NORME INTERNATIONALE
INTERNATIONAL STANDARD

CEI
IEC
1226

Première édition
First edition
1993-05

Centrales nucléaires – Systèmes d'instrumentation et de contrôle-commande importants pour la sûreté – Classification

Nuclear power plants – Instrumentation and control systems important for safety – Classification

Numéro de référence
Reference number
CEI/IEC 1226: 1993

Numéros des publications

Depuis le 1er janvier 1997, les publications de la CEI sont numérotées à partir de 60000.

Publications 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.

Validité de la présente publication

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 la date de reconfirmation de la publication sont disponibles dans le Catalogue de la CEI.

Les renseignements relatifs à des questions à l'étude et des travaux en cours entrepris par le comité technique qui a établi cette publication, ainsi que la liste des publications établies, se trouvent dans les documents ci-dessous:

- **«Site web» de la CEI***
- **Catalogue des publications de la CEI**
  Publié annuellement et mis à jour régulièrement
  (Catalogue en ligne)*
- **Bulletin de la CEI**
  Disponible à la fois au «site web» de la CEI* et comme périodique imprimé

Terminologie, symboles graphiques et littéraux

En ce qui concerne la terminologie générale, le lecteur se reportera à la CEI 60050: *Vocabulaire Electrotechnique International* (VEI).

Pour les symboles graphiques, les symboles littéraux et les signes d'usage général approuvés par la CEI, le lecteur consultera la CEI 60027: *Symboles littéraux à utiliser en électrotechnique,* la CEI 60417: *Symboles graphiques utilisables sur le matériel. Index, relevé et compilation des feuilles individuelles,* et la CEI 60617: *Symboles graphiques pour schémas.*

* Voir adresse «site web» sur la page de titre.

Numbering

As from 1 January 1997 all IEC publications are issued with a designation in the 60000 series.

Consolidated publications

Consolidated versions of some IEC publications including amendments are available. 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.

Validity of this publication

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 the date of the reconfirmation of the publication is available in the IEC catalogue.

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 to be found at the following IEC sources:

- **IEC web site***
- **Catalogue of IEC publications**
  Published yearly with regular updates
  (On-line catalogue)*
- **IEC Bulletin**
  Available both at the IEC web site* and as a printed periodical

Terminology, graphical and letter symbols

For general terminology, readers are referred to IEC 60050: *International Electrotechnical Vocabulary* (IEV).

For graphical symbols, and letter symbols and signs approved by the IEC for general use, readers are referred to publications IEC 60027: *Letter symbols to be used in electrical technology*, IEC 60417: *Graphical symbols for use on equipment. Index, survey and compilation of the single sheets* and IEC 60617: *Graphical symbols for diagrams.*

* See web site address on title page.

NORME INTERNATIONALE
INTERNATIONAL STANDARD

CEI
IEC
1226

Première édition
First edition
1993-05

Centrales nucléaires – Systèmes d'instrumentation et de contrôle-commande importants pour la sûreté – Classification

Nuclear power plants – Instrumentation and control systems important for safety – Classification

Bureau Central de la Commission Electrotechnique Internationale 3, rue de Varembé Genève, Suisse

Commission Electrotechnique Internationale
International Electrotechnical Commission
Международная Электротехническая Комиссия

CODE PRIX
PRICE CODE S

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

SOMMAIRE

CONTENTS

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

Centrales nucléaires - Systèmes d'instrumentation et de contrôle-commande importants pour la sûreté - Classification

AVANT-PROPOS

1) La CEI (Commission Electrotechnique 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 en ce qui concerne les questions techniques, préparés par les comités d'études où sont représentés tous les Comités nationaux s'intéressant à ces questions, expriment dans la plus grande mesure possible un accord international sur les sujets examinés.

3) Ces décisions constituent des recommandations internationales publiées sous forme de normes, de rapports techniques ou de guides et agréées comme telles 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 du 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.

La Norme internationale CEI 1226 a été établie par le sous-comité 45A: Instrumentation des réacteurs, du comité d'études 45 de la CEI: Instrumentation nucléaire.

Le texte de cette norme est issu des documents suivants:

DIS	Rapport de vote
45A(BC)128	45A(BC)133

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

L'annexe A est donnée uniquement à titre d'information.

INTERNATIONAL ELECTROTECHNICAL COMMISSION

Nuclear power plants - Instrumentation and control systems important for safety - Classification

FOREWORD

1) The IEC (International Electrotechnical Commission) is a world-wide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of the IEC is to promote international cooperation 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 Standardization Organization (ISO) in accordance with conditions determined by agreement between the two organizations.

2) The formal decisions or agreements of the IEC on technical matters, prepared by technical committees on which all the National Committees having a special interest therein are represented, express, as nearly as possible, an international consensus of opinion on the subject dealt with.

3) They have the form of recommendations for international use published in the form of standards, 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.

International Standard IEC 1226 has been prepared by sub-committee 45A: Reactor instrumentation, of IEC technical committee 45: Nuclear instrumentation.

The text of this standard is based upon the following documents:

DIS	Report on Voting
45A(CO)128	45A(CO)133

Full information on the voting for the approval of this part can be found in the Voting Report indicated in the above table.

Annex A is for information only.

Introduction

La présente Norme internationale répond à une recommandation de l'Agence Internationale de l'Energie Atomique (AIEA), concernant le classement par catégories des fonctions, systèmes et matériels d'instrumentation et de contrôle-commande (FSE) des centrales nucléaires en fonction de leur importance pour la sûreté. L'objectif de cette norme est de classer les fonctions, systèmes et équipements qui sont importants pour la sûreté en trois catégories et d'élaborer des prescriptions cohérentes avec leur importance respective pour la sûreté. Les catégories de sûreté des FSE sont déterminées en fonction de leur contribution à la réduction des événements initiateurs hypothétiques (EIH). Les méthodes de classement devraient, dans le cas idéal, être fondées sur une évaluation quantitative des risques; une méthode utilisant des critères semi-quantitatifs ou semi-qualitatifs est en effet sujette à interprétation. Il y a de plus en plus d'évaluations quantitatives des risques dans le monde des centrales nucléaires de puissance et les résultats de ces études, lorsqu'ils sont disponibles, devraient être utilisés comme base de classification. Cependant, du fait de la fréquente indisponibilité des résultats d'études de probabilité, il existe actuellement un besoin de méthode de classification qui ne soit pas fondée sur une évaluation quantitative des risques.

Cette norme a été élaborée pour offrir une méthode de classement par catégories fondée sur des critères qualitatifs et qui ne nécessite pas l'utilisation des résultats d'une évaluation des risques. Une réédition de cette norme est prévue, qui rassemblerait à la fois les critères de classification qualitatifs et quantitatifs. Il faut appliquer soigneusement et rigoureusement les critères qualitatifs donnés, afin de garantir que le classement obtenu - bien que conservatif - soit en accord avec les résultats d'une classification fondée sur une évaluation des risques.

Lorsqu'il existe des résultats numériques d'évaluation probabiliste des risques, il convient d'utiliser de préférence les critères quantitatifs; pour cela, il est possible d'utiliser les mesures quantitatives d'importance, issues des résultats des études d'évaluation de risques menées dans le cadre du processus de conception ou de vérification de la centrale. Les mesures d'importance sont généralement intitulées calculs Fussell-Vesely, calculs de réduction de risques ou calculs d'analyse de risque et peuvent être utilisés pour fournir des comparaisons relatives sur l'importance pour la sûreté des différents systèmes ou sous-systèmes.

Utilisation du classement par catégories

L'AIEA a recommandé que les systèmes d'instrumentation et de contrôle-commande (I&C) des centrales nucléaires (NPP) soient classés en catégories, selon leur importance pour la sûreté. La classification en catégories des fonctions, et des systèmes et matériels associés (FSE) peut être effectuée après identification de la signification de chaque fonction, système ou matériel dans le maintien de la sûreté de la centrale. La sûreté de la NPP consiste en la prévention ou la réduction des accidents, dans le but d'éviter tout dépassement des limites de dégagement de matières radioactives dans l'environnement (en termes de fréquences d'occurrence ou d'amplitude de rejets) ou des limites de doses pour le personnel d'exploitation.

Une classification correcte des FSE implique qu'il soit porté une attention suffisante par les concepteurs, les exploitants et les autorités réglementaires aux fonctions, systèmes et matériels qui assurent la sûreté dans les domaines des spécifications, de la conception, de la qualification, de l'assurance de la qualité (AQ), du contrôle de la qualité (CQ), de la fabrication, de l'installation, de la maintenance et des essais.

Cette norme fixe les critères et méthodes de répartition des FSE I&C d'une centrale nucléaire en trois catégories, A, B et C, en fonction de l'importance de ces FSE pour la sûreté, et en une catégorie de matériels non classés pour les FSE qui n'ont pas de rôle direct de sûreté. Elle définit les exigences génériques de chaque catégorie et les exigences techniques spécifiques traitant de l'assurance qualité, de la fiabilité, des essais et de la maintenance.

La catégorie attribuée à chaque FSE établit des exigences techniques génériques et spécifiques. Les exigences génériques pour chaque FSE sont destinées à apporter l'assurance que ce FSE sera capable d'exécuter de manière fiable la fonction demandée. Cela s'applique aux aspects de fonctionnalité, de fiabilité, de performances, de résistance aux conditions d'ambiance et d'assurance qualité. Le niveau de garantie nécessaire pour chacun de ces aspects doit être cohérent avec leur importance pour la sûreté.

Introduction

This International Standard responds to an International Atomic Energy Agency (IAEA) recommendation to categorize nuclear power plants' instrumentation and control functions, systems and equipment (FSE) according to their importance for safety. The intent of this standard is to classify functions, systems and equipment that are important for safety into three general categories, and to develop requirements that are consistent with the importance for safety of each of these classification categories. The safety category of the FSE is determined by their contribution to the mitigation of Postulated Initiating Events (PIE). The methods of categorization ideally would be based upon a quantitative assessment of risk, because an approach that uses semi-quantitative or qualitative criteria is open to interpretation. Quantitative assessments of risk are increasingly being undertaken throughout the world nuclear power plant community and, where available, the results of these studies should be used as the basis for categorization. Because the results of probabilistic studies are often not available, there is a current need for a categorization method that does not depend upon quantitative risk assessment.

This standard has been prepared to provide a categorization method that is based on qualitative criteria and that does not require the use of risk assessment results. It is intended that it will be re-issued in the future incorporating both qualitative and quantitative categorization criteria. The qualitative criteria currently given must be applied carefully to ensure that the categorizations strictly obtained will be consistent with the results of a categorization based (albeit conservatively) on a risk assessment.

Quantitative criteria should take precedence where numerical risk assessment results are available, and one means of accomplishing this is to use the quantitative importance measures that are derived from the results of probabilistic risk assessment studies carried out as part of the plant design or evaluation process. The importance measures are commonly termed Fussell-Vesely calculations, risk reduction calculations, and risk achievement calculations, and can be used to provide relative comparisons of importance for safety of different systems or subsystems.

Use of categorization

The IAEA has recommended that Instrumentation and Control (I&C) systems of Nuclear Power Plants (NPP) should be assigned to categories according to their importance for safety. The classification of functions, and the associated systems and items of equipment (FSE) into categories can be carried out following the identification of the significance of each function, system or item of equipment in the maintenance of NPP safety. NPP safety is the prevention or mitigation of accidents so that limits of frequency or magnitude for the release of radioactive material to the environment or doses to the operating staff are not exceeded.

Correct classification of FSE directs the appropriate degree of attention by the plant's designers, operators and regulatory authorities to the specification, design, qualification, Quality Assurance and Quality Control (QA and QC), manufacturing, installation, maintenance, and testing of the FSEs that ensure safety.

This standard establishes the criteria and methods to be used to assign the I&C FSE of an NPP to three categories A, B and C, which depend on the importance of the FSE for safety, and an unclassified category for FSE with no direct safety role. It outlines generic requirements for each category, and specifies basic technical requirements for matters such as QA, reliability, testing and maintenance.

The category to which an FSE is assigned determines generic and specific technical requirements. Generic requirements for each FSE are based on providing the appropriate level of ensurance that the FSE will achieve the required performance and reliability when called upon. This applies to the aspects of functionality, reliability, performance, environmental durability and QA. The level of ensurance to be shown for each of these aspects shall be consistent with the importance of the FSE to safety.

a) L'assurance de fonctionnalité est établie par la création d'une spécification exhaustive de prescriptions, et par l'application des normes et codes appropriés.

b) L'assurance de fiabilité est fournie par la sélection de composants, de structures et de niveaux de redondance et de diversité appropriés, associés aux notions de séparation physique et/ou de barrière, d'isolation électrique et d'essais périodiques en service.

c) L'assurance de performance est donnée par la création de spécifications des performances requises, l'application des procédures de contrôle de la qualité, de processus de vérification et de validation pendant la conception et la fabrication, les essais initiaux des FSE unitaires et globaux et les essais en service.

d) L'assurance de résistance aux conditions d'ambiance est assurée par les programmes de qualification du matériel afin de garantir que les effets du vieillissement et des conditions d'environnement existant au moment où le matériel est appelé à fonctionner ne dégradent pas ses performances au-dessous des valeurs prévues dans l'analyse.

e) L'assurance de la prise en compte à chaque étape, allant de la conception à la mise en service, en passant par la fabrication, les essais et l'installation, des aspects de fonctionnalité, de performances, de résistance aux conditions d'ambiance et de fiabilité, est donnée par la réalisation de chaque étape des travaux sous le contrôle d'un programme d'AQ et de CQ approprié.

NOTE - Le Guide de sûreté 50-SG-D8 de l'AIEA, section 3.1.1, recommande que les FSE I&C soient classés en catégories, en fonction de leur importance pour la sûreté. Il prescrit l'étude des facteurs cités ci-dessous en fixant les catégories, soit directement, soit lors de l'établissement de l'importance des fonctions remplies par les systèmes I&C:

1) la probabilité et la gravité potentielle des conséquences d'événements initiateurs hypothétiques (EIH) si le système I&C prévu tombe en panne;

2) le temps disponible entre l'EIH et le moment où le déclenchement de la fonction de sûreté est prescrit;

3) la durée pendant laquelle le système I&C est nécessaire après le déclenchement de la fonction de sûreté;

4) la fiabilité nécessaire au déclenchement d'autres actions possibles et leur opportunité;

5) la fiabilité des remèdes qui peuvent être apportés à toute défaillance du système I&C et leur opportunité;

6) la potentialité du système à provoquer lui-même un EIH, les dispositions prises dans les systèmes de sûreté ou les systèmes I&C liés à la sûreté pour ce genre d'EIH, et la combinaison des conséquences et de la probabilité d'un tel EIH.

a) Ensurance of functionality is established by the creation of a complete and comprehensive requirements specification, and the application of appropriate standards and codes.

b) Ensurance of reliability is provided by the selection of appropriate components, structures and levels of redundancy and diversity in association with physical separation and/or barriers, electrical isolation and periodic testing during service.

c) Ensurance of performance is gained by the creation of specifications of the required performance, the application of QC procedures, verification and validation processes during design and manufacture, preservice testing of the individual and integrated FSE, and testing during service.

d) Ensurance of environmental durability is established by equipment qualification programmes to ensure that ageing effects and environmental conditions that exist at the time the equipment is required to operate do not degrade its performance below that required.

e) Ensurance that the aspects of functionality, performance, environmental durability and reliability have been properly considered at each stage from conception, through design, manufacture, test, installation, commissioning and entry into service is provided by carrying out each stage of the work under the control of an appropriate QA and QC programme.

NOTE - IAEA Safety Guide 50-SG-D8, section 3.1.1, recommends that safety related I&C FSE should be placed in categories, according to their importance for safety. It requires consideration of the factors quoted below in establishing the categories, either directly or while establishing the importance of the functions that the I&C systems carry out:

1) the probability and potential severity of consequences of Postulated Initiating Events (PIEs) if the I&C system provided fails;

2) the period available between the occurrence of the PIE and the time the initiation of the safety function is required;

3) the length of time for which the I&C system is required once the safety function is initiated;

4) the timeliness and reliability with which alternative actions can be taken;

5) the timeliness and reliability with which any failure in the I&C system can be remedied;

6) the potential of the I&C system itself to cause a PIE, the provisions made in the safety systems or safety related I&C systems for such a PIE, and the combination of consequences and probability of such a PIE.

Centrales nucléaires - Systèmes d'instrumentation et de contrôle-commande importants pour la sûreté - Classification

1 Domaine d'application

La présente Norme internationale établit une méthode de classification des fonctions d'information et de commande des centrales nucléaires, et des systèmes et du matériel I&C qui assurent ces fonctions, en catégories indiquant leur importance pour la sûreté. La classification qui en résulte permet alors l'établissement de critères de conception appropriés.

Les critères de conception sont les mesures de la qualité garantissant qu'il y a adéquation de chaque FSE relativement à son importance pour la sûreté. Dans cette norme, les critères retenus concernent la fonctionnalité, la fiabilité, les performances, la résistance aux conditions d'ambiance et l'assurance de la qualité (AQ).

Cette norme est applicable à toutes les fonctions d'information et de commande ainsi qu'aux systèmes et aux matériels I&C qui remplissent ces fonctions. Les fonctions, systèmes et matériels considérés assurent une protection automatique, un contrôle en boucle ouverte ou fermée et fournissent des informations à l'équipe de conduite. Elles maintiennent les conditions de la centrale dans les limites de fonctionnement sûr, déclenchent des actions automatiques ou permettent des actions manuelles qui minimisent les accidents ou empêchent ou minimisent les rejets radioactifs sur le site ou dans l'environnement. Les FSE susceptibles de remplir ces tâches sauvegardent la santé et la sécurité des opérateurs de la centrale et du public.

Cette norme complète, sans les annuler ni les remplacer, les guides de sûreté et les codes de pratique publiés par l'Agence Internationale de l'Energie Atomique (AIEA). Cette norme est conforme aux principes généraux donnés dans le Code de sûreté 50-C-D (Rév.1) et les Guides de sûreté 50-SG-D3, 50-SG-D8 et 50-SG-D11 de l'AIEA et elle définit une méthode structurée d'application des directives contenues dans ces codes et normes pour les FSE I&C d'une centrale nucléaire.

2 Références normatives

Les documents normatifs suivants contiennent des dispositions qui par la référence qui y est faite constituent des dispositions valables pour la présente Norme internationale. Au moment de la publication de cette norme, les éditions indiquées étaient en vigueur . Tout document normatif est sujet à révision et les parties prenantes aux accords fondés sur la présente Norme internationale sont invitées à rechercher la possibilité d'appliquer les éditions les plus récentes des documents normatifs indiqués ci-après. Les membres de la CEI et de l'ISO possèdent le registre des Normes internationales en vigueur.

CEI 780:1984, *Qualification des constituants électriques du système de sûreté des centrales électronucléaires*
CEI 812:1985, *Techniques d'analyse de la fiabilité des systèmes - Procédure d'analyse des modes de défaillance et de leurs effets (AMDE)*
CEI 863:1986, *Présentation des résultats de la prévision des caractéristiques de fiabilité, maintenabilité et disponibilité*
CEI 880:1986, *Logiciel pour les calculateurs utilisés dans les systèmes de sûreté des centrales nucléaires*
CEI 964:1989, *Conception des salles de commande des centrales nucléaires de puissance*
CEI 980:1989, *Pratiques recommandées pour la qualification sismique du matériel électrique du système de sûreté dans les centrales électronucléaires*
CEI 987:1989, *Calculateurs programmés importants pour la sûreté des centrales nucléaires*

AIEA Code 50-C-D (Rév.1):1988 , *Conception pour la sûreté des centrales nucléaires*
AIEA Code 50-C-AQ (Rév.1):1988, *Assurance de la qualité pour la sûreté des centrales nucléaires*
AIEA Guide de sûreté 50-SG-D1:1979, *Fonctions de sûreté et classification des composants pour les BWR, PWR et PTR*
AIEA Guide de sûreté 50-SG-D3:1980, *Systèmes de protection et dispositifs connexes dans les centrales nucléaires*
AIEA Guide de sûreté 50-SG-D8:1984, *Systèmes d'instrumentation et de commande liés à la sûreté dans les centrales nucléaires*
AIEA Guide de sûreté 50-SG-D11:1986, *Principes généraux de sûreté dans la conception des centrales nucléaires*

Nuclear power plants - Instrumentation and control systems important for safety - Classification

1 Scope

This International Standard establishes a method of classification of the information and command functions for nuclear power plants, and the I&C and equipment that provide those functions, into categories that designate the importance for safety of the FSE. The resulting classification then determines relevant design criteria.

The design criteria are the measures of quality by which the adequacy of each FSE in relation to its importance to plant safety is ensured. In this standard, the criteria are those of functionality, reliability, performance, environmental durability and QA.

This standard is applicable to all the information and command functions, and the instrumentation and control systems and equipment that provide those functions. The functions, systems and equipment under consideration provide automated protection, closed or open loop control, and information to the operating staff. They keep the NPP conditions inside the safe operating envelope and provide automatic actions, or enable manual actions, that mitigate accidents or prevent or minimize radioactive releases to the site or wider environment. The FSE that fulfil these roles safeguard the health and safety of the NPP operators and the public.

This standard complements, and does not replace or supersede, the Safety Guides and Codes of Practice published by the International Atomic Energy Agency (IAEA). This standard follows the general principles given in IAEA Safety Code 50-C-D (Rev. 1) and Safety Guides 50-SG-D3, 50-SG-D8 and 50-SG-D11, and it defines a structured method of applying the guidance contained in those codes and standards to the I&C FSE of an NPP.

2 Normative references

The following normative documents contain provisions which, through reference in this text, constitute provisions of this International Standard. At the time of publication, the editions indicated were valid. All normative documents are subject to revision, and parties to agreements based on this International Standard are encouraged to investigate the possibility of applying the most recent editions of the normative documents indicated below. Members of IEC and ISO maintain registers of currently valid International Standards.

IEC 780:1984, *Qualification of electrical items of the safety system for nuclear power generating stations*
IEC 812:1985, *Analysis techniques for system reliability - Procedure for Failure Mode and Effects Analysis (FMEA)*
IEC 863:1986, *Presentation of reliability, maintainability and availability predictions*
IEC 880:1986, *Software for computers in the safety system of nuclear power stations*
IEC 964:1989, *Design for control rooms of nuclear power plants*
IEC 980:1989, *Recommended practices for seismic qualification of electrical equipment of the safety system for nuclear generating stations*
IEC 987:1989, *Programmed digital computers important for safety for nuclear power stations*

IAEA Code 50-C-D (Rev.1):1988, *Code on the safety of nuclear power plants: Design*
IAEA Code 50-C-QA (Rev. 1):1988, *Quality assurance on the safety of nuclear power plants*
IAEA Safety Guide 50-SG-D1:1979, *Safety functions and component classification for BWR, PWR and PTR*
IAEA Safety Guide 50-SG-D3:1980, *Protection system and related features in nuclear power plants*
IAEA Safety Guide 50-SG-D8:1984, *Safety related instrumentation and control systems for nuclear power plants*
IAEA Safety Guide 50-SG-D11:1986, *General design safety principles for nuclear power plants*

3 Définitions

Pour les besoins de la présente Norme internationale, les définitions suivantes - données par ordre alphabétique - s'appliquent. Elles sont cohérentes avec celles d'autres codes, guides et normes CEI ou AIEA en vigueur ou, pour celles marquées d'un astérisque, identiques à celles-ci.

code: Ensemble de prescriptions dont l'application directe représente une obligation légale dans le pays où le code est en vigueur.

code de pratique: Ensemble de recommandations dont l'application n'est pas obligatoire, et dont le manquement ne serait pas une négligence sur le plan légal, mais qui est le reflet de bonnes pratiques industrielles.

devrait: Dans cette norme, le terme "devrait" est utilisé pour indiquer les exigences auxquelles il est vivement recommandé, mais non impératif, de se conformer.

critère de défaillance unique*: 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.

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.

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.».

doit: Dans cette norme, le terme "doit" est utilisé pour indiquer des exigences qu'il est impératif de respecter pour se conformer à cette norme.

en continu: Etat d'un système qui remplit ses fonctions spécifiées comme l'exige la conception de la centrale.

essais de type: Détermination ou vérification de l'aptitude d'un type de matériel à satisfaire aux exigences spécifiées en soumettant un élément ou un certain nombre d'éléments représentatif de ce type à un ensemble de conditions physiques, chimiques, d'environnement ou opérationnelles.

événements initiateurs hypothétiques (EIH)*: Evénements qui entraînent des incidents de fonctionnement prévus et des situations accidentelles, leurs effets plausibles, causes de défaillances et leurs combinaisons plausibles[1].

fonction: But ou objectif spécifique à réaliser et qui peut être spécifié ou décrit sans référence aux moyens physiques nécessaires à sa réalisation.

fonction de sûreté*: But particulier à atteindre aux fins de la sûreté.

---

1) Les causes initiales des événements initiateurs hypothétiques peuvent être des défaillances plausibles du matériel et/ou des erreurs humaines (les unes et les autres aussi bien à l'intérieur qu'à l'extérieur de la centrale), des phénomènes naturels de référence et des agressions de référence dues à des activités humaines. Il faut que la spécification des événements initiateurs hypothétiques soit acceptée par l'organisme réglementaire pour la centrale nucléaire. Voir le Code 50-C-D de l'AIEA et le Guide de sûreté 50-SG-D8 de l'AIEA pour plus de détails.

3 Definitions

For the purposes of this International Standard, the following definitions - given in alphabetical order - apply. They are consistent, or identical if marked *, with those used in other current IEC or IAEA codes, guides and standards.

code: A set of requirements with which direct compliance is a legal requirement in the country where the code is in force.

code of practice: A set of recommendations with which compliance is not a requirement, and from which deviation would not be negligent in a legal sense, but represents good or best industry practice.

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 physically different from each other, or by functional diversity, where similar systems achieve the specified objective in different ways.

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 carry out 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.»

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.

function: A specific purpose or objective to be accomplished, that can be specified or described without reference to the physical means of achieving it.

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".

FSE: 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 collections of components and the components themselves that are employed to achieve the functions.

guide: A publication of the IAEA that recommends good practice for NPP designers, constructors, operators or regulators, and which may lead to the production of IEC or other national or international standards.

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.

may: Throughout this standard, the term "may" indicates that compliance with the recommendation is optional.

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.

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".

FSE : 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.

FSE I&C importants pour la sûreté: Ceux-ci comprennent:

a) les FSE I&C dont le défaut ou la défaillance pourrait entraîner pour le personnel du site ou le public une exposition inacceptable aux rayonnements;
b) les FSE I&C qui empêchent les événements opérationnels prévus de provoquer une séquence significative;
c) les FSE I&C qui réduisent les conséquences des pannes ou défaillances de structures, systèmes ou composants.

FSE I&C liés à la sûreté: FSE I&C importants pour la sûreté qui ne font pas partie des systèmes de sûreté.

guide: Publication de l'AIEA qui recommande de bonnes pratiques aux concepteurs, constructeurs, opérateurs ou exploitants de centrales nucléaires et qui est susceptible de conduire à la production de normes CEI ou à d'autres normes nationales ou internationales.

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

norme: Ensemble d'exigences obligatoires dont la conformité n'est pas une prescription légale mais dont le manquement sans raison valable constituerait une négligence.

performances: Efficacité avec laquelle une fonction prévue est exécutée (par exemple temps de réponse, précision, sensibilité aux modifications des paramètres).

pourrait: Dans cette norme, le terme "pourrait" indique que la conformité avec la recommandation est optionnelle.

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.

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.

sous-FSE: Un FSE peut être divisé en plusieurs sous-FSE qui peuvent être considérés isolément mais dont l'action conjointe permet la réalisation du FSE dans sa totalité.

sous-système* : Division d'un système dotée elle-même des caractéristiques de ce système.

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.

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.

nuclear safety: The ability of an NPP to avoid or prevent a nuclear accident, that is an unplanned or uncontrolled criticality of a magnitude that causes damage.

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

performance: The effectiveness with which an intended function is carried out (e.g. time response, accuracy, sensitivity to parameter changes).

Postulated Initiating Events (PIE)* : Events that lead to anticipated operational occurrences and accident conditions, their credible causal failure effects and their credible combinations.[1]

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.

safety function*: A specific purpose that must be accomplished for safety.

safety systems*: 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 sequences.

safety related I&C FSE: Those I&C FSE important for safety that are not part of the safety systems.

shall: Throughout this standard, the term "shall" indicates requirements that are mandatory for compliance with the standard.

should: Throughout this standard, the term "should" indicates requirements that are not mandatory for compliance with the standard but are strongly recommended.

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 exceeding 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.

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.

standard: A set of mandatory requirements with which compliance is not a legal requirement, but with which failure to comply without valid reason would be negligent.

sub-FSE: An FSE may be divided into several sub-FSE that may be considered in isolation but act together to achieve the overall FSE.

subsystem*: A division of a system that in itself has the characteristics of a system.

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

---

1) The initial causes of Postulated Initiating Events may be credible equipment failures and/or operator errors (both within and external to the nuclear power plant), design basis natural events and design basis external man-induced events. Specification of the Postulated Initiating Events is to be acceptable to the regulatory body for the nuclear power plant. Refer to IAEA Code 50-C-D and IAEA Safety Guide 50-SG-D8 for further details.

système*: Groupement d'éléments connectés entre eux, constitué, dans un objectif donné, pour accomplir une fonction spécifiée.

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

4 Abréviations

AIEA	Agence Internationale de l'Énergie Atomique
ALARA	Aussi faible qu'il soit raisonnablement possible de réaliser
AMDE	Analyse des Modes de Défaillance et de leurs Effets
AQ	Assurance de la qualité
CQ	Contrôle de la qualité
EIH	Événement Initiateur Hypothétique
EPS	Évaluation Probabiliste de Sûreté
FSE	Fonction(s), Systèmes et matériels associés qui la (les) mettent en œuvre
I&C	Instrumentation et contrôle-commande
NPP	Centrale nucléaire
RS	Recette Site
RU	Recette Usine

5 Prescriptions

Les FSE I&C de la centrale doivent être classés en catégories, selon leur importance pour la sûreté. Les critères de conception, de fabrication, d'installation, de mise en service, de maintenance et d'essais en service propres à la catégorie concernée doivent être ensuite appliqués aux FSE pendant chacune de ces phases.

5.1 *Eléments de base*

Le principe de défense en profondeur est fermement établi dans le dimensionnement de sûreté des centrales nucléaires. Selon l'idée de base, il devrait exister plusieurs niveaux ou échelons de défense dans la prévention des conditions non sûres, en outre, il est toujours préférable de recourir à la prévention, avant d'en arriver à la nécessité d'une limitation des conséquences. En raison du grand nombre des FSE, nécessaires au fonctionnement et au maintien de la sûreté d'une centrale et notamment du fait de l'application du principe de défense en profondeur, il est important de connaître leur importance respective pour la sûreté.

Le Guide de sûreté 50-SG-D1 de l'AIEA établit l'idée de classer les systèmes d'une centrale en fonction de leur importance pour la sûreté et donne des exemples de classification des principaux systèmes de différents types de centrales. Les Guides de sûreté 50-SG-D3 et 50-SG-D8 établissent une distinction entre les systèmes de sûreté, qui sont les systèmes prévus pour assurer une mise à l'arrêt sûre du réacteur et l'évacuation de la chaleur résiduelle du cœur ou réduire les conséquences de conditions de fonctionnement prévues ou de situations accidentelles, et les systèmes I&C liés à la sûreté, qui sont des systèmes I&C importants pour la sûreté mais qui ne sont pas compris dans les systèmes de sûreté.

L'importance pour la sûreté et les exigences correspondantes concernant les différentes parties des systèmes de sûreté et des systèmes I&C liés à la sûreté peuvent différer, de sorte qu'il convient de leur assigner des catégories de sûreté différentes. Certains systèmes I&C sont susceptibles d'avoir une action significative sur la sûreté et nécessitent de ce fait une attention appropriée. D'autres systèmes I&C n'ont, par contre, qu'une importance moyenne, faible ou nulle pour la sûreté. Ils nécessitent par conséquent de respecter des exigences moins contraignantes pour garantir leurs performances et la justification de sûreté et, de ce fait, reposent sur des exigences techniques différentes.

Cette norme étend la stratégie de classification présentée dans le Guide de sûreté 50-SG-D1 de l'AIEA, et définit les critères et les méthodes à utiliser pour classer les FSE I&C dans l'une des trois catégories A, B et C, selon l'importance du matériel pour la sûreté, ou dans une catégorie de FSE non classée sans fonction de sûreté directe.

type testing: The determination or verification of the capability of a type of equipment to meet specified requirements by subjecting a representative item, or number of items, of the type to a set of physical, chemical, environmental or operational conditions.

4 Abbreviations

ALARA	As Low As Reasonably Achievable
FAT	Factory Acceptance Test
FMEA	Failure Modes and Effects Analysis
FSE	Function(s), and the associated Systems and Equipment that implement it (them)
IAEA	International Atomic Energy Agency
I&C	Instrumentation and Control
NPP	Nuclear Power Plant
PIE	Postulated Initiating Event
PRA	Probabilistic Risk Assessment
QA	Quality Assurance
QC	Quality Control
SAT	Site Acceptance Test

5 Requirements

I&C FSE of the NPP shall be assigned to categories according to their importance for safety. The design, manufacturing, installation, commissioning and in-service maintenance and testing criteria of that category shall then be applied to the FSE during each of those phases.

5.1 *Background*

The principle of defence in depth is firmly established in the safety design basis of nuclear power plants. The fundamental idea is that there should be several layers or echelons of defence in the prevention of unsafe conditions, and that the prevention of unsafe conditions, before mitigation is required, is always to be preferred. Because of the large number of FSEs that are required to operate and keep safe an NPP, a number that increases with the principle of defence in depth, it is important that the significance to safety of each FSE is known.

IAEA Safety Guide 50-SG-D1 establishes the idea of classification of NPP systems according to their importance for safety, and gives examples of the classification of the major systems of several types of NPP. Safety Guides 50-SG-D3 and 50-SG-D8 establish the distinction between the safety systems, which are the systems provided to ensure the safe shutdown of the reactor and heat removal from the core or to limit the consequences of anticipated operational occurrences or accident conditions, and safety related I&C systems, which are the I&C systems important for safety that are not part of the safety systems.

The safety importance of, and the corresponding requirements placed on, parts of the safety systems and safety related I&C systems will differ, so that it is appropriate to assign them to different safety categories. Some I&C systems can have a significant effect on safety and therefore require appropriate attention. Other I&C systems have intermediate, low, or no significance to safety. They have correspondingly less stringent requirements for ensurance of performance and safety justification, and therefore have different technical requirements.

This standard extends the classification strategy presented in IAEA Safety Guide 50-SG-D1, and establishes the criteria and methods to be used to assign the I&C FSEs of an NPP to one of three categories A, B and C, depending on the importance of the equipment to safety, or to an unclassified category for FSE with no direct safety role.

5.2 *Description des catégories*

5.2.1 *Catégorie A*

La catégorie A est utilisée pour désigner les FSE dont le rôle est important pour l'obtention ou le maintien de la sûreté nucléaire. Ces fonctions doivent empêcher les EIH de conduire à une séquence d'événements significative ou atténuer leurs conséquences. Les FSE de catégorie A peuvent être assurés de façon automatique ou par des actions manuelles, sous réserve que de telles actions soient du ressort des capacités des opérateurs. La catégorie A sert également à identifier les FSE dont la défaillance pourrait être la cause directe de séquences significatives d'événements. Les FSE de catégorie A ont des prescriptions de disponibilité élevées. Leur fonctionnalité peut être limitée de manière que leur disponibilité puisse être garantie avec un haut niveau de confiance.

5.2.2 *Catégorie B*

La catégorie B est utilisée pour désigner les FSE qui ont une action complémentaire à ceux de la catégorie A dans l'obtention ou le maintien de la sûreté nucléaire. Le fonctionnement d'un FSE de catégorie B peut éviter le déclenchement d'un FSE de catégorie A. La catégorie B peut également améliorer ou compléter l'exécution d'une fonction de catégorie A en atténuant un EIH de façon à éviter ou réduire une détérioration d'équipement ou un rejet d'activité. La catégorie B sert également à identifier les FSE dont la défaillance serait susceptible d'initier ou d'aggraver un EIH. Du fait de la présence de fonctions de catégorie A qui assurent une ultime prévention ou limitation des EIH, les exigences de sûreté d'un FSE de catégorie B ne doivent pas nécessairement être aussi élevées que celles relatives à un FSE de catégorie A. Cela permet, si nécessaire, aux FSE de catégorie B d'avoir une fonctionnalité plus élevée que ceux de catégorie A pour ce qui concerne les méthodes de détection de la nécessité de leur mise en service ou dans leurs actions ultérieures.

5.2.3 *Catégorie C*

La catégorie C est utilisée pour désigner les FSE qui ont un rôle indirect ou auxiliaire dans l'exécution ou le maintien de la sûreté nucléaire. La catégorie C recouvre tous les FSE importants pour la sûreté mais qui n'entrent pas dans les catégories A ou B. Ils peuvent participer à la réponse globale à un accident mais ne sont pas directement impliqués dans l'atténuation des conséquences physiques de l'accident.

5.3 *Base de classification*

Les fonctions d'instrumentation de contrôle-commande, ainsi que les systèmes et le matériel qui les produisent (FSE), doivent être évalués en fonction des conséquences de leurs défaillances, tel un non fonctionnement lorsque cela est requis ou un fonctionnement intempestif. Il faut tenir compte également des astreintes de la maintenance et des essais. Il faut considérer l'ensemble des EIH ainsi que l'analyse des séquences significatives d'événements afin d'identifier les fonctions qui doivent être remplies par les systèmes FSE I&C.

L'étude des fonctions accomplies par les systèmes FSE I&C doit déboucher sur l'attribution de la catégorie A, B ou C, ou de la mention "non classé". La mention "non classé" sera attribuée lorsque la fonction ne sera pas jugée significative pour la sûreté.

La présence d'un FSE de catégorie inférieure (respectivement B, C ou "non classé") ne doit pas remettre en cause l'attribution ou la suppression d'un FSE de catégorie supérieure (respectivement A, B ou C).

L'application, à un niveau national, des principes et des critères de cette norme peut conduire à une nomenclature différente des catégories A, B ou C. L'application nationale doit cependant être conforme aux principes, aux critères et aux exigences associées donnés dans cette norme. Cela implique la nécessité d'établir et de documenter la correspondance appropriée avec les catégories définies ci-dessus.

Un FSE I&C correspondant aux systèmes de sûreté, tels que définis dans le Guide de sûreté 50-SG-D8 de l'AIEA, sera généralement affecté à la catégorie A. Les FSE définis dans ce guide comme étant liés à la sûreté seront affectés aux catégories A, B ou C.

5.2 *Description of categories*

5.2.1 *Category A*

Category A denotes the FSE which play a principal role in the achievement or maintenance of NPP safety. These FSE prevent PIEs from leading to a significant sequence of events, or mitigate the consequences of PIEs. Category A FSEs may be accomplished automatically or via manual actions, providing such actions are within the capabilities of human operators. Category A also denotes FSE whose failure could directly cause a significant sequence of events. Category A FSE have high availability requirements. They may be limited in their functionality so that their availability can be very confidently guaranteed.

5.2.2 *Category B*

Category B denotes FSE that play a complementary role to the category A FSE in the achievement or maintenance of NPP safety. The operation of a category B FSE may avoid the need to initiate a category A FSE. Category B FSE may improve or complement the execution of a category A FSE in mitigating a PIE, so that plant or equipment damage or activity release may be avoided or minimized. Category B also denotes FSE whose failure could initiate or worsen the severity of a PIE. Because of the presence of category A FSE to provide the ultimate prevention or mitigation of PIEs, the safety requirements for the category B FSE need not be as high as those for the category A FSE. This allows, if necessary, the category B FSE to be of higher functionality than category A FSEs in their method of detecting a need to act or in their subsequent actions.

5.2.3 *Category C*

Category C denotes FSE that play an auxiliary or indirect role in the achievement or maintenance of NPP safety. Category C includes FSE that have some safety significance, but are not category A or B. They can be part of the total response to an accident but not be directly involved in mitigating the physical consequences of the accident.

5.3 *Basis of classification*

I&C FSE shall be assessed in relation to the consequences of their malfunction, such as failure to operate when required to do so, or spurious operation. Maintenance and testing shall be considered in this assessment. PIEs within the NPP's design basis shall be considered. The consideration shall include the analysis of significant sequences of events, to identify the functions required to be carried out by the I&C FSE.

This consideration of the functions carried out by the I&C FSE shall result in the assignment of each FSE to one of categories A, B or C, or unclassified. An unclassified assignment is made if the FSE is not significant to safety.

The presence of a lower category FSE (respectively B, C or unclassified) shall not avoid the provision of, or deletion of, a higher category FSE (respectively A, B or C).

National application of the principles and criteria of this standard may assign differing nomenclature to categories A, B and C. The national application shall be according to the principles, criteria and associated requirements given in this standard. This shall involve establishing and documenting an appropriate correspondence to the categories defined.

I&C FSE falling within the boundary of the safety systems, as defined in IAEA Safety Guide 50-SG-D8 will generally be assigned to category A. I&C FSE defined as safety related in that guide will be assigned to categories A, B or C.

6 Critères de répartition dans les différentes catégories

Les critères qui doivent être appliqués pour l'attribution aux FSE de la catégorie A, B ou C sont donnés ci-dessous.

Si un FSE ne satisfait à aucun des critères ci-dessous mentionnés, il sera considéré comme non classé.

Dans le cas d'une possibilité de répartition dans plusieurs catégories à la fois, c'est la catégorie la plus haute applicable qui sera en dernier lieu attribuée à chaque FSE et aux sous-FSE nécessaires à l'accomplissement d'un FSE.

6.1 *Catégorie A*

La catégorie A doit être attribuée à un FSE I&C, s'il satisfait à l'un des critères ci-dessous:

a) s'il est requis pour atténuer les conséquences d'un EIH pour prévenir une séquence significative d'événements;

b) si sa défaillance, alors qu'il est appelé à fonctionner suite à un EIH, est susceptible de conduire à une séquence significative d'événements;

c) si sa défaillance ou un défaut le concernant, ne pourrait pas être atténuée par un autre FSE de catégorie A et pourrait conduire directement à une séquence significative d'événements;

d) s'il est requis pour fournir des informations ou des possibilités de commande permettant des actions manuelles destinées à prévenir ou limiter les conséquences d'EIH.

En référence au point d), des facteurs tels que la disponibilité de sources redondantes d'information, la durée suffisante pour l'évaluation par l'opérateur des sources alternatives d'information et le fait que des actions manuelles sont les seuls moyens de limiter les conséquences de la séquence d'événements doivent être pris en considération dans l'attribution d'un FSE d'une catégorie. Si une action manuelle est requise pour préserver la sûreté de la centrale, le FSE I&C qui permet cette action sera affecté à la catégorie A.

6.2 *Catégorie B*

La catégorie B sera attribuée à un FSE I&C, s'il satisfait à l'un des critères ci-dessous et s'il n'a pas été classé dans la catégorie A:

a) s'il agit sur la centrale de manière que les variables de processus soient maintenues dans les limites prévues par l'analyse de sûreté;

b) si une panne ou une défaillance le concernant pouvait nécessiter le fonctionnement d'un FSE de catégorie A afin d'éviter une séquence significative d'événements;

c) s'il est utilisé pour empêcher ou limiter un rejet radioactif mineur ou une dégradation mineure du combustible à l'intérieur du domaine de dimensionnement de la centrale, mais d'importance moindre qu'une séquence significative d'événements[1];

d) s'il est prévu pour alerter le personnel de la salle de contrôle de défaillances dans les FSE de catégorie A;

e) s'il est prévu pour surveiller de manière permanente l'aptitude des FSE de catégorie A à exécuter leur tâche de sûreté lorsqu'ils y sont appelés;

f) s'il est utilisé pour réduire de façon significative la fréquence des EIH, ainsi qu'il est demandé dans l'analyse de sûreté.

---

1) Il faut que la définition d'un rejet radioactif mineur ou d'une dégradation du combustible soit conforme aux pratiques nationales. Un rejet radioactif mineur pourrait être dû au rejet de fluide réfrigérant sans détérioration du combustible. Une dégradation mineure du combustible pourrait occasionner des dommages à une petite surface du gaînage sans rejet de fluide réfrigérant ou perte de la capacité normale de réfrigération du cœur.

6 Assignment criteria

The criteria that shall be applied for assignment of FSE to categories A, B and C are given below.

If an FSE does not meet any of the criteria given below, then it shall be "unclassified".

In the case of multiple assignment, the final assignment of category to each FSE, and to the sub-FSE that are needed to achieve the FSE, shall be the highest applicable category.

6.1 *Category A*

An I&C FSE shall be assigned to category A if it meets any of the following criteria:

a) it is required to mitigate the consequences of a PIE to prevent it from leading to a significant sequence;

b) its failure when required to operate in response to a PIE could result in a significant sequence of events;

c) a fault or failure in the FSE would not be mitigated by another category A FSE, and would lead directly to a significant sequence of events;

d) it is required to provide information or control capabilities that allow specified manual actions to be taken to mitigate the consequences of a PIE to prevent it from leading to a significant sequence.

In reference to point d), factors such as the availability of redundant information sources, sufficient time for operator evaluation of alternative sources of information, and whether the manual actions are the only sources of mitigation of the sequence of events shall be considered in categorizing FSE. If manual action is required to preserve NPP safety, the I&C FSE that enables this action shall be assigned to category A.

6.2 *Category B*

An I&C FSE shall be assigned to category B if it meets any of the following criteria and is not otherwise assigned to category A:

a) it controls the plant so that process variables are maintained within the limits assumed in the safety analysis;

b) a requirement for operation of a category A FSE in order to avoid a significant sequence would result from faults or failures of the (category B) FSE;

c) it is used to prevent or mitigate a minor radioactive release, or minor degradation of fuel, within the NPP design basis, but of less importance than a significant sequence of events[1];

d) it is provided to alert control room staff to failures in category A FSE;

e) it is provided to monitor continuously the availability of category A FSE to accomplish their safety duties;

f) it is used to reduce considerably the frequency of a PIE as claimed in the safety analysis.

---

1) The definition of a minor radioactive release or minor degradation of the fuel shall be according to national practice. A minor radioactive release might be that due to a release of coolant without additional fuel damage. Minor degradation of the fuel might involve damage to a small amount of fuel cladding without release of coolant or loss of ability to cool the core satisfactorily.

6.3 *Catégorie C*

La catégorie C sera attribuée à un FSE I&C s'il satisfait à l'un des critères ci-dessous et s'il n'est affecté ni à la catégorie A ni à la catégorie B:

a) s'il est utilisé pour réduire la fréquence attendue des EIH;
b) s'il est utilisé pour réduire la fréquence des sollicitations ou améliorer les performances des FSE de catégorie A;
c) s'il est utilisé pour enregistrer ou surveiller les conditions des FSE et déterminer leur état de sûreté (prêt à fonctionner, en fonctionnement, en panne ou inopérant), particulièrement pour ceux dont la défaillance provoquerait un EIH;
d) s'il est utilisé pour surveiller et décider d'actions de limitation des conséquences à la suite d'agressions internes à l'intérieur du domaine de dimensionnement de la centrale (par exemple, incendie, inondation);
e) s'il est utilisé pour assurer la sécurité du personnel pendant ou à la suite d'événements impliquant ou risquant de provoquer un rejet de radioactivité dans la centrale ou un risque d'exposition aux rayonnements;
f) s'il est utilisé pour avertir le personnel d'un dégagement important de radioactivité dans la centrale ou d'un risque d'exposition aux rayonnements;
g) s'il est utilisé pour surveiller et décider d'actions de limitation des conséquences suite à des agressions externes (séismes, vent violent);
h) s'il concerne le contrôle d'accès interne à la centrale.

7 Procédure de classification

Un diagramme de la procédure est donné à la figure 1.

7.1 *Identification de la base de conception*

La nature de la centrale et le type de réacteur (par exemple réacteurs à eau pressurisée, réacteurs à eau bouillante ou autre type de réacteur), les EIH associés et les principaux critères de conception sur la redondance des systèmes ou matériels mécaniques et électriques constituent les données principales du processus de classement par catégorie des FSE I&C. Une autre donnée essentielle est l'identification des principaux FSE de limitation des conséquences et leurs systèmes supports pour chaque EIH.

L'attribution de catégories aux FSE dépend de leur rôle dans la prévention ou la limitation des EIH. Le processus de classement par catégories nécessite l'examen du rôle des FSE dans la prévention et la limitation des conséquences des EIH dans tous les modes de fonctionnement et toutes les conditions de la centrale (par exemple la mise en service, le fonctionnement normal, le rechargement en combustible). Un FSE peut en effet jouer un rôle important dans certains modes de fonctionnement seulement et également à la suite d'EIH tels que des événements naturels (par exemple sismiques, inondations, vents violents, orages) et des agressions internes (par exemple incendie, inondations internes, missiles, dégagements radioactifs provenant d'une centrale voisine, rejets chimiques provenant d'autres centrales ou industries).

7.2 *Identification et classement par catégorie des FSE*

A un stade précoce de la conception de la centrale, il faut identifier les fonctions ayant un rôle de sûreté. Il convient que le processus d'identification de ces fonctions et de leur attribution soit à des FSE I&C, soit aux opérateurs humains, soit effectué selon la CEI 964. A la suite de cette identification initiale, une catégorie devra être attribuée aux FSE I&C, selon les critères de l'article 6.

A ce stade initial du processus de conception, il peut s'avérer impossible d'identifier en détail tous les FSE, car les caractéristiques de la centrale n'auront alors pas été définies en totalité. Le processus d'identification et de classification du FSE doit donc se poursuivre itérativement pendant toute la phase de conception. En cas d'incertitude pour l'attribution initiale d'une catégorie à un FSE, il convient d'accompagner ce classement d'un document explicatif.

Les fonctions exécutées par chaque système I&C doivent être passées en revue de manière à identifier les sous-systèmes éventuels des FSE et leur attribuer une catégorie appropriée.

6.3 *Category C*

An I&C FSE shall be assigned to category C if it meets any of the following criteria and is not otherwise assigned to category A or category B:

a) it is used to reduce the expected frequency of a PIE;
b) it is used to reduce the demands on, or to enhance the performance of, a category A FSE;
c) it is used for the surveillance or recording of conditions of FSE, to determine their safety status (fit for operation, operating, failed or inoperative), especially those whose malfunction could cause a PIE;
d) it is used to monitor and take mitigating action following internal hazards within the NPP design basis (e.g. fire, flood);
e) it is used to ensure personnel safety during or following events that involve or result in release of radioactivity in the NPP, or risk of radiation exposure;
f) it is used to warn personnel of a significant release of radioactivity in the NPP or of a risk of radiation exposure;
g) it is used to monitor and take mitigating action following natural events (e.g. seismic disturbance, extreme wind);
h) it is the NPP internal access control.

7 Classification procedure

An outline of the procedure is shown in figure 1.

7.1 *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, lightning), and internal hazards (e.g. fire, internal flood, missiles, radioactive release from adjacent NPP, or chemical releases from other plants or industries).

7.2 *Identification and categorization of FSE*

At an early stage in the design of the NPP, functions with a safety role shall be identified. The process of identifying these functions and assigning them to the I&C FSE or to the human operators should be carried out according to IEC 964. Following this initial identification of FSE, a category for each FSE shall be assigned according to the criteria of clause 6.

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 an FSE to a category is uncertain, then an explanatory note should be added to the categorization.

The functions carried out by each I&C system shall be reviewed, to identify the sub-FSE within the FSE and to assign the appropriate category to each sub-FSE.

Du fait que certains FSE peuvent avoir des missions multiples, le processus de répartition peut amener les mêmes FSE à figurer dans plusieurs catégories. Dans ce cas, l'attribution finale pour chaque FSE et pour les sous-FSE nécessaires à sa réalisation doit correspondre à la catégorie la plus élevée.

A mesure que la redondance, la diversité et les autres exigences techniques des FSE sont connues avec plus de précision, par exemple avec l'avancement de l'analyse de sûreté et le développement des procédures de conduite, la liste de catégories doit être affinée et révisée pour en tirer la liste finale. Celle-ci doit figurer dans la documentation nécessaire à l'obtention de l'autorisation de fonctionnement de la centrale et à son maintien.

8 Détermination des prescriptions

Les exigences de conception garantissent l'adéquation de chaque système à son importance pour la sûreté de la centrale. Les exigences concernent la garantie de la fonctionnalité, des performances, de la fiabilité, de la résistance aux conditions d'ambiance, de l'assurance de la qualité (AQ) et du contrôle de la qualité (CQ).

La conformité aux codes et les normes appropriés pendant la phase de conception, la qualification du matériel à résister aux incidents de fonctionnement prévus, ainsi que les procédures AQ et CQ pendant les phases de conception, de fabrication, d'installation et d'exploitation sont nécessaires pour garantir que le fonctionnement des FSE sera conforme aux spécifications fonctionnelles. Les codes, guides et normes énumérés à l'article 2 de cette norme sont des références normatives et constituent donc des dispositions de celle-ci.

Il convient d'utiliser, si possible, des FSE pourvus d'un retour d'expérience prouvé et documenté de fonctionnement fiable dans des installations nucléaires ou d'autres applications industrielles.

8.1 *Prescriptions pour la garantie de fonctionnalité*

8.1.1 *Prescriptions générales*

La prescription de base pour garantir la fonctionnalité consiste en l'existence d'une spécification fonctionnelle claire, complète et non ambiguë qui doit servir de base aux vérifications du FSE pendant la conception, la fabrication, l'installation et l'exploitation, et doit servir de référence pour toutes modifications en exploitation.

8.1.2 *Prescriptions spécifiques*

a) *Catégorie A*

Les activités de conception doivent être menées conformément aux prescriptions des codes, guides et normes en vigueur, adaptées au niveau élevé de garantie de fonctionnalité demandé pour un FSE de catégorie A. La conception doit viser à faciliter la vérification de la fonctionnalité avec un souci de simplicité. Cela doit avoir pour conséquence le report des fonctions ayant une importance moindre pour la sûreté hors du système. (Par exemple, il convient que les calculs d'affichages spéciaux et la traduction de protocoles de communications ne soient pas effectués par le logiciel du système de sûreté.) En cas d'utilisation de matériel informatique, il faut se conformer aux prescriptions de la CEI 880 et de la CEI 987.

b) *Catégorie B*

La conception doit être assurée à partir de codes, de guides et de normes reconnus, tels par exemple la démarche de conception décrite dans la CEI 964 pour la salle de commande, ou en particulier des systèmes et matériels possédant un retour d'expérience de fonctionnement satisfaisant dans une application similaire peuvent être utilisés.

c) *Catégorie C*

On doit vérifier que les systèmes et matériels ont été conçus ou essayés pour remplir les fonctions spécifiées dans toutes les conditions de fonctionnement, y compris les conditions les plus défavorables de fonctionnement prévues ou lors d'événements pendant lesquels la fonction est requise.

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 category to each FSE, and to the sub-FSE that are needed to achieve the FSE, shall be the highest applicable category.

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 shall be refined and revised, to derive a final list. This list shall be included in the documentation that is required to obtain and maintain the NPP operating licence.

8 Determination of requirements

The design criteria are the requirements by which the adequacy of FSE in relation to their importance to plant safety are ensured. The criteria are those concerned with the ensurance of functionality, performance, reliability, environmental durability, and QA and QC.

To ensure that the FSE as designed will function as stipulated by the functional specification requires compliance with adequate codes and standards during the design phase, qualification of the equipment to survive anticipated operational occurrences, and QA and QC during the design, manufacture, installation and service phases. The codes, guides and standards listed in clause 2 of this standard are normative references and therefore are provisions of this standard.

Wherever possible, FSE with a documented, proven history of reliable operation in nuclear or other industrial applications should be used.

8.1 *Requirements for ensurance of functionality*

8.1.1 *Basic requirements*

The basic requirement for ensurance of functionality is the existence of clear, comprehensive and unambiguous functional requirements and design specifications against which the FSE shall be checked during design, manufacture, installation, and service, and shall be used as a reference for any in-service modifications.

8.1.2 *Specific requirements*

a) *Category A*

The design shall be according to the requirements of recognized codes, guides and standards that are appropriate to the high level of ensurance of functionality required for a category A FSE. The design shall aim to ease verification by maintaining simplicity. This shall result in the exclusion of lower category functions from the FSE. (For example, special display calculations and translation of communication protocols should not be carried out by safety system software.) Where computer equipment is used, the requirements of IEC 880 and IEC 987 shall be met.

b) *Category B*

The design process shall be carried out following appropriate recognized codes, guides and standards (such as the design process described in IEC 964 for main control rooms), or systems and equipment with a documented history of satisfactory operation in a similar application may be used.

c) *Category C*

The design should be examined to verify that the systems and equipment have been designed or tested to provide the specified functions under the full range of operating conditions, including the most adverse anticipated operational conditions or occurrences under which the function is required.

8.2 *Prescriptions pour la garantie de la fiabilité*

8.2.1 *Prescriptions générales*

La fiabilité requise pour tous les FSE de catégorie A, B ou C doit être déterminée soit à partir d'une évaluation probabiliste de sûreté quantitative de la centrale, soit à partir de jugements qualitatifs d'ingénieur, et comprise dans la spécification. Ces analyses doivent être exécutées de manière structurée selon des procédures approuvées et doivent être documentées.

Bien que les exigences de fiabilité pour les FSE dans les différentes catégories puissent être identiques, le niveau de garantie de l'aptitude du FSE à respecter la fiabilité spécifiée sera différent dans les trois catégories; la catégorie A nécessitera le niveau de garantie le plus élevé.

Les prescriptions de base pour garantir une fiabilité élevée reposent sur une redondance ou une diversification appropriées et une séparation et/ou ségrégation spatiale, géographique, physique et électrique. Pour tous les FSE, il faut étudier les moyens de détection des défauts et de réparation pendant la conception et les modifications ultérieures.

L'évaluation de la fiabilité et de la disponibilité doit prendre en compte les périodes de réparation, d'essais et de maintenance, et la possibilité de défaillances autorévélées ou non. Les hypothèses de l'analyse de fiabilité concernant les périodes de maintenance, d'essais et de réparations doivent être vérifiées pendant le fonctionnement et des actions correctives entreprises en cas d'anomalies.

8.2.2 *Prescriptions spécifiques*

a) *Catégorie A*

Les systèmes appartenant à cette catégorie doivent être redondants, de manière à satisfaire au minimum au critère de défaillance unique. Leur conception doit reposer sur une séparation et/ou une ségrégation appropriées pour assurer qu'un événement interne unique ne peut pas empêcher le fonctionnement des trains redondants du système.

L'application du critère de défaillance unique doit être faite, conformément au Code 50-C-D de l'AIEA (Rév. 1), alinéas 329 à 336.

Les exigences de fiabilité des FSE I&C de catégorie A doivent être spécifiées comme précisé en 8.2.1. Il faut donc établir des prescriptions de fiabilité pour les fonctions nécessaires à l'obtention d'un risque suffisamment faible d'une séquence significative d'événements et d'en tirer ensuite des exigences de fiabilité pour les systèmes et matériels I&C. La fiabilité des systèmes I&C nécessaires à la fonction doit être ensuite évaluée et comparée à la spécification. S'il existe des discordances, celles-ci doivent être résolues.

L'évaluation de fiabilité doit prendre en compte les effets des défaillances en mode commun, y compris les défaillances de matériel, de logiciel et les erreurs humaines pendant le fonctionnement en puissance et les opérations de maintenance, de modification et de réparation. Les techniques utilisées pour évaluer ces effets vont du jugement purement qualitatif d'ingénieur aux analyses quantitatives détaillées, elles-mêmes dépendantes d'estimations qualitatives. Le type d'analyse choisi doit être en accord avec les exigences de fiabilité, la technique devant être d'autant plus rigoureuse que l'exigence de fiabilité est plus élevée.

Lorsque l'examen des effets des défaillances de mode commun, incluant notamment les défaillances de logiciel ou des erreurs humaines, met en évidence des limites à la fiabilité des systèmes redondants, la diversification peut s'avérer nécessaire pour ce FSE[1]. La fonction concernée peut alors nécessiter deux ou plusieurs systèmes ou sous-systèmes, différents les uns des autres.

---

1) Pour un système individuel incluant des logiciels développés selon les plus hauts critères de qualité (CEI 880 et CEI 987), un objectif de fiabilité de l'ordre de 10^{-4} défaillance/demande peut être demandé après la prise en considération de toutes les contraintes de spécifications, de conception, de fabrication, d'installation, de fonctionnement et de maintenance. Cette valeur inclut les risques de mode commun dans les voies redondantes du système et s'applique à la totalité de la chaîne fonctionnelle des capteurs via le traitement jusqu'aux équipements commandés. Des exigences de fiabilité supérieure à celle-ci ne sont pas exclues, mais elles devront reposer sur une justification appropriée prenant en compte tous les éléments mentionnés.

8.2 *Requirements for ensurance of reliability*

8.2.1 *Basic requirements*

The reliability required from any FSE in categories A, B or C shall be determined by either a quantitative probabilistic assessment of the NPP, or by qualitative engineering judgement, and included in the specification. These analyses shall be carried out in a structured way to a set of approved procedures, and shall be documented.

Although the reliability requirements for FSEs in different categories may be the same, the level of ensurance that the FSE will achieve the specified reliability will be different for the three categories, with category A requiring the highest ensurance.

The basic requirements for ensuring high reliability concern the provision of appropriate redundancy, diversity and spatial, geographical, physical and electrical separation and/or segregation. For all FSEs, means of fault detection and repair shall be considered during design and subsequent modifications.

The assessments of reliability and availability shall take account of repair periods, testing and maintenance periods, and the potential for both self-revealed and non-self-revealed failure. The assumptions made in the reliability analysis with respect to maintenance, testing, and repair periods shall be verified during operation, and corrective action taken if discrepancies are noted.

8.2.2 *Specific requirements*

a) *Category A*

A category A FSE shall have redundancy so that the single failure criterion is met as a minimum. Appropriate separation and/or segregation shall be employed to ensure that single internal hazards cannot disable redundant trains of the FSE.

The application of the single failure criterion shall be following IAEA Code 50-C-D (Rev. 1), paragraphs 329 to 336.

The reliability requirements for category A I&C FSE shall be specified as indicated in 8.2.1. This shall be carried out by establishing the reliability requirements for the functions needed to achieve an acceptably low risk of a significant sequence of events, and then by determining from this the reliability requirements for the I&C FSE. The reliability of the I&C FSEs that are necessary to achieve the function shall then be assessed and compared to the specification. If discrepancies exist, these shall be resolved.

The reliability assessment shall consider the effects of common mode failures, including hardware failures, software failures, and human errors during operation, maintenance, alteration and repair activities. The techniques used to assess these effects range from purely qualitative engineering judgement to detailed quantitative analyses, which may themselves depend on qualitative estimates. The type of analysis chosen shall be consistent with the reliability requirement, the higher the reliability requirement, the more rigorous the technique.

Where consideration of the effects of common mode failures, such as software failures or human error, shows limits on achievable reliability for redundant FSEs, then diversity may be necessary for that FSE[1]. The function concerned may then require two or more sub-FSEs, diverse from one another.

1) For an individual system which incorporates software developed in accordance with the highest quality criteria (IEC 880 and IEC 987), a figure of the order of 10^{-4} failure/demand may be an appropriate limit to place on the reliability that may be claimed, when all of the potential sources of failure due to the specification, design, manufacture, installation, operating environment, and maintenance practices, are taken into account. This figure includes the risk of common mode failure in the redundant channels of the system, and applies to the whole of the system, from sensors through processing to the outputs to the actuated equipment. Claims for better reliabilities than this are not precluded, but will need special justification, taking into account all of the factors mentioned.

Pour les systèmes de catégorie A, une procédure d'analyse des modes de défaillance et de leurs effets (AMDE) doit être réalisée conformément à la CEI 812. L'analyse doit être conduite à un niveau de détail conforme au niveau d'intégration de la conception, allant du niveau composant pour les FSE simples avec peu de composants jusqu'au niveau module pour les FSE hautement intégrés.

Lorsqu'un système comporte des auto-tests intégrés et que ceux-ci font partie de l'analyse de fiabilité du système, l'AMDE doit en faire une évaluation pour déterminer le taux de couverture. Lorsque l'AMDE fait apparaître que certaines défaillances risquent de ne pas être détectées et révélées aux opérateurs par les autotests du FSE, des essais doivent être réalisés pour les mettre en évidence. Les intervalles séparant ces essais doivent être déterminés à partir de la fréquence présumée des défaillances non détectées et de la fiabilité exigée du système.

Si l'on ne dispose pas de données de fiabilité, les intervalles entre les essais seront déterminés en fonction de ceux pratiqués pour des FSE similaires. A mesure que l'on dispose de plus d'expérience en ce domaine, les intervalles entre les essais feront l'objet d'une nouvelle évaluation.

b) *Catégorie B*

La fiabilité souhaitée pour cette catégorie de système doit être établie et comparée à la fiabilité calculée du FSE. Il est souhaitable que les systèmes de cette catégorie soient dotés d'une redondance, mais cela n'est pas indispensable si le FSE peut remplir ses objectifs de fiabilité sans cela. Si la redondance n'est pas prévue, le FSE doit faire l'objet d'une évaluation systématique afin d'identifier les défaillances uniques qui peuvent empêcher son fonctionnement; il faut analyser la probabilité et les conséquences pour la sûreté de ces défaillances. Lorsque l'amplitude ou la fréquence des effets pour la sûreté rendent inacceptables les conséquences des défaillances uniques, la redondance doit être prévue.

Les composants utilisés doivent présenter une qualité et une fiabilité élevées, et des moyens pour assurer que ces défauts peuvent être rapidement détectés et réparés doivent être prévus.

c) *Catégorie C*

Les systèmes de cette catégorie ne nécessitent généralement pas de redondance, mais celle-ci peut être prévue si nécessaire pour que le FSE puisse remplir ses objectifs de fiabilité.

Pour les systèmes de catégorie C, où la redondance est nécessaire à la disponibilité spécifiée, il convient d'évaluer la fiabilité et d'étudier la redondance comme pour la catégorie B.

8.3 *Prescriptions pour la garantie des performances*

8.3.1 *Prescriptions générales*

Les prescriptions de base pour garantir les performances sont les suivantes:

a) Les prescriptions de performance doivent être spécifiées.

b) Un programme d'assurance de la qualité doit être établi conformément au Code 50-C-AQ de l'AIEA, qui requiert la définition et la vérification des spécifications de performances et d'essais.

c) Les essais de composants, modules, sous-systèmes et systèmes doivent être menés conformément au plan d'assurance de la qualité pour faire la preuve de leurs performances satisfaisantes pendant les périodes de fabrication, d'assemblage et d'installation sur le site, selon leur catégorie.

   Des essais suffisants doivent être effectués en usine sur les composants, modules et sous-systèmes pour garantir que le FSE, avec l'assurance de la qualité de la fabrication, fonctionne conformément à la spécification requise. Il faut effectuer des essais combinés des systèmes I&C avec les systèmes mécaniques et fluides de la centrale, avant la mise en service de la centrale, dans une configuration nécessitant la disponibilité des fonctions de sûreté fournies par le FSE.

   Les essais sur site ont le même objectif quelle que soit la catégorie, toutefois, le contrôle de la qualité et les exigences de documentation varient selon la catégorie, conformément aux prescriptions de 8.5.

For category A FSEs, a failure mode and effect analysis (FMEA) shall be carried out following IEC 812. The detail of the analysis shall be at a level consistent with the level of integration of the design, such as at the component level for simple FSEs with few components, and at a module level for highly integrated FSEs.

Where a FSE has built-in self-testing features, and these are claimed as part of the reliability analysis of the FSE, the FMEA shall assess these features to find the coverage of the self tests. Where the FMEA shows that some failures may not be detected and revealed to the operators by the FSE's self-testing features, then proof tests shall be developed to reveal such failures. The intervals for the proof test shall be determined from the likely frequency of occurrence of the undetected failure and the reliability required of the FSE.

Where reliability data is not available, the test interval shall be chosen by comparison with other similar FSE. As experience is accumulated, the test interval for the FSE shall be re-evaluated.

b) *Category B*

The required reliability for the FSE shall be established and compared to the calculated reliability of the FSE as designed. It is desirable that an FSE in this category should have redundancy, but this is not essential if the FSE can achieve its reliability targets without it. If redundancy is not provided, the FSE shall be systematically evaluated to identify single failures that can prevent its operation, and the likelihood and safety consequences of these failures shall be analysed. Where the consequences of single failures are not acceptable because of the magnitude or frequency of their effect on safety, redundancy shall be provided.

The components employed shall be shown to be of high quality and reliability, and means to ensure that faults can be quickly detected and repaired shall be incorporated.

c) *Category C*

An FSE in this category does not generally need redundancy, but this may be provided if it is necessary in order for the FSE to achieve its specified reliability.

For category C FSEs where redundancy is necessary to achieve the specified availability, reliability should be assessed and redundancy considered as for category B.

8.3 *Requirements for ensurance of performance*

8.3.1 *Basic requirements*

The basic requirements for ensurance of performance are that:

a) Performance requirements shall be specified.

b) A QA programme shall be established according to IAEA Code 50-C-QA. This shall require specifications of performance and testing to be defined and verified.

c) Testing of components, modules, subsystems, and FSEs shall be carried out according to the QA plan to show satisfactory performance during manufacturing, assembly, and site installation periods, as appropriate to the category of the FSE.

   Tests shall be carried out on components, modules and subsystems to ensure that, with the manufacturing QA, the FSE operates according to the requirements specification. Combined tests of the installed I&C FSE with the mechanical and fluid systems shall take place at the NPP before operation of the NPP in a mode requiring the availability of the safety functions provided by the FSE.

   The intent of the site tests is the same, regardless of category, but the quality control and documentation requirements vary according to category, as stated in 8.5.

d) Des essais périodiques et/ou des essais durant le fonctionnement doivent avoir lieu pendant la période d'exploitation de la centrale, pour prouver le maintien des performances et de la disponibilité. Les essais doivent être conçus de façon à détecter les défaillances dans le matériel. Les défauts identifiés doivent être corrigés selon une procédure de contrôle de modification. Il faut conserver les enregistrements de ces corrections.

e) Lorsque des équipements informatiques sont utilisés, un programme de qualité sur le cycle de vie du logiciel doit être prévu en cohérence avec la catégorie du FSE.

8.3.2 *Prescriptions spécifiques*

a) *Catégorie A*

Des essais de type du matériel doivent être réalisés afin de montrer qu'un matériel de construction identique à celui qui doit être installé dans la centrale fonctionne comme prévu à la conception, lorsqu'il est placé dans l'environnement d'exploitation prévu.

Des essais fonctionnels des composants, modules, sous-systèmes et, si possible, des FSE complets, doivent être réalisés. Ces essais doivent être certifiés par le client ou son représentant.

En cas d'utilisation de matériel informatique, le système doit être soumis à une vérification et à une validation formelles, selon la CEI 880 et la CEI 987.

Les essais fonctionnels peuvent être effectués soit en usine, soit sur le site. Que les essais soient effectués en usine ou sur le site, on doit s'assurer que l'ensemble des fonctions et des équipements ont été testés. Lorsqu'il n'est pas possible d'apporter cette démonstration, des justifications particulières doivent être présentées.

Les essais sur le site doivent, dans la mesure du possible, vérifier que toutes les fonctions de sûreté spécifiées des systèmes et des matériels installés peuvent être réalisées avec les performances requises. Ces essais doivent prendre en considération les variations des paramètres de fonctionnement. Ces essais constituent la recette site et doivent être certifiés par le client ou son représentant.

En cas d'utilisation de matériel informatique, un programme de qualité sur le cycle de vie du logiciel doit être prévu conformément à la CEI 880.

Les essais certifiés effectués lors du réacteur en fonctionnement et/ou les essais périodiques doivent prouver la capacité de réaliser toutes les fonctions de sûreté requises. Les essais périodiques doivent permettre de démontrer la capacité fonctionnelle de tous les sous-FSE nécessaires à la réalisation du FSE soumis à l'essai. On peut prévoir des intervalles de l'ordre de 1 mois à 1 an entre les essais, selon la complexité, et le degré de fonctionnement dynamique et d'autotests mis en œuvre dans la conception.

Les essais peuvent nécessiter la suppression des signaux de sortie, ou la prévision de lignes de contournement. S'il est prévu des lignes de contournement, leur mise en œuvre doit être justifiée pour prouver qu'elles ne risquent pas d'empêcher le FSE de réaliser ses fonctions de sûreté spécifiées. Leur utilisation pourra par exemple être physiquement restreinte à un seul train de FSE redondant à la fois.

Pour certains FSE, il convient que la conception comprenne un niveau de redondance permettant la réalisation d'essais périodiques pendant le fonctionnement de la centrale. Ces FSE sont ceux susceptibles de n'être pas suffisamment fiables ou efficaces sans essais périodiques, qu'il ne serait pas possible d'essayer pendant le fonctionnement de la centrale dans des situations pouvant exiger leur disponibilité et qui sont dépourvus de dispositifs d'autotests capables de déceler toutes les défaillances. Il n'est pas nécessaire de prévoir une redondance pour le FSE complet, mais seulement pour les parties qui doivent être essayées pendant le fonctionnement du système.

b) *Catégorie B*

Des essais de type de matériel doivent être réalisés afin de montrer qu'un matériel de construction similaire à celui devant être installé dans la centrale fonctionne comme prévu à la conception lorsqu'il est placé dans l'environnement d'exploitation prévu et spécifié en 8.4.2 b). La démonstration doit être apportée que les différences éventuelles entre les matériels ne remettent pas en cause les résultats des essais.

d) On-line and/or periodic testing shall take place during operation to show that performance is maintained. The testing shall be designed to detect failures within the equipment and any deficiencies identified shall be corrected following a change control procedure. Suitable records of those corrections shall be kept.

e) Where computer equipment is used, a software life cycle quality programme appropriate to the category of the FSE shall be implemented.

8.3.2 *Specific requirements*

a) *Category A*

Type testing shall have been carried out to show that equipment of identical construction to that to be installed at the NPP will function as required by the design when subjected to the anticipated operating environment.

Functional testing of components, modules, subsystems and, whenever practicable, complete FSEs, shall be carried out. These tests shall be witnessed by the licensee, or his representative.

Where computer equipment is used, the system shall be subject to formal verification and validation following IEC 880 and IEC 987.

Functional testing may be performed at the factory or at the site. Tests performed at the factory and at the site shall be co-ordinated to ensure that a full coverage of testings is achieved. Where it is not possible to prove that all of the specified functions can be achieved, special justification shall be provided.

Site testing shall test, as far as practicable, that all specified safety functions of the installed systems and equipment can be achieved with the required performance. This testing shall take into account variations in operating parameters. This is the site acceptance test (SAT), and shall be witnessed by the licensee, or his representative.

Where computer equipment is used, a software life cycle quality programme in accordance with IEC 880 shall be implemented.

On-line and/or periodic tests shall show the ability to carry out all required safety functions. The periodic testing shall include confirmation of the functional capacity of all sub-FSEs that are needed to achieve the FSE being tested. Test intervals for category A items may be expected to be about monthly to annually, depending on the complexity, and the degree of dynamic operation and self-testing implemented in the design.

Testing may require suppression of output signals, or the provision of bypass facilities. If bypass facilities are incorporated, their integrity shall be justified to show that they cannot be applied in a way that would prevent the FSE achieving its specified safety functions. For example, their use might be physically restricted to a single train of a redundant FSE at a time.

For some FSEs, the design should include redundancy that allows routine testing during plant operation. Such FSEs would be those that cannot be shown to be sufficiently reliable or effective without periodic tests, which it would not otherwise be possible to test with the plant operating in the mode where the FSE is required to be available, and which do not incorporate self-testing features that can reveal all failures. It is not necessary to incorporate redundancy for the whole FSE, only for those parts that must be tested with the system in service.

b) *Category B*

Type testing shall have been carried out to show that equipment of similar construction to that to be installed at the NPP will function as required by the design when subjected to the anticipated operating environment, as specified in 8.4.2 b), provided that analysis has been performed to show that differences in the equipment do not invalidate the test results.

Les essais fonctionnels doivent être effectués avant la mise en service de façon à montrer que toutes les fonctions spécifiées peuvent être obtenues par les systèmes utilisant des matériels similaires (au sens du paragraphe précédent) à ceux installés dans la centrale. Tout ou partie des essais peuvent être effectués sur le site.

Lorsque des équipements informatiques sont utilisés, les logiciels doivent être développés selon la démarche structurée en accord avec la CEI 880. Cependant, pour la catégorie B, l'application des exigences les plus sévères de la CEI 880 n'est pas imposée[1].

Les recettes sites doivent montrer, dans la mesure où cela est réalisable, que toutes les fonctions de sûreté requises du matériel installé peuvent être obtenues. Les essais du matériel de commande doivent indiquer la capacité à répondre correctement aux transitoires et aux modifications de demande. Les essais du matériel d'affichage et d'alarme doivent comprendre des essais d'injection des signaux d'entrée pertinents afin de prouver que les performances sont satisfaisantes.

Les essais durant le fonctionnement et les essais périodiques de performances doivent permettre de démontrer la capacité fonctionnelle des sous-systèmes.

Il convient de choisir les intervalles entre les essais de manière que le taux prévu de défaillance ou de non fonctionnement sur sollicitation soit conforme aux prescriptions de l'analyse de fiabilité.

c) *Catégorie C*

Le client peut considérer que les essais effectués en usine sont de nature à démontrer le respect des performances requises. Des essais de type et des essais fonctionnels peuvent être effectués si nécessaire, mais ils ne sont pas exigés en règle générale.

Une recette site (RS) peut être réalisée sur le site de la centrale, afin de prouver que le FSE répond aux spécifications de fonctionnalité et de performances.

Les essais périodiques des performances peuvent se limiter à des vérifications lors de périodes de rechargement du combustible ou lors d'autres périodes d'arrêt. A titre de guide, ce type d'essais doit être réalisé à intervalles ne dépassant pas 1 ou 2 ans. Lorsqu'une redondance est prévue, il convient de prévoir des essais individuels de la capacité fonctionnelle de tous les FSE ou sous-FSE redondants. Cette prescription pourra être satisfaite au moyen d'essais en continu.

8.4 *Prescriptions pour la garantie de la résistance aux conditions d'ambiance*

8.4.1 *Prescriptions générales*

Il est nécessaire de s'assurer que les conditions d'environnement auxquelles le FSE peut être soumis pendant et après un EIH ne provoqueront pas de défaillances dans le système. Cette assurance peut être fournie par la qualification formelle du matériel ou grâce à d'autres techniques.

8.4.2 *Prescriptions spécifiques*

a) *Catégorie A*

Les mesures prises pour garantir la continuité de fonctionnement d'un FSE de catégorie A dans toutes les conditions prévues doivent comprendre la qualification formelle du matériel, selon la CEI 780 pour les conditions d'environnement et la CEI 980 pour les conditions sismiques. Les résultats des essais doivent être enregistrés et conservés dans les dossiers durant toute la vie de la centrale. Toutes les défaillances survenant pendant les essais de qualification doivent faire l'objet d'investigations; leur cause et leur remède doivent être documentés.

La qualification du matériel de catégorie A peut être démontrée soit par des essais, soit par l'analyse, soit par la combinaison des deux méthodes, soit encore avec les données du retour d'expérience disponibles.

---

1) Les futurs amendements à la CEI 880 comporteront des prescriptions spécifiques pour les logiciels des systèmes de catégorie B.

Functional testing shall have been carried out prior to operation to show that each specified function can be achieved by systems using equipment of similar construction to that to be installed at the NPP. Some or all of this testing may be done at site.

Where computer equipment is used, the software shall be developed in a systematic structured fashion in accordance with the intent of IEC 880. However, full application of the most rigorous requirements of IEC 880 is not required. [1]

SAT testing shall show, as far as practicable, that all specified safety functions of the installed equipment can be achieved. Tests of control equipment shall show the ability to respond correctly to transients and changes in demand. Testing of display and alarm equipment shall include injection tests of relevant input signals to show satisfactory performance.

On-line and/or periodic testing of performance shall include confirmation of the functional capacity of sub-FSEs.

The test interval shall be chosen so that the assessed failure rate or probability of failure to operate on demand meets the requirements of the reliability analysis.

c) *Category C*

The licensee may accept that the manufacturer's tests are adequate to demonstrate that the specified performance will be achieved. Specific type and functional testing should be performed when necessary, but is not normally required.

SATs should be carried at the NPP site to show that the FSE achieves the specified functionality and performance.

Periodic testing of performance may be limited to checks at refuelling outages, or at similar shutdown periods. As a guide, such testing shall be carried out at intervals no longer than 1 or 2 years. Where redundancy is provided, individual checks of the functional capacity of all redundant FSEs or sub-FSEs shall be included. On-line tests are a means of meeting this requirement.

8.4 *Requirements for ensurance of environmental durability*

8.4.1 *Basic requirements*

It is necessary to provide ensurance that the FSEs will not fail due to the environmental conditions that they may be subjected to during and following a PIE. This ensurance may be provided by formal qualification of the equipment, or by other techniques.

8.4.2 *Specific requirements*

a) *Category A*

The measures taken to provide ensurance that category A FSE will continue to operate under all anticipated operating conditions shall include formal equipment qualification, following IEC 780 for environmental and IEC 980 for seismic conditions. The results of the tests shall be recorded and retained in the lifetime records of the NPP. Any failures during the qualification tests shall be investigated, and the cause and cure of the failure documented.

The qualification of category A equipment may be achieved using one, or a combination of several different methods: by tests, by analysis, a combination of these two, or possibly by using available experience data.

---

1) Future amendments to IEC 880 will contain specific requirements for software in category B systems.

b) *Catégorie B*

Le matériel appartenant à la catégorie B peut nécessiter une qualification formelle. L'environnement prévu le plus défavorable où le matériel sera amené à fonctionner doit être établi et indiqué dans la spécification de qualification; il conviendra d'examiner systématiquement la conception du matériel par rapport à cette spécification.

Lorsque le matériel est nouveau, ou appelé à fonctionner dans des conditions pour lesquelles un produit du marché n'est pas normalement conçu (comme un séisme ou des conditions d'environnement extrêmes), un ensemble de règles doit être établi pour servir de base à la conception du matériel ou à l'évaluation d'une conception existante. Ces règles doivent être basées sur l'expérience acquise à partir des prescriptions de conception particulières du matériel de catégorie A.

c) *Catégorie C*

Le matériel de catégorie C peut être accepté selon les normes commerciales courantes, sauf si son rôle nécessite une qualification particulière, à savoir des prescriptions sismiques ou des spécifications particulières contre les incendies; ou bien s'il doit empêcher les surtensions ou la perturbation électrique des matériels de la catégorie C d'affecter des FSE de catégorie A ou B. Les demandes de fonctionnement dans des conditions anormales d'environnement doivent conduire à l'existence de dossiers spécifiés.

8.5 *Prescriptions en matière d'assurance de la qualité/contrôle de la qualité (AQ/CQ)*

8.5.1 *Prescriptions générales*

Les objectifs du contrôle de la qualité sont la gestion de la conception, le contrôle des modifications et la traçabilité des actions effectuées. La conception doit être documentée de façon suffisamment détaillée pour constituer un support à la fabrication, l'installation, la mise en service et les phases opérationnelles de la centrale. On veillera en particulier à prévoir une documentation permettant de futures modifications de la conception.

En outre, les dispositions en matière d'AQ/CQ, en termes de développement et d'essais particuliers, devraient être adaptées au caractère novateur ou à la complexité d'une conception nouvelle ou lors de modifications. Il y a lieu que ces activités de développement soient documentées selon les besoins, pour étayer toute demande ayant trait à l'importance pour la sûreté du FSE.

8.5.2 *Prescriptions spécifiques*

a) *Catégorie A*

Les prescriptions d'AQ doivent être conformes au Code de l'AIEA 50-C-AQ. La documentation doit permettre l'établissement d'un historique, comprenant à la fois la conception, la fabrication et les aspects de fonctionnement des équipements. Elle doit comprendre tous les équipements jusqu'au niveau du module. La configuration doit faire l'objet de contrôles jusqu'à l'élément le plus petit identifiable. L'identification des numéros des lots, des matériels, etc., doit être étendue à tout le système jusqu'au niveau des modules individuels.

La documentation de CQ doit permettre à un contrôleur de remonter d'un élément du logiciel ou du matériel jusqu'à la spécification qui définit les prescriptions le concernant et de redescendre à partir d'une prescription jusqu'au composant qui la met en œuvre.

b) *Catégorie B*

Le niveau d'AQ appliqué au FSE de catégorie B peut être inférieur à celui appliqué à un FSE de catégorie A, bien que le programme d'AQ doive être cohérent avec celui de la catégorie A. Les prescriptions pour la documentation et la traçabilité doivent être celles utilisées en pratique commerciale courante.

c) *Catégorie C*

Le FSE de catégorie C peut être accepté à un niveau commercial d'AQ avec un CQ correspondant.