IEC 60744

Edition 2.0 2018-05

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

Nuclear power plants – Instrumentation and control systems important to safety – Safety logic assemblies used in systems performing category A functions: Characteristics and test methods

Centrales nucléaires de puissance – Systèmes d'instrumentation et de contrôle-commande importants pour la sûreté – Ensembles logiques de sûreté utilisés dans les systèmes réalisant des fonctions de catégorie A: Caractéristiques et méthodes d'essai

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

ICS 21.120.20

ISBN 978-2-8322-5681-7

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

NUCLEAR POWER PLANTS – INSTRUMENTATION AND CONTROL SYSTEMS IMPORTANT TO SAFETY – SAFETY LOGIC ASSEMBLIES USED IN SYSTEMS PERFORMING CATEGORY A FUNCTIONS: CHARACTERISTICS AND TEST METHODS

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 itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
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 60744 has been prepared by subcommittee 45A: Instrumentation, control and electrical power systems of nuclear facilities, of IEC technical committee 45: Nuclear instrumentation.

This second edition cancels and replaces the first edition published in 1983. This edition constitutes a technical revision.

This edition includes the following significant technical changes with respect to the previous edition:

a) update of the references to standards published or revised since the issue of the first edition of the current standard, including IEC 61513 and IEC 61226;
b) additional requirements for operational and maintenance bypass use; requirements of voting logic; requirements for interfacing with the MCR and SCR.

The text of this International Standard is based on the following documents:

FDIS	Report on voting
45A/1188/FDIS	45A/1200/RVD

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

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

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

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

IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

INTRODUCTION

a) Technical background, main issues and organisation of the Standard

This standard IEC 60744 specifically focuses on safety logic assemblies used in NPPs (Nuclear Power Plants). Safety logic assemblies were originally hardwired parts of protection systems mainly used to control actuators. IEC 60744 specifically focuses on the design, including technology, interfaces with MCR and SCR, tests and qualification. It gives requirements for display of the safety system inputs and state.

IEC 60744 is the document concerning safety logic assembly functions and performance.

The use of a computer based equipment or software is covered comprehensively by other standards. The technology used to design SLAs therefore involves mainly hard-wired technologies and submicronic highly integrated components (HPDs), the implementation of which is limited due to the very high safety requirements.

The document addresses the design and test characteristics of safety logic assemblies, especially regarding functional requirements, reliability issues, and associated control means including alarm, indication and control. Also it suggests the requirements for performance, testing and qualification for safety logic assemblies, and the interface requirements for communication between assemblies.

It is intended that the document be used by operators of NPPs (utilities), systems evaluators and licensors.

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

IEC 60744 is the third level IEC SC 45A document tackling the specific issue of testing and design characteristics of safety logic assemblies.

IEC 60744 is to be read in association with IEC 61513 which is the appropriate IEC SC 45A document which provides guidance on I&C safety system, and IEC 60964 which is the appropriate document for guidance on the Control Rooms, since the safety system has extensive interfaces with the MCR and SCR.

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 the Standard

It is important to note that this document establishes no additional functional requirements at safety system level.

Aspects for which special recommendations have been provided in this document are:

- The voting of partial trips to identify each safety actuation
- The output assemblies that provide the trips and actuations
- The design and test characteristics of functional requirements
- The reliability issue of safety logic assemblies
- The performance characteristics of logic assemblies
- Testing, qualification and interface requirements of safety logic assemblies

To ensure that the document will continue to be relevant in future years, the emphasis has been placed on issues of principle, rather than specific technologies.

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 documents of the IEC SC 45A standard series are IEC 61513 and IEC 63046. IEC 61513 provides general requirements for I&C systems and equipment that are used to perform functions important to safety in NPPs. IEC 63046 provides general requirements for electrical power systems of NPPs; it covers power supply systems including the supply systems of the I&C systems. IEC 61513 and IEC 63046 are to be considered in conjunction and at the same level. IEC 61513 and IEC 63046 structure the IEC SC 45A standard series and shape a complete framework establishing general requirements for instrumentation, control and electrical systems for nuclear power plants.

IEC 61513 and IEC 63046 refer directly to other IEC SC 45A standards for general topics related to categorization of functions and classification of systems, qualification, separation, defense against common cause failure, control room design, electromagnetic compatibility, cybersecurity, software and hardware aspects for programmable digital systems, coordination of safety and security requirements and management of ageing. The standards referenced directly at this second level should be considered together with IEC 61513 and IEC 63046 as a consistent document set.

At a third level, IEC SC 45A standards not directly referenced by IEC 61513 or by IEC 63046 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 45 standard series, corresponds to the Technical Reports which are not normative.

The IEC SC 45A standards series consistently implements and details the safety and security principles and basic aspects provided in the relevant IAEA safety standards and in the relevant documents of the IAEA nuclear security series (NSS). In particular this includes the IAEA requirements SSR-2/1, establishing safety requirements related to the design of nuclear power plants (NPPs), the IAEA safety guide SSG-30 dealing with the safety classification of structures, systems and components in NPPs, the IAEA safety guide SSG-39 dealing with the design of instrumentation and control systems for NPPs, the IAEA safety guide SSG-34 dealing with the design of electrical power systems for NPPs and the implementing guide NSS17 for computer security at nuclear facilities. The safety and security terminology and definitions used by SC 45A standards are consistent with those used by the IAEA.

IEC 61513 and IEC 63046 have adopted a presentation format similar to the basic safety publication IEC 61508 with an overall life-cycle framework and a system life-cycle framework. Regarding nuclear safety, IEC 61513 and IEC 63046 provide the interpretation of the general requirements of IEC 61508-1, IEC 61508-2 and IEC 61508-4, for the nuclear application sector. In this framework IEC 60880, IEC 62138 and IEC 62566 correspond to IEC 61508-3 for the nuclear application sector. IEC 61513 and IEC 63046 refer to ISO as well as to IAEA GS-R-3 and IAEA GS-G-3.1 and IAEA GS-G-3.5 for topics related to quality assurance (QA). At level 2, regarding nuclear security, IEC 62645 is the entry document for the IEC SC 45A security standards. It builds upon the valid high level principles and main concepts of the generic security standards, in particular ISO/IEC 27001 and ISO/IEC 27002; it adapts them and completes them to fit the nuclear context and coordinates with the IEC 62443 series. At level 2, regarding control rooms, IEC 60964 is the entry document for the IEC SC 45A control rooms standards and IEC 62342 is the entry document for the IEC SC 45A ageing management standards.

NOTE 1 It is assumed that for the design of I&C systems in NPPs that implement conventional safety functions (e.g. to address worker safety, asset protection, chemical hazards, process energy hazards) international or national standards would be applied.

NOTE 2 IEC SC 45A domain was extended in 2013 to cover electrical systems. In 2014 and 2015 discussions were held in IEC SC 45A to decide how and where general requirement for the design of electrical systems were to be considered. IEC SC 45A experts recommended that an independent standard be developed at the same level as IEC 61513 to establish general requirements for electrical systems. Project IEC 63046 is now launched to cover this objective. When IEC 63046 is published this NOTE 2 of the introduction of IEC SC 45A standards will be suppressed.

NUCLEAR POWER PLANTS – INSTRUMENTATION AND CONTROL SYSTEMS IMPORTANT TO SAFETY – SAFETY LOGIC ASSEMBLIES USED IN SYSTEMS PERFORMING CATEGORY A FUNCTIONS: CHARACTERISTICS AND TEST METHODS

1 Scope

This document provides requirements and recommendations for the design, construction and test of safety logic assemblies used in safety systems to perform category A safety functions (in accordance with IEC 61226). Safety logic assemblies include logic such as the hardwired logic assembly interfacing computer-based systems to switchgear, actuators or contactors to provide trip or engineered safety feature actuations. Safety logic assemblies are significant parts of a safety system and may include voting logic between redundant channels.

This document provides a general description of safety logic assemblies for safety actuators control. The principles to meet dependability objectives are presented. The main features relating to the design requirements are described and explained.

Various tests and their requirements are given in order to validate the design (including the qualification tests), the manufacturing and the correct installation on site.

Annex A (informative) gives a list of possible applications of safety logic assemblies.

Annex B (normative) suggests a list of possible hardwired technologies with their respective requirements to design safety logic assemblies.

Annex C (informative) gives explanations on dependability and its attributes to improve reliability and to reduce the final risk which compromises the safety and the availability of the NPP.

The scope of this document does not address the design of a protection system, it covers only the technological and architectural solutions required to design a safety logic assembly. The design of safety systems using safety logic assemblies is covered by IEC 61513.

The detailed and specific functions implemented in a safety logic assembly strongly depend on the design of each reactor and are not addressed in this document.

As this document is focused on I&C part of the system, the final voting logic made with power breakers is excluded from the scope of this document.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements 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 60255 (all parts), *Measuring relays and protection equipment*

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/IEEE 60780-323, *Nuclear facilities – Electrical equipment important to safety – Qualification*

IEC 60812, *Analysis techniques for system reliability – Procedure for failure mode and effects analysis (FMEA)*

IEC 60964, *Nuclear power plants – Control rooms – Design*

IEC 60965, *Nuclear power plants – Control rooms – Supplementary control room for reactor shutdown without access to the main control room*

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

IEC 61000 (all parts), *Electromagnetic compatibility (EMC)*

IEC 61225, *Nuclear power plants – Instrumentation and control systems important to safety – Requirements for electrical supplies*

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

IEC 61227, *Nuclear power plants – Control rooms – Operator controls*

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

IEC 62003, *Nuclear power plants – Instrumentation and control important to safety – Requirements for electromagnetic compatibility testing*

IEC 62241, *Nuclear power plants – Main control room – alarm functions and presentation*

IEC 62566:2012, *Nuclear power plants – Instrumentation and control important to safety – Development of HDL-programmed integrated circuits for systems performing category A functions*

IAEA-GSR Part 2, *Leadership and Management for Safety*

SOMMAIRE

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

CENTRALES NUCLÉAIRES DE PUISSANCE – SYSTÈMES D'INSTRUMENTATION ET DE CONTRÔLE-COMMANDE IMPORTANTS POUR LA SÛRETÉ – ENSEMBLES LOGIQUES DE SÛRETÉ UTILISÉS DANS LES SYSTÈMES RÉALISANT DES FONCTIONS DE CATÉGORIE A: CARACTÉRISTIQUES ET MÉTHODES D'ESSAI

AVANT-PROPOS

1) La Commission Electrotechnique Internationale (IEC) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de l'IEC). L'IEC 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, l'IEC – 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 l'IEC"). 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 l'IEC, participent également aux travaux. L'IEC 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 l'IEC concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de l'IEC intéressés sont représentés dans chaque comité d'études.
3) Les Publications de l'IEC se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de l'IEC. Tous les efforts raisonnables sont entrepris afin que l'IEC s'assure de l'exactitude du contenu technique de ses publications; l'IEC 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 l'IEC s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de l'IEC dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de l'IEC et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
5) L'IEC elle-même ne fournit aucune attestation de conformité. Des organismes de certification indépendants fournissent des services d'évaluation de conformité et, dans certains secteurs, accèdent aux marques de conformité de l'IEC. L'IEC n'est responsable d'aucun des services effectués par les organismes de certification indépendants.
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 l'IEC, 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 l'IEC, 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 l'IEC ou de toute autre Publication de l'IEC, 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 l'IEC peuvent faire l'objet de droits de brevet. L'IEC ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de brevets et de ne pas avoir signalé leur existence.

La Norme internationale IEC 60744 a été établie par le sous-comité 45A: Systèmes d'instrumentation, de contrôle-commande et d'alimentation électrique des installations nucléaires, du comité d'études 45 de l'IEC: Instrumentation nucléaire.

Cette deuxième édition annule et remplace la première édition parue en 1983. Cette édition constitue une révision technique.

Cette édition inclut les modifications techniques majeures suivantes par rapport à l'édition précédente:

a) actualisation des références aux normes publiées ou révisées depuis la publication de la première édition de la norme actuelle, y compris l'IEC 61513 et l'IEC 61226;

b) exigences supplémentaires concernant l'utilisation du bipasse de fonctionnement et du bipasse de maintenance; exigences concernant la logique de vote et exigences concernant l'interface avec les MCR et SCR.

Le texte de cette Norme internationale est issu des documents suivants:

FDIS	Rapport de vote
45A/1188/FDIS	45A/1200/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.

Ce document a été rédigé selon les Directives ISO/IEC, Partie 2.

Le comité a décidé que le contenu de ce document ne sera pas modifié avant la date de stabilité indiquée sur le site web de l'IEC sous "http://webstore.iec.ch" dans les données relatives au document recherché. A cette date, le document sera

- reconduit,
- supprimé,
- remplacé par une édition révisée, ou
- amendé.

IMPORTANT – Le logo *"colour inside"* qui se trouve sur la page de couverture de cette publication indique qu'elle contient des couleurs qui sont considérées comme utiles à une bonne compréhension de son contenu. Les utilisateurs devraient, par conséquent, imprimer cette publication en utilisant une imprimante couleur.

INTRODUCTION

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

L'IEC 60744 traite spécifiquement des ensembles logiques de sûreté utilisés dans les centrales nucléaires de puissance (CNP). Les ensembles logiques de sûreté étaient à l'origine des éléments câblés des systèmes de protection utilisés principalement pour commander les actionneurs. L'IEC 60744 traite spécifiquement de la conception, y compris la technologie, les interfaces avec les MCR et SCR, les essais et la qualification. Elle spécifie des exigences concernant l'affichage des entrées et de l'état des systèmes de sûreté.

L'IEC 60744 est le document qui traite des fonctions et des performances des ensembles logiques de sûreté.

L'utilisation des matériels informatiques ou de logiciel est couverte de façon exhaustive par d'autres normes. La technologie utilisée pour la conception des SLA intègre principalement des technologies câblée et des composants à haute intégration submicronique (HPD), dont la mise en œuvre est contrainte par le très haut niveau d'exigence de sûreté.

Le document traite des caractéristiques de conception et d'essai des ensembles logiques de sûreté, notamment en ce qui concerne les exigences fonctionnelles, les questions de fiabilité et les moyens de contrôle-commande associés, y compris l'alarme, l'indication et le contrôle-commande. Le document propose également les exigences concernant les performances, les essais et la qualification relatifs aux ensembles logiques de sûreté et les exigences d'interface concernant la communication entre les ensembles.

L'objectif du document est d'être utilisé par les exploitants de centrales nucléaires de puissance (réseaux), les évaluateurs de systèmes et les régulateurs.

b) Position de la présente norme dans la structure de la série de normes du SC 45A de l'IEC

L'IEC 60744 est le document du SC 45A de l'IEC de troisième niveau qui traite de la question spécifique des caractéristiques d'essai et de conception des ensembles logiques de sûreté.

L'IEC 60744 doit être utilisée en association avec l'IEC 61513 qui constitue le document approprié du SC 45A de l'IEC fournissant un guide sur le système de sûreté I&C et l'IEC 60964 qui constitue le document approprié servant de guide sur les salles de commande, étant donné que le système de sûreté comprend des interfaces extensives avec les MCR et SCR.

Voir le point d) de la présente introduction pour de plus amples informations détaillées sur la structure de la série de normes du SC 45A de l'IEC.

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

Il est important de noter que le présent document n'établit pas d'exigence fonctionnelle supplémentaire pour les systèmes de sûreté.

Le présent document spécifie des recommandations particulières pour les aspects suivants:

- Le vote sur les déclenchements partiels afin d'identifier chaque actionnement de sûreté
- Les ensembles de sortie qui assurent les arrêts rapides et les actionnements
- Les caractéristiques de conception et d'essai des exigences fonctionnelles
- La question de fiabilité des ensembles logiques de sûreté
- Les caractéristiques de performances des ensembles logiques

- Les exigences d'essai, de qualification et d'interface des ensembles logiques de sûreté

Afin d'assurer la pertinence du présent document pour les années à venir, l'accent est mis sur les questions de principe plutôt que sur les technologies particulières.

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

Les documents de niveau supérieur de la collection de normes produites par le SC 45A de l'IEC sont les normes IEC 61513 et IEC 63046. La norme IEC 61513 traite des exigences générales 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. La norme IEC 63046 traite des exigences générales relatives aux systèmes d'alimentation électrique; elle couvre les systèmes d'alimentation électrique jusqu'à et y compris les alimentations des systèmes d'I&C. Les normes IEC 61513 et IEC 63046 doivent être considérées ensemble et au même niveau. Les normes IEC 61513 et IEC 63046 structurent la collection de normes du SC 45A de l'IEC et forment un cadre complet, cohérent et consistant établissant les exigences générales relatives aux systèmes d'I&C et électriques des centrales nucléaires de puissance.

Les normes IEC 61513 et IEC 63046 font directement référence aux autres normes du SC 45A de l'IEC traitant de sujets génériques, tels que la catégorisation des fonctions et le classement des systèmes, la qualification, la séparation des systèmes, la défense contre les défaillances de cause commune, la conception des salles de commande, compatibilité électromagnétique, la cybersécurité, les aspects logiciels et matériels relatifs aux systèmes programmés numériques, la coordination des exigences de sûreté et de sécurité et la gestion du vieillissement. Il convient de considérer que ces normes, de second niveau, forment, avec les normes IEC 61513 et IEC 63046, un ensemble documentaire cohérent.

Au troisième niveau, les normes du SC 45A de l'IEC, qui ne sont généralement pas référencées directement par les normes IEC 61513 ou IEC 63046, 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 l'IEC correspond aux rapports techniques qui ne sont pas des documents normatifs.

Les normes de la collection produite par le SC 45A de l'IEC sont élaborées de façon à être en accord avec les principes de sûreté et de sécurité de haut niveau établis par les normes de sûreté de l'AIEA pertinentes pour les centrales nucléaires, ainsi qu'avec les documents pertinents de la collection de l'AIEA pour la sécurité nucléaire (NSS), en particulier avec le document d'exigences SSR-2/1 qui établit les exigences de sûreté relatives à la conception des centrales nucléaires, avec le guide de sûreté SSG-30 qui traite du classement de sûreté des structures, systèmes et composants des centrales nucléaires, avec le guide de sûreté SSG-39 qui traite de la conception de l'instrumentation et du contrôle commande des centrales nucléaires, avec le guide de sûreté SSG-34 qui traite de la conception des systèmes d'alimentation électrique des centrales nucléaires, et avec le guide de mise en œuvre NSS17 traitant de la sécurité informatique pour les installations nucléaires. La terminologie et les définitions utilisées pour la sûreté et la sécurité dans les normes produites par le SC 45A sont conformes à celles utilisées par l'AIEA.

Les normes IEC 61513 et IEC 63046 ont adopté une présentation similaire à celle de l'IEC 61508, avec un cycle de vie d'ensemble et un cycle de vie des systèmes. Au niveau sûreté nucléaire, les normes IEC 61513 et IEC 63046 sont l'interprétation des exigences générales de l'IEC 61508-1, de l'IEC 61508-2 et de l'IEC 61508-4 pour le secteur nucléaire. Dans ce domaine, l'IEC 60880, l'IEC 62138 et l'IEC 62566 correspondent à l'IEC 61508-3 pour le secteur nucléaire. Les normes IEC 61513 et IEC 63046 font référence aux normes ISO ainsi qu'aux documents AIEA GS-R-3 et AIEA GS-G-3.1 et AIEA GS-G-3.5 pour ce qui concerne l'assurance qualité. Au second niveau, la norme IEC 62645 est le document

chapeau des normes du SC 45A de l'IEC portant sur la sécurité nucléaire. Elle est élaborée sur les principes pertinents de haut niveau des normes ISO/IEC 27001 et ISO/IEC 27002; elle les adapte et les complète pour qu'ils deviennent pertinents pour le secteur nucléaire; elle est coordonnée étroitement avec la norme IEC 62443. Au second niveau, la norme IEC 60964 est le document chapeau des normes du SC 45A de l'IEC portant sur les salles de commande et la norme IEC 62342 est le document chapeau des normes du SC 45A de l'IEC portant sur la gestion du vieillissement.

NOTE 1 Il est fait l'hypothèse que pour la conception des systèmes d'I&C qui sont supports de fonctions de sûreté conventionnelle (par exemple pour garantir la sécurité des travailleurs, la protection des biens, la prévention contre les risques chimiques, la prévention contre les risques liés au procédé énergétique) on applique des normes nationales ou internationales.

NOTE 2 Le domaine de l'IEC SC 45A a été étendu en 2013 pour couvrir les systèmes électriques. En 2014 et en 2015 des discussions ont eu lieu au sein de l'IEC SC 45A pour décider des modalités et du cadre d'établissement des exigences générales portant sur la conception des systèmes électriques. Les experts de l'IEC SC 45A ont recommandé que pour établir des exigences générales pour les systèmes électriques une norme indépendante soit développée au même niveau que l'IEC 61513. Le projet IEC 63046 est lancé pour atteindre cet objectif. Lorsque la norme IEC 63046 sera publiée la présente NOTE 2 de l'introduction sera supprimée.

CENTRALES NUCLÉAIRES DE PUISSANCE – SYSTÈMES D'INSTRUMENTATION ET DE CONTRÔLE-COMMANDE IMPORTANTS POUR LA SÛRETÉ – ENSEMBLES LOGIQUES DE SÛRETÉ UTILISÉS DANS LES SYSTÈMES RÉALISANT DES FONCTIONS DE CATÉGORIE A: CARACTÉRISTIQUES ET MÉTHODES D'ESSAI

1 Domaine d'application

Le présent document spécifie les exigences et les recommandations pour la conception, la fabrication et les essais des ensembles logiques de sûreté utilisés dans les systèmes de sûreté pour réaliser des fonctions de sûreté de catégorie A (conformément à l'IEC 61226). Les ensembles logiques de sûreté réalisent des fonctions logiques comme, par exemple, la logique câblée faisant l'interface entre la partie programmée et les interrupteurs d'arrêt du réacteur, les actionneurs ou les contacteurs pour déclencher l'arrêt du réacteur ou les actions de sauvegarde. Les ensembles logiques de sûreté sont des éléments importants d'un système de sûreté et peuvent comporter une logique de vote entre des voies redondantes.

Le présent document décrit de manière générale les ensembles logiques de sûreté pour la commande des actionneurs de sûreté. Il donne les principes permettant d'atteindre les objectifs de sûreté de fonctionnement. Il décrit et explicite également les principales caractéristiques relatives aux exigences de conception.

Divers essais sont spécifiés, ainsi que leurs exigences, pour valider la conception (y compris les essais de qualification), la fabrication et l'installation correcte sur site.

L'Annexe A (informative) donne une liste des applications possibles des ensembles logiques de sûreté.

L'Annexe B (normative) propose une liste des technologies câblées possibles avec leurs exigences respectives portant sur la conception des ensembles logiques de sûreté.

L'Annexe C (informative) explicite la sûreté de fonctionnement et ses attributs afin d'améliorer la fiabilité et de réduire le risque final qui compromet la sûreté et la disponibilité des centrales nucléaires de puissance.

Le domaine d'application du présent document ne traite pas de la conception d'un système de protection, mais couvre uniquement les solutions technologiques et architecturales que nécessite la conception d'un ensemble logique de sûreté. L'IEC 61513 traite de la conception des systèmes de sûreté qui utilisent des ensembles logiques de sûreté.

Les fonctions spécifiques détaillées mises en œuvre dans un ensemble logique de sûreté dépendent dans une large mesure de la conception de chaque réacteur et ne sont pas traitées dans le présent document.

L'objectif principal de ce document étant la partie instrumentation et contrôle-commande du système, la logique de vote finale réalisée à partir de disjoncteurs de puissance est exclue du domaine de ce document.

2 Références normatives

Les documents suivants cités dans le texte constituent, pour tout ou partie de leur contenu, des exigences 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).

IEC 60255 (toutes les parties), *Relais de mesure et dispositifs de protection*

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

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

IEC/IEEE 60780-323, *Installations nucléaires – Équipements électriques importants pour la sûreté – Qualification*

IEC 60812, *Techniques d'analyse de la fiabilité du système – Procédure d'analyse des modes de défaillance et de leurs effets (AMDE)*

IEC 60964, *Centrales nucléaires de puissance – Salles de commande – Conception*

IEC 60965, *Centrales nucléaires de puissance – Salles de commande – Salle de commande supplémentaire pour l'arrêt des réacteurs sans accès à la salle de commande principale*

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

IEC 61000 (toutes les parties), *Compatibilité électromagnétique (CEM)*

IEC 61225, *Centrales nucléaires de puissance – Systèmes d'instrumentation et de contrôle-commande importants pour la sûreté – Exigences pour les alimentations électriques*

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

IEC 61227*, Centrales nucléaires de puissance – Salles de commande – Commandes opérateurs*

IEC 61513, *Centrales nucléaires de puissance – Instrumentation et contrôle-commande importants pour la sûreté – Exigences générales pour les systèmes*

IEC 62003, *Centrales nucléaires de puissance – Instrumentation et contrôle-commande importants pour la sûreté – Exigences relatives aux essais de compatibilité électromagnétique*

IEC 62241, *Centrales nucléaires de puissance – Salle de commande principale – Fonctions et présentation des alarmes*

IEC 62566:2012*, Centrales nucléaires de puissance – Instrumentation et contrôle-commande importants pour la sûreté – Développement des circuits intégrés programmés en HDL pour les systèmes réalisant des fonctions de catégorie A*

IAEA-GSR Part 2, *Leadership and Management for Safety*