IEC 62340

Edition 1.0 2007-12

INTERNATIONAL STANDARD

NORME INTERNATIONALE

Nuclear power plants – Instrumentation and control systems important to safety – Requirements for coping with common cause failure (CCF)

Centrales nucléaires de puissance – Systèmes d'instrumentation et de contrôle-commande importants pour la sûreté – Exigences permettant de faire face aux défaillances de cause commune (DCC)

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

PRICE CODE
CODE PRIX

T

ICS 27.120.20

ISBN 2-8318-9452-2

CONTENTS

FOREWORD 3
INTRODUCTION 5

1 Scope 7
2 Normative references 8
3 Terms and definitions 8
4 Abbreviations 12
5 Conditions and strategy to cope with CCF 13
5.1 General 13
5.2 Characteristics of CCF 13
5.3 Principal mechanisms for CCF of digital I&C systems 13
5.4 Conditions to defend against CCF of individual I&C systems 14
5.5 Design strategy to overcome CCF 15
6 Requirements to overcome faults in the requirements specification 15
6.1 Deriving the requirements specification for the I&C from the plant safety design base 15
6.2 Application of the defence-in-depth principle and functional diversity 16
6.3 CCF related issues at existing plants 17
7 Design measures to prevent coincidental failure of I&C systems 17
7.1 The principle of independence 17
7.2 Design of independent I&C systems 18
7.3 Application of functional diversity 18
7.4 Avoidance of failure propagation via communications paths 19
7.5 Design measures against system failure due to maintenance activities 19
7.6 Integrity of I&C system hardware 19
7.7 Precaution against dependencies from external dates or messages 20
7.8 Assurance of physical separation and environmental robustness 20
8 Tolerance against postulated latent software faults 20
9 Requirements to avoid system failure due to maintenance during operation 21

Annex A (informative) Relation between IEC 60880 and this standard 22

INTERNATIONAL ELECTROTECHNICAL COMMISSION

NUCLEAR POWER PLANTS – INSTRUMENTATION AND CONTROL SYSTEMS IMPORTANT TO SAFETY – REQUIREMENTS FOR COPING WITH COMMON CAUSE FAILURE (CCF)

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). 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. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
5) IEC provides no marking procedure to indicate its approval and cannot be rendered responsible for any equipment declared to be in conformity with an IEC Publication.
6) All users should ensure that they have the latest edition of this publication.
7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

International Standard IEC 62340 has been prepared by subcommittee 45A: Instrumentation and control of nuclear facilities, of IEC technical committee 45: Nuclear instrumentation.

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

FDIS	Report on voting
45A/668/FDIS	45A/676/RVD

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

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.

The committee has decided that the contents of this publication will remain unchanged until the maintenance result date indicated on the IEC web site under "http://webstore.iec.ch" in the data related to the specific publication. At this date, the publication will be

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

INTRODUCTION

a) Background, main issues and organisation of this Standard

In order to achieve a high safety level, redundancy is applied as one of the key features for designing instrumentation and control systems (I&C systems) important to safety. Since a Common Cause Failure (CCF) could compromise the effectiveness of redundancy, it is essential to take adequate measures against it. The nuclear industry has pioneered systems design and engineering to address CCF. Over the last thirty years it has implemented and reached consensus on a number of practices to handle and overcome CCF.

The intention of this standard is to address the whole scope of aspects to overcome Common Cause Failures (CCFs) and to provide an overview of the relevant requirements for I&C systems that are used to perform functions important to safety (according to IEC 61226) in nuclear power plants.

b) Situation of the current Standard in the structure of the IEC SC 45A standard series

IEC 62340 is a second level IEC SC 45A document tackling the issue of CCF.

This international standard supplements IEC 61513 and related standards with requirements to reduce and overcome the possibility of CCF of I&C functions of category A. The requirements given by this standard are applicable to category A (IEC 61226) functions if their failure would be unacceptable with respect to the plant safety design.

For more details on the structure of the IEC SC 45A standard series, see item d) of this introduction.

c) Recommendations and limitations regarding the application of this Standard

This standard applies to I&C systems important to safety of new NPPs as well as to the replacement of I&C systems of existing plants. The I&C functions may need to be kept or upgraded if an I&C system is replaced. The requirements of this standard also consider the replacement of I&C which entails changes in the structure of I&C systems.

For existing plants, only a subset of the requirements from this standard may be applicable and this subset should be identified at the beginning of any project. The requirements and recommendations which are not to be implemented in an I&C upgrading or replacement project should be justified on a case by case basis by an overall safety assessment. The potential consequences of not following this standard in some aspects due to plant constrains should be considered in comparison to the added safety gained through the upgrade as a whole.

To avoid overlapping requirements, this standard takes advantage of other existing standards by referring to the relevant (sub)clauses, especially to the nuclear sector standards IEC 61513, IEC 60709, IEC 60780 and IEC 60880. New requirements are given where not covered by these standards.

d) Description of the structure of the IEC SC 45A standard series and relationships with other IEC documents and other bodies documents (IAEA, ISO)

The top-level document of the IEC SC 45A standard series is IEC 61513. It provides general requirements for I&C systems and equipment that are used to perform functions important to safety in NPPs. IEC 61513 structures the IEC SC 45A standard series.

IEC 61513 refers directly to other IEC SC 45A standards for general topics related to categorization of functions and classification of systems, qualification, separation of systems,

defence against common cause failure, software aspects of computer-based systems, hardware aspects of computer-based systems, and control room design. The standards referenced directly at this second level should be considered together with IEC 61513 as a consistent document set.

At a third level, IEC SC 45A standards not directly referenced by IEC 61513 are standards related to specific equipment, technical methods, or specific activities. Usually these documents, which make reference to second-level documents for general topics, can be used on their own.

A fourth level extending the IEC SC 45A standard series, corresponds to the Technical Reports which are not normative.

IEC 61513 has adopted a presentation format similar to the basic safety publication IEC 61508 with an overall safety life-cycle framework and a system life-cycle framework and provides an interpretation of the general requirements of IEC 61508-1, IEC 61508-2 and IEC 61508-4, for the nuclear application sector. Compliance with IEC 61513 will facilitate consistency with the requirements of IEC 61508 as they have been interpreted for the nuclear industry. In this framework IEC 60880 and IEC 62138 correspond to IEC 61508-3 for the nuclear application sector.

IEC 61513 refers to ISO as well as to IAEA 50-C-QA (now replaced by IAEA GS-R-3) for topics related to quality assurance (QA).

The IEC SC 45A standards series consistently implements and details the principles and basic safety aspects provided in the IAEA code on the safety of NPPs and in the IAEA safety series, in particular the Requirements NS-R-1, establishing safety requirements related to the design of Nuclear Power Plants, and the Safety Guide NS-G-1.3 dealing with instrumentation and control systems important to safety in Nuclear Power Plants. The terminology and definitions used by SC 45A standards are consistent with those used by the IAEA.

NUCLEAR POWER PLANTS – INSTRUMENTATION AND CONTROL SYSTEMS IMPORTANT TO SAFETY – REQUIREMENTS FOR COPING WITH COMMON CAUSE FAILURE (CCF)

1 Scope

I&C systems important to safety may be designed using conventional hard-wired equipment, computer-based equipment or by using a combination of both types of equipment. This International Standard provides requirements and recommendations[1] for the overall architecture of I&C systems, which may contain either or both technologies.

The scope of this standard is:

a) to give requirements related to the avoidance of CCF of I&C systems that perform category A functions;

b) to additionally require the implementation of independent I&C systems to overcome CCF, while the likelihood of CCF is reduced by strictly applying the overall safety principles of IEC SC 45A (notably IEC 61226, IEC 61513, IEC 60880 and IEC 60709);

c) to give an overview of the complete scope of requirements relevant to CCF, but not to overlap with fields already addressed in other standards. These are referenced.

This standard emphasises the need for the complete and precise specification of the safety functions, based on the analysis of design basis accidents and consideration of the main plant safety goals. This specification is the pre-requisite for generating a comprehensive set of detailed requirements for the design of I&C systems to overcome CCF.

This standard provides principles and requirements to overcome CCF by means which ensure independence[2]:

a) between I&C systems performing diverse safety functions within category A which contribute to the same safety target;

b) between I&C systems performing different functions from different categories if e.g. a category B function is claimed as back-up of a category A function and;

c) between redundant channels of the same I&C system.

The implementation of these requirements leads to various types of defence against initiating CCF events.

Means to achieve protection against CCF are discussed in this standard in relation to:

a) susceptibility to internal plant hazards and external hazards;

b) propagation of physical effects in the hardware (e.g. high voltages); and

c) avoidance of specific faults and vulnerabilities within the I&C systems notably:

   1) propagation of functional failure in I&C systems or between different I&C systems (e.g. by means of communication, fault or error on shared resources),

---

[1] To support a clear addressing of all requirements and recommendations these are introduced by a clause number.

[2] Independence between I&C systems or between redundant channels of the same I&C system is the capability that in case of a postulated failure of one system or one channel the other systems or channels perform their functions as intended.

2) existence of common faults introduced during design or during system operation (e.g. maintenance induced faults),
3) insufficient system validation so that the system behaviour in response to input signal transients does not adequately correspond to the intended safety functions,
4) insufficient qualification of the required properties of hardware, insufficient verification of software components, or insufficient verification of compatibility between replaced and existing system components.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 60671, *Nuclear power plants – Instrumentation and control systems important to safety – Surveillance testing*

IEC 60709, *Nuclear power plants – Instrumentation and control systems important to safety – Separation*

IEC 60780, *Nuclear power plants – Electrical equipment of the safety system – Qualification*

IEC 60880, *Nuclear power plants – Instrumentation and control systems important to safety – Software aspects for computer-based systems performing category A functions*

IEC 60980, *Recommended practices for seismic qualification of electrical equipment of the safety system for nuclear generating stations*

IEC 61000-4 (all parts), *Electromagnetic compatibility (EMC) – Part 4: Testing and measurement techniques*

IEC 61226, *Nuclear power plants – Instrumentation and control systems important to safety – Classification of instrumentation and control functions*

IEC 61513, *Nuclear power plants – Instrumentation and control for systems important to safety – General requirements for systems*

IAEA Safety Guide NS-G-1.3, *Instrumentation and control systems important to safety in Nuclear Power Plants*

IAEA Safety Guide SG-D11, *General design safety principles for nuclear power plants*

IAEA Safety Glossary Ed.2.0, 2006

SOMMAIRE

AVANT-PROPOS 25
INTRODUCTION 27

1 Domaine d'application 29
2 Références normatives 30
3 Termes et définitions 31
4 Abréviations 35
5 Conditions et stratégie permettant de faire face aux DCC 35
5.1 Généralités 35
5.2 Caractéristiques des DCC 35
5.3 Principaux mécanismes des DCC des systèmes informatisés d'I&C 36
5.4 Conditions permettant de lutter contre les DCC des systèmes d'I&C individuels 36
5.5 Stratégie de conception permettant de surmonter les DCC 37
6 Exigences permettant de surmonter les défauts de spécification d'exigences 38
6.1 Elaboration des spécifications d'I&C à partir des bases de conception de sûreté de la tranche 38
6.2 Application des principes de défense en profondeur et de diversité fonctionnelle 39
6.3 Questions relatives aux DCC pour les centrales existantes 40
7 Mesures de conception pour lutter contre les défaillances concomitantes des systèmes d'I&C 40
7.1 Principe d'indépendance 40
7.2 Conception des systèmes d'I&C indépendants 41
7.3 Application de la diversité fonctionnelle 41
7.4 Evitement de la propagation des défaillances par les canaux de communication 42
7.5 Mesures à prendre contre les défaillances système provoquées par les activités de maintenance 42
7.6 Intégrité du matériel du système d'I&C 43
7.7 Précautions contre les dépendances liées à des dates ou à des messages externes 43
7.8 Assurance de la séparation physique et de la robustesse aux conditions d'ambiance 44
8 Tolérance aux défauts logiciels cachés hypothétiques 44
9 Exigences permettant d'éviter les défaillances système dues à la maintenance en exploitation 45

Annexe A (informative) Relation entre la CEI 60880 et cette norme 46

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

CENTRALES NUCLÉAIRES DE PUISSANCE – SYSTÈMES D'INSTRUMENTATION ET DE CONTRÔLE-COMMANDE IMPORTANTS POUR LA SÛRETÉ – EXIGENCES PERMETTANT DE FAIRE FACE AUX DÉFAILLANCES DE CAUSE COMMUNE (DCC)

AVANT-PROPOS

1) La Commission Electrotechnique Internationale (CEI) 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, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de la CEI"). Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec la CEI, participent également aux travaux. La CEI collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
2) Les décisions ou accords officiels de la CEI concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de la CEI intéressés sont représentés dans chaque comité d'études.
3) Les Publications de la CEI se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de la CEI. Tous les efforts raisonnables sont entrepris afin que la CEI s'assure de l'exactitude du contenu technique de ses publications; la CEI ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.
4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de la CEI s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de la CEI dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de la CEI et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
5) La CEI n'a prévu aucune procédure de marquage valant indication d'approbation et n'engage pas sa responsabilité pour les équipements déclarés conformes à une de ses Publications.
6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.
7) Aucune responsabilité ne doit être imputée à la CEI, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de la CEI, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de la CEI ou de toute autre Publication de la CEI, ou au crédit qui lui est accordé.
8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.
9) L'attention est attirée sur le fait que certains des éléments de la présente Publication de la CEI peuvent faire l'objet de droits de propriété intellectuelle ou de droits analogues. La CEI ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de propriété et de ne pas avoir signalé leur existence.

La Norme internationale CEI 62340 a été établie par le sous-comité 45A: Instrumentation et contrôle-commande des installations nucléaires, du comité d'études 45 de la CEI: Instrumentation nucléaire.

Le texte de cette norme est issu des documents suivants:

FDIS	Rapport de vote
45A/668/FDIS	45A/676/RVD

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

Cette publication a été rédigée selon les Directives ISO/CEI, Partie 2.

Le comité a décidé que le contenu de cette publication ne sera pas modifié avant la date de maintenance indiquée sur le site web de la CEI sous «http://webstore.iec.ch» dans les données relatives à la publication recherchée. A cette date, la publication sera

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

INTRODUCTION

a) Contexte technique, questions importantes et structure de la présente norme

L'application du principe de redondance est un des points clef de la conception des systèmes d'instrumentation et de contrôle-commande (systèmes d'I&C) importants pour la sûreté qui permet d'atteindre un haut niveau de sûreté. Les Défaillances de Cause Commune (DCC) pouvant remettre en cause l'efficacité de la redondance, il est essentiel de prendre des mesures palliatives appropriées contre celles-ci. L'industrie nucléaire a été pionnière dans le domaine du traitement des DCC au niveau de la conception et de l'ingénierie des systèmes. Au cours des trois dernières décades un consensus a pu être atteint et mis en œuvre au niveau d'un certain nombre de pratiques permettant de traiter et de surmonter les DCC.

L'intention de cette norme est de couvrir complètement le domaine des aspects permettant de surmonter les DCC et de fournir une vue générale des exigences pertinentes applicables aux systèmes d'I&C utilisés pour réaliser les fonctions importantes pour la sûreté (conformément à la CEI 61226) dans les centrales nucléaires.

b) Position de la présente norme dans la collection de normes du SC 45A de la CEI

La CEI 62340 est un document de deuxième niveau du SC 45A de la CEI traitant des DCC.

Cette norme internationale complète la CEI 61513 et ses normes fille par des exigences permettant de réduire la probabilité d'occurrence des DCC de fonctions d'I&C de catégorie A et de les surmonter. Les exigences fournies par cette norme s'appliquent aux fonctions de catégorie A (CEI 61226) dont la défaillance n'est pas acceptable par rapport à la conception de sûreté de la centrale.

Pour plus de détails sur la collection de normes du SC 45A de la CEI voir le point d) de cette introduction.

c) Recommandations et limites relatives à l'application de cette norme

Cette norme est applicable aux systèmes d'I&C importants pour la sûreté des nouvelles centrales nucléaires comme aux systèmes d'I&C de remplacement dans les centrales existantes. Lors du remplacement d'un système d'I&C, il peut être nécessaire de maintenir en l'état ou de mettre à niveau les fonctions d'I&C. Les exigences de cette norme prennent aussi en compte les remplacements d'I&C qui entraînent des modifications de la structure de l'I&C.

Pour les centrales existantes, seul un sous-ensemble des exigences de cette norme peut être applicable et il convient d'identifier ce sous-ensemble au début de chaque projet. Il convient de justifier au cas par cas, lors de l'évaluation de sûreté d'ensemble, les exigences et les recommandations qui ne sont pas mises en œuvre dans le cadre d'une mise à niveau ou d'un remplacement. Il convient de comparer dans un tout, les conséquences potentielles du non-respect de certains points de cette norme du fait de contraintes liées à la centrale, aux gains de sûreté obtenus lors de la mise à niveau.

Pour éviter d'empiéter sur des exigences existantes, cette norme tire avantage d'autres normes publiées en faisant référence aux paragraphes pertinents de celles-ci, et plus particulièrement à ceux des normes du secteur nucléaire: à savoir la CEI 61513, la CEI 60709, la CEI 60780 et la CEI 60880. Les nouvelles exigences sont fournies lorsqu'elles ne relèvent pas des domaines de ces normes.

d) Description de la structure de la collection des normes du SC 45A de la CEI et relations avec d'autres documents de la CEI et d'autres organisations (AIEA, ISO)

Le document de niveau supérieur de la collection de normes produites par le SC 45A de la CEI est la norme CEI 61513. Cette norme traite des exigences relatives aux systèmes et

équipements d'instrumentation et de contrôle-commande (systèmes d'I&C) utilisés pour accomplir les fonctions importantes pour la sûreté des centrales nucléaires, et structure la collection de normes du SC 45A de la CEI.

La CEI 61513 fait directement référence aux autres normes du SC 45A de la CEI traitant de sujets génériques, tels que la catégorisation des fonctions et le classement des systèmes, la qualification, la séparation des systèmes, les défaillances de cause commune, les aspects logiciels et les aspects matériels relatifs aux systèmes programmés, et la conception des salles de commande. Il convient de considérer que ces normes, de second niveau, forment, avec la norme CEI 61513, un ensemble documentaire cohérent.

Au troisième niveau, les normes du SC 45A de la CEI, qui ne sont généralement pas référencées directement par la norme CEI 61513, sont relatives à des matériels particuliers, à des méthodes ou à des activités spécifiques. Généralement ces documents, qui font référence aux documents de deuxième niveau pour les activités génériques, peuvent être utilisés de façon isolée.

Un quatrième niveau qui est une extension de la collection de normes du SC 45A de la CEI correspond aux rapports techniques qui ne sont pas des documents normatifs.

La CEI 61513 a adopté une présentation similaire à celle de la CEI 61508, avec un cycle de vie et de sûreté global, un cycle de vie et de sûreté des systèmes, et une interprétation des exigences générales de la CEI 61508-1, de la CEI 61508-2 et de la CEI 61508-4 pour le secteur nucléaire. La conformité à la CEI 61513 facilite la compatibilité avec les exigences de la CEI 61508 telles qu'elles ont été interprétées dans l'industrie nucléaire. Dans ce cadre, la CEI 60880 et la CEI 62138 correspondent à la CEI 61508-3 pour le secteur nucléaire.

La CEI 61513 fait référence aux normes ISO ainsi qu'au document AIEA 50-C-QA (remplacé depuis par le document AIEA GS-R-3) pour ce qui concerne l'assurance qualité.

Les normes produites par le SC 45A de la CEI sont élaborées de façon à être en accord avec les principes de sûreté fondamentaux du Code AIEA sur la sûreté des centrales nucléaires, ainsi qu'avec les guides de sûreté de l'AIEA, en particulier avec le document d'exigences NS-R-1 qui établit les exigences de sûreté relatives à la conception des centrales nucléaires et avec le guide de sûreté NS-G-1.3 qui traite de l'instrumentation et du contrôle-commande importants pour la sûreté des centrales nucléaires. La terminologie et les définitions utilisées dans les normes produites par le SC 45A sont conformes à celles utilisées par l'AIEA.

CENTRALES NUCLÉAIRES DE PUISSANCE – SYSTÈMES D'INSTRUMENTATION ET DE CONTRÔLE-COMMANDE IMPORTANTS POUR LA SÛRETÉ – EXIGENCES PERMETTANT DE FAIRE FACE AUX DÉFAILLANCES DE CAUSE COMMUNE (DCC)

1 Domaine d'application

Les systèmes d'I&C importants pour la sûreté peuvent être conçus en utilisant des matériels câblés conventionnels, des matériels informatiques ou en utilisant une combinaison des deux types de matériel. Cette norme fournit des exigences et des recommandations[1] pour l'ensemble de l'architecture des systèmes d'I&C qui peuvent contenir l'une, l'autre ou les deux technologies.

L'objectif de cette norme est de:

a) fournir des exigences relatives à l'évitement des DCC dans les systèmes d'I&C réalisant des fonctions de catégorie A;

b) exiger de façon complémentaire la mise en œuvre de systèmes d'I&C indépendants pour surmonter les DCC, lorsque la probabilité d'occurrence des DCC est déjà réduite en appliquant strictement les principes de sûreté prévalant au SC 45A de la CEI (en particulier ceux énoncés dans les CEI 61226, CEI 61513, CEI 60880 et CEI 60709);

c) donner une vue générale du domaine complet des exigences applicables aux DCC sans empiéter sur les domaines d'autres normes, celles-ci étant référencées.

Cette norme met l'accent sur la nécessité d'avoir un ensemble complet et précis de spécifications des fonctions de sûreté, reposant sur l'analyse des accidents de dimensionnement et sur la prise en compte des principaux objectifs de sûreté de la centrale. Ces spécifications sont un prérequis pour la production d'un ensemble exhaustif d'exigences qui est à la base de la conception permettant de surmonter les DCC.

Elle fournit les principes et les exigences pour surmonter les DCC par des moyens qui assurent l'indépendance[2]:

a) entre systèmes d'I&C réalisant diverses fonctions de sûreté de la catégorie A qui contribuent au même objectif de sûreté;

b) entre systèmes réalisant différentes fonctions dans différentes catégories, par exemple lorsqu'une fonction de catégorie B est déclarée comme assurant le secours d'une fonction de catégorie A et;

c) entre les canaux redondants au sein d'un même système d'I&C.

Différents types de défense contre les évènements initiateurs de DCC découlent de la mise en place de ces exigences.

Dans cette norme, les moyens permettant de se protéger contre les DCC sont traités en termes de:

a) sensibilité aux risques internes et externes à l'installation;

---

1 Afin de pouvoir identifier sans ambiguïté toutes les exigences et toutes les recommandations celles-ci sont numérotées dans le texte.

2 L'indépendance entre systèmes d'I&C ou entre chaînes redondantes du même système d'I&C est la capacité que les autres systèmes ou chaînes ont de réaliser leurs fonctions telles que prévues, en cas de défaillance hypothétique d'un système ou d'une chaîne d'autres systèmes.

b) propagation des effets physiques dans le matériel (par exemple surtensions); et

c) évitement d'erreurs ou de vulnérabilités propres aux systèmes d'I&C, en particulier:

   1) propagation des défaillances fonctionnelles au sein des systèmes d'I&C ou entre les différents systèmes d'I&C (par exemple par le biais des communications, de défauts ou d'erreurs affectant des ressources partagées),

   2) existence de défauts communs introduits lors de la conception ou durant l'exploitation du système (par exemple induits par des défauts de maintenance),

   3) validation système insuffisante telle que le comportement du système en réponse à des transitoires de données d'entrée ne pas correspond bien aux fonctions de sûreté prévues,

   4) qualification insuffisante des propriétés nécessaires des composants matériels, vérification insuffisante des composants logiciels, ou vérification insuffisante de la compatibilité des composants du système existants et de ceux qui ont été remplacés.

2 Références normatives

Les documents de référence suivants sont indispensables pour l'application du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

CEI 60671, *Centrales nucléaires de puissance – Systèmes d'instrumentation et de contrôle-commande importants pour la sûreté – Essais de surveillance*

CEI 60709, *Centrales nucléaires de puissance – Systèmes d'instrumentation et de contrôle commande importants pour la sûreté – Séparation*

CEI 60780, *Centrales nucléaires – Equipements électriques de sûreté – Qualification*

CEI 60880, *Centrales nucléaires de puissance – Instrumentation et contrôle-commande importants pour la sûreté – Aspects logiciels des systèmes programmés réalisant des fonctions de catégorie A*

CEI 60980, *Pratiques recommandées pour la qualification sismique du matériel électrique du système de sûreté dans les centrales électronucléaires*

CEI 61000-4 (toutes les parties), *Compatibilité électromagnétique (CEM) – Partie 4: Techniques d'essai et de mesure*

CEI 61226, *Centrales nucléaires de puissance – Systèmes d'instrumentation et de contrôle commande importants pour la sûreté – Classement des fonctions d'instrumentation et de contrôle commande*

CEI 61513, *Centrales nucléaires – Instrumentation et contrôle commande des systèmes importants pour la sûreté – Prescriptions générales pour les systèmes*

AIEA Guide de Sûreté NS-G-1.3, *Instrumentation and control systems important to safety in Nuclear Power Plants*

AIEA Guide de Sûreté SG-D11, *General design safety principles for nuclear power plants*

AIEA Glossaire de sûreté, Ed. 2.0, 2006