, consideration of the existence of other features which may mitigate the loss of the function may reduce the reliability target for a given FSE. The target might be assigned as a result of a PSA study. For some functions, it may not be practical to determine a specific target number. Therefore, the targets are divided into three ranges. The boundaries between these ranges should be determined by the system designer and may vary from country to country, or even between nuclear power plants within a country. The following are given as an example and may be used for guidance.

High	$<10^{-4}$ probability of failure on demand
Moderate	10^{-4} to 10^{-2} probability of failure on demand
Low	$>10^{-2}$ probability of failure on demand

For continuous functions, failure on demand should be replaced by failures per unit of time. Furthermore, for certain safety functions, it is necessary to have very high reliability, on the order of 10^{-6} failures per demand. To achieve such very high reliability, it is generally considered necessary to provide multiple, diverse functions. Each of these functions would be placed in the high reliability target, and the independence between them evaluated to assure that the very high reliability goal is met. Reliability includes not only the quantitative elements such as redundancy, failure rate and test interval, but also the qualitative elements that give assurance to the quantitative number evaluated. Such qualitative elements include the independence and depth of the design verification, the qualification of the personnel involved in the design and maintenance of the FSE, the thoroughness of the quality assurance programmes of the organizations involved in the FSE, etc.

Time: time is also an important factor in the assurance of a function. For short action times, where human intervention is not possible, a higher degree of assurance for the automatic functions is necessary. For moderate action times, where the human operator, if provided with adequate means, may take preplanned actions from normal control stations, a lower dependence on the automatic functions can be taken. Finally, long action times, which allow for the planning and execution of alternative actions should the preplanned actions prove to be unavailable or ineffective will place the minimum reliance on any given FSE. Time is not necessarily measured from the beginning of the event. For instance, a precisely timed action may be required some hours or days after the initiating event. However, when that action is needed, there is no chance to recover from its failure. This may put the required action time in the shorter range.

6.5.2 Méthode de classement

Afin d'effectuer ce classement quantitatif, il faut que le concepteur détermine tout d'abord le rôle de la défense en profondeur pour chaque FSE. Sur la base de ce rôle, l'un des trois groupes: prévention, achèvement et mitigation peut être choisi. Chacun de ces groupes est décrit respectivement aux tableaux 4, 5 et 6.

Ensuite, il convient de déterminer l'objectif de fiabilité selon les niveaux élevé, moyen ou faible. Cet objectif sera utilisé comme axe horizontal des différentes grilles.

L'élément de temps requis pour l'action est considéré comme axe vertical. Les éléments de temps sont interprétés différemment en fonction de la grille choisie, comme cela est expliqué ci-après.

L'intersection de l'objectif de fiabilité et de l'élément de temps dans la grille choisie déterminera la catégorie de sûreté, à savoir A, B, C ou NS, pour ces FSE.

Groupe prévention

Les FSE qui préviennent l'apparition des EIH incluent les dispositifs de verrouillage importants pour la sûreté et les fonctions de limitation. Les fonctions de contrôle-commande en fonctionnement normal dont la défaillance pourrait constituer un EIH sont également incluses. Il faut que les fonctions qui répondent à une perturbation dans un autre équipement soient affectées au groupe d'action à court terme. Les exemples d'actions à court terme sont la réduction de la puissance requise suite à une perte partielle de l'eau alimentaire normale. Les fonctions de contrôle-commande de régulation en fonctionnement normal des paramètres de centrale sont placées dans le groupe d'action intermédiaire. Enfin, les FSE dont l'objectif est de surveiller les conditions de fonctionnement de la centrale pour garantir qu'elles sont dans les limites des analyses de sûreté sont dans le groupe d'action à long terme.

Si ces fonctions de surveillance étaient défaillantes, une durée considérable serait probablement nécessaire à l'opérateur pour rétablir les conditions souhaitées. La grille du groupe "prévention" des FSE est présentée ci-après dans le tableau 4.

Tableau 4 – Prévention

Elément de temps	Objectif de fiabilité		
	Elevé	Moyen	Faible
Répondre à la défaillance	A	B	C
Contrôler la défaillance	B	C	NS
Conserver les conditions antérieures à l'événement	C	NS	NS

Groupe achèvement

Le groupe achèvement est le plus connu. Il inclut la plupart des fonctions des systèmes de sûreté classiques, telles que l'arrêt automatique du réacteur (arrêt d'urgence du réacteur), apport d'eau alimentaire supplémentaire et isolement des voies défectueuses. Cette grille ne comprend que deux groupes d'éléments de temps. Les actions qui doivent être prises immédiatement après la détection de l'EIH sont classées dans le groupe d'action à court terme. Les actions manuelles, disponibles en support des fonctions automatiques, sont placées dans le groupe d'action à plus long terme. La limite de temps entre ces groupes est soumise aux réglementations de divers pays. De nombreux pays considèrent que l'action de l'opérateur n'intervient que 30 min après l'événement. A noter que, compte tenu de l'incertitude de la fiabilité des actions humaines, les FSE manuels ne sont pas placés dans le groupe de l'objectif de fiabilité élevée.

6.5.2 The classification scheme

To perform this quantitative classification, the designer must first determine the defence-in-depth role for each FSE. Based on this role, one of the three groups, prevention, termination or mitigation can be selected, each of which is detailed in tables 4, 5 and 6 respectively.

Next, the reliability target should be determined to be in the high, moderate or low range. This target will be used for the horizontal axis of the selected grid.

Finally the time element required for action is determined for the vertical axis. Time elements are interpreted differently depending on the selected grid, as is explained below.

The intersection of the reliability target and time element in the selected grid will determine the safety category, i.e. A, B, C or NS, for that FSE.

Prevention group

FSE that prevent postulated initiating events include safety related interlocks and limitation functions. Also, control functions for normal operations whose failure would constitute a PIE are included. Functions which must respond to an upset in other equipment are assigned to the short action time group. Examples of such short times include the power reduction required following partial loss of normal feedwater. Control functions that normally regulate principle plant parameters are placed in the intermediate action time group. Finally, FSE whose purpose is to monitor the conditions of the plant to assure that they are within the boundaries of the safety analysis assumptions are in the long action time group.

Presumably, if these monitoring functions were to fail, the operator would have a considerable length of time to re-establish the desired conditions. The grid for the prevention group of FSE follows in table 4.

Table 4 – Prevention

Time element	Reliability target		
	High	Moderate	Low
Response to fault	A	B	C
Control failure	B	C	NS
Maintain pre-event conditions	C	NS	NS

Termination group

The termination group is the most familiar. It includes most of the classical safety system functions such as automatic reactor shutdown (scram), initiation of auxiliary feedwater and isolation of faulted lines. This grid has only two time element groups. For actions that must be carried out immediately on the detection of the PIE, the short action group is selected. Manual actions, if available to backup the automatic functions, will be in the longer action time group. The temporal dividing point between these groups is subject to the regulations of various countries. Many countries consider that operator action may not be taken for 30 min following an event. Note that given the uncertainty in establishing the reliability of human actions, no manual FSE are found in the high reliability target group.

Tableau 5 – Achèvement

Elément de temps	Objectif de fiabilité		
	Elevé	Moyen	Faible
Action automatique	A	A	B
Action humaine	–	A	C

Groupe mitigation

Les fonctions de mitigation prévoient en général la sécurité du public pendant de longues durées après l'apparition d'un EIH. Pour les FSE placés dans ce groupe, les actions à court terme comprennent les actions automatiques ou qu'il faut minuter avec précision en fonction de l'état de la centrale ou des évènements. Les actions à moyen terme comprennent les actions opérateur qui peuvent être engagées avec les ressources immédiatement disponibles. Les actions à long terme reflètent la possibilité de planifier et d'obtenir les ressources nécessaires pour accomplir la fonction. Ces actions à long terme peuvent inclure le soutien des organisations externes, telles que les pompiers municipaux fournissant de l'eau supplémentaire. Il convient que le point de séparation entre les actions à moyen terme et à long terme soit accepté par les organismes de réglementation du pays. Une valeur de 10 h est prise ici comme nombre indicatif. La grille de mitigation des FSE est présentée au tableau 6.

Tableau 6 – Mitigation

Elément de temps	Objectif de fiabilité		
	Elevé	Moyen	Faible
Action automatique	A	B	C
Action humaine à court terme <10 h	–	B	NS
Action humaine à long terme >10 h	–	C	NS

6.5.3 Combinaison des résultats

Une fonction donnée peut jouer des rôles multiples dans la défense en profondeur. Par exemple, elle peut prévenir un événement initiateur envisagé, mais peut aussi être requise pour terminer un autre événement différent. Dans ce cas, les plages des objectifs de fiabilité et de temps d'action peuvent être différentes selon le rôle. Il convient que la catégorie soit déterminée pour les divers rôles de la fonction, la catégorie la plus élevée étant ensuite affectée à la fonction.

Dès lors où toutes les fonctions ont été affectées à une catégorie, elles sont rassemblées en groupes et les systèmes et équipements associés sont affectés afin d'effectuer les fonctions. Les systèmes et équipements associés héritent de la catégorie la plus élevée des fonctions qu'ils effectuent. Il peut être possible d'affecter un composant donné au sein d'un système à une catégorie plus faible que le système dans son ensemble, à condition de pouvoir apporter la preuve qu'une indépendance suffisante est maintenue, de manière à ce que la défaillance de ce composant ne dégrade pas les parties du système qui effectuent des fonctions appartenant à une catégorie plus élevée. Par exemple, les équipements de communication qui indiquent l'état des systèmes d'arrêt du réacteur à l'opérateur peuvent être inclus dans une catégorie inférieure à celle des systèmes d'arrêt du réacteur eux-mêmes si une isolation adéquate est prévue dans l'interface entre les équipements de communication et les voies du système de sûreté.

Table 5 – Termination

Time element	Reliability target		
	High	Moderate	Low
Automatic action	A	A	B
Human action	–	A	C

Mitigation group

Mitigation functions generally provide for the safety of the public for extended periods after a PIE. For FSE in this group, the short action times are for automatic functions or actions which must be precisely timed in relation to plant status or events. Intermediate action times are for those operator actions that can be conducted with the resources readily available. Longer action times reflect the possibility of planning and procuring the necessary resources to accomplish the function. These long actions may include the support of external organizations, such as the town fire brigade supplying additional water. The dividing point between intermediate and long term actions should be agreed with the country's regulatory authority. A value of 10 h is taken here as an indicative number. The grid for mitigate FSE is presented in the table 6.

Table 6 – Mitigation

Time element	Reliability target		
	High	Moderate	Low
Automatic action	A	B	C
Short term human action <10 h	–	B	NS
Long term human action >10 h	–	C	NS

6.5.3 Combining the results

A given function may play multiple roles in the defence in depth. For instance, it may prevent one postulated initiating event, but be required to terminate a different event. In such cases, the reliability and action time target ranges may be different for each role. The category should be determined for the various roles of the function, and then the highest category assigned to the function.

Once all functions have been assigned a category, they are collected into groups, and associated systems and equipment are allocated to perform the functions. The associated systems and equipment inherit the highest category of the functions that they perform. It may be possible for a given component within a system to have a lower category than the overall system, provided it can be demonstrated that sufficient independence is maintained so that failure of that component will not degrade the portions of the system that carry out the higher category functions. For example, communications equipment that report the status of the reactor shutdown systems to the operator may be of a lower category than the reactor shutdown systems themselves if adequate isolation is provided in the interface between the communications equipment and the safety system channels.

Annexe A
(informative)

Proposition de modélisation du CC dans les EPS

A.1 Domaine d'application

La présente annexe décrit une proposition de modélisation du contrôle-commande (CC) dans les évaluations probabilistes de sûreté (EPS). En tenant compte des difficultés et des limites des études de sûreté de fonctionnement réalisées au sujet des dispositifs du CC automatiques, elle propose une modélisation simplifiée du CC.

A.1.1 Antécédents

Une EPS nécessite, pour l'évaluation quantitative de la fréquence de fusion du cœur (FFC), des valeurs représentant les défaillances des divers systèmes ou des missions humaines. La contribution du CC à la FFC peut être du même ordre de grandeur que celle des systèmes mécaniques, en conséquence une EPS a besoin de valeurs représentant le CC pour évaluer la conception globale et le niveau de sûreté. La priorité est bien entendu accordée aux systèmes automatiques de protection: le système principal de protection et les chaînes de réduction du risque, le cas échéant.

Des études de sûreté de fonctionnement sont réalisables de façon satisfaisante en se basant sur les défaillances simples des composants d'un système du CC donné, mais il apparaît que dans les systèmes complexes tels qu'un système de protection à quatre trains, certaines défaillances systématiques peuvent se produire et être dues à

- des erreurs fonctionnelles de conception ou de spécifications,
- des défauts de logiciels,
- des erreurs de modes opératoires.

Ces défauts sont des défaillances de cause commune affectant les voies redondantes d'un système du CC donné; il s'agit d'erreurs préexistantes non détectées. Elles ne dépendent pas du temps et elles peuvent être modélisées par une valeur donnée. Le principal problème dans l'établissement de ces valeurs réside dans le fait qu'aucun calcul analytique ou statistique ne peut apporter une aide quelconque.

La solution proposée dans la modélisation simplifiée du CC est basée sur des conventions d'experts concernant ces valeurs données, en fonction du niveau de qualité de chaque système du CC. Ce niveau de qualité inclut les règles d'évitement ou de tolérance des défaillances systématiques.

L'architecture matérielle dépend également du niveau de qualité requis.

A.1.2 Modélisation du CC dans les EPS

La modélisation simplifiée du CC pourrait être appliquée à la plupart des missions de sûreté du CC, néanmoins il convient d'être prudent. Dans l'état actuel de l'art, on ne peut l'utiliser que pour le système principal de protection et pour certains systèmes d'activation automatique, pour lesquels il a été établi.

Annex A
(informative)

Proposal for modelling I&C in PSA

A.1 Scope

This annex deals with a modelling proposal of I&C in the probabilistic safety assessments (PSA). Taking into account the difficulties and limits of dependability studies concerning I&C automatic control devices, it proposes a simplified modelling of I&C.

A.1.1 Background

For quantitative assessment of core melt frequency (CMF), PSA needs figures for the failure of various systems or human missions. I&C contribution to CMF might be of the same range as mechanical systems and so, PSA needs figures for I&C to evaluate the overall design and the safety level. The priority is of course for the automatic protection systems: main protection system and, if necessary, risk reduction channels.

Dependability studies are achievable for hardware single failures of components of a given I&C system, but it appears that in those complex systems such as a four-train protection system, some systematic failures could occur and be due to

- design or specification functional errors,
- software defaults,
- operating errors.

These faults are common cause failures of redundant trains of a given I&C system; they are pre-existing non detected errors. They do not depend on time and they can be modelled by a cut-off value. The main problem in establishing those figures is that no analytic or statistic calculation could help.

The solution proposed in the simplified I&C modelling is based on expert agreements on cut-off values, according to the level of quality of each I&C system. This level of quality includes rules for avoidance or tolerance on systematic failures.

Hardware architecture also depends of the required quality level.

A.1.2 I&C modelling in PSA

The simplified I&C modelling could be applied to most of I&C safety missions, but one has to be careful. The state of the art is to use it for the main protection system and for some other automatic activation channels, for which it has been built-up.

La pertinence de ce type de modélisation pour les missions du CC liées à l'action humaine au niveau de la salle de commande principale n'est pas établie. Néanmoins, l'état de l'art actuel permet de combiner différentes chaînes de protection du CC pour un accident donné, cette modélisation est alors utile pour vérifier l'acceptabilité du nombre et de la diversité de ces chaînes, en tenant compte de la fréquence de l'événement initiateur.

A.2 Description de la modélisation

A.2.1 Description globale

La modélisation simplifiée est basée sur une décomposition structurelle des systèmes numériques de protection (voir figure A.1). Pour une chaîne de protection donnée, nous avons

- la partie capteur (ou acquisition),
- la partie logique, et
- la partie actionneur.

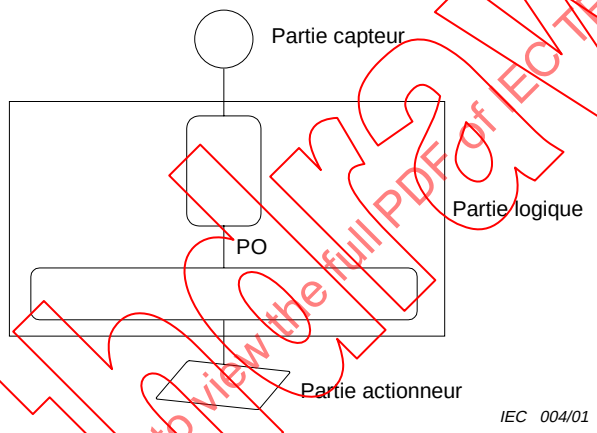

Figure A.1 – Modélisation d'une chaîne

Il est attribué à chaque partie une valeur d'indisponibilité enveloppe compatible avec le retour d'expérience concernant la fiabilité des dispositifs de commande automatiques pour les centrales en exploitation, cette valeur étant du même ordre de grandeur que les valeurs proposées dans les autres normes internationales. Ainsi, ces valeurs sont basées sur le jugement d'experts se positionnant sur des sujets critiques (comme les taux de couverture des diagnostics des auto-tests internes) et en utilisant des critères précis. Ces valeurs nécessitent un consensus international qui doit être établi entre les différents experts.

A.2.2 Partie capteur

Cette partie est décrite par 

Elle est, en fait, constituée d'un groupe de capteurs redondants (le terme capteur inclut la cellule de mesure, le convertisseur électronique et la connectique de transmission) qui assure la surveillance du même paramètre. Le nombre de capteurs au sein de ce groupe dépend du niveau interne de redondance de la chaîne de protection; par exemple, une redondance de 2/4 requiert quatre capteurs.

The pertinence of this type of modelling for I&C missions linked to human action in the main control room is not established. Nevertheless, the present state of the art allows I&C protection channels to be combined for a given accident and it is helpful to check the acceptability of the number and diversity of those channels, taking into account the frequency of the initiating event.

A.2 Modelling description

A.2.1 Global description

The simplified modelling is based upon a structural decomposition of numeric protection systems (see figure A.1). For one given protection channel, there is:

- the acquisition part,
- the logic part, and
- the actuator part.

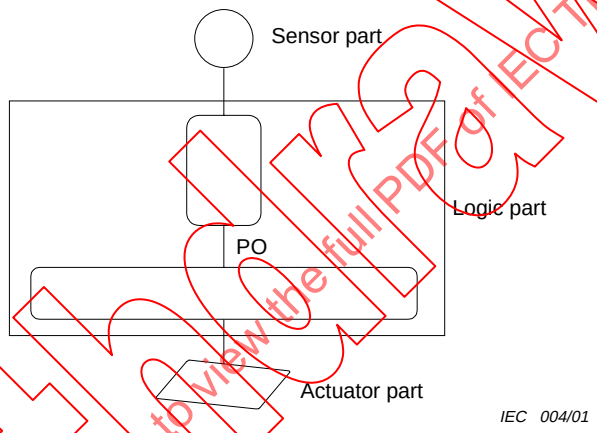

Figure A.1 – Channel modelling

Each part is given an encompassing unavailability value coherent with the automatic control devices reliability feedback made for the operating plants and are of the same range of the values proposed in other international standards. So, those values are based on expert judgement replying to critical subjects (like diagnostic coverage rates of internal self-tests) by using precise criteria. These values need an international consensus, which has to be established between the different experts.

A.2.2 Sensor part

This part is described by

In fact, it is made up of a group of redundant sensors (the term sensor includes the measuring cell and the electronic converter and communication) and implements the surveillance of the same parameter. The number of sensors within this group depends on the internal degree of protection channel redundancy; for example, 2/4 redundancy requires four sensors.