IEC 61513

Edition 2.0 2011-08

INTERNATIONAL STANDARD

NORME INTERNATIONALE

Nuclear power plants – Instrumentation and control important to safety – General requirements for systems

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

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

PRICE CODE
CODE PRIX XD

ICS 27.120.20

ISBN 978-2-88912-663-7

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

NUCLEAR POWER PLANTS – INSTRUMENTATION AND CONTROL IMPORTANT TO SAFETY – GENERAL REQUIREMENTS FOR SYSTEMS

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 61513 has been prepared by subcommittee 45A: Instrumentation and control of nuclear facilities, of IEC technical committee 45: Nuclear instrumentation.

This second edition cancels and replaces the first edition, published in 2001, and constitutes a technical revision.

The main technical changes with regard to the previous edition are as follows:

- to align the standard with the new revisions of IAEA NS-R-1 and NS-G-1.3, to review the existing requirements and to update the terminology and definitions;
- to take account of, as far as possible, requirements associated with standards published since the first edition, especially IEC 60880, IEC 61226, IEC 62138, IEC 62340 and IEC 60987;
- to take into account the fact that software engineering techniques have advanced significantly in the intervening years;

- to integrate requirements for staff training.

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

FDIS	Report on voting
45A/838/FDIS	45A/848/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 stability 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) Technical background, main issues and organisation of the standard

This International Standard sets out requirements applicable to instrumentation and control systems and equipment (I&C systems) that are used to perform functions important to safety in nuclear power plants (NPPs).

This standard highlights the relations between

- the safety objectives of the NPP and the requirements for the overall architecture of the I&C systems important to safety;
- the overall architecture of the I&C systems and the requirements of the individual systems important to safety.

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

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

IEC 61513 is the first level IEC SC 45A document tackling the issue of general requirements for systems. It is the entry point of the IEC SC 45A standard series.

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

It is important to note that this standard establishes no additional functional requirements for safety systems.

To ensure that the standard 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 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 categorisation 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 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. Regarding nuclear safety, it provides the interpretation of the general requirements of IEC 61508-1 [1][1], IEC 61508-2 and IEC 61508-4, for the nuclear application sector. In this framework, IEC 60880 and IEC 62138 correspond to IEC 61508-3 [2] for the nuclear application sector.

IEC 61513 refers to ISO as well as to IAEA GS-R-3 and IAEA GS-G-3.1 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 document 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.

NOTE 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, protection from chemical hazards and process energy hazards), international or national standards would be applied, that are based on the requirements of such a standard as the IEC 61508 series.

1 References in square brackets refer to the bibliography.

NUCLEAR POWER PLANTS – INSTRUMENTATION AND CONTROL IMPORTANT TO SAFETY – GENERAL REQUIREMENTS FOR SYSTEMS

1 Scope

1.1 General

I&C systems important to safety may be implemented using conventional hard-wired equipment, computer-based (CB) equipment or by using a combination of both types of equipment (see Note 1). This International Standard provides requirements and recommendations (see Note 2) for the overall I&C architecture which may contain either or both technologies.

This standard highlights also the need for complete and precise requirements, derived from the plant safety goals, as a pre-requisite for generating the comprehensive requirements for the overall I&C architecture, and hence for the individual I&C systems important to safety.

This standard introduces the concept of a safety life cycle for the overall I&C architecture, and a safety life cycle for the individual systems. By this, it highlights the relations between the safety objectives of the NPP and the requirements for the overall architecture of the I&C systems important to safety, and the relations between the overall I&C architecture and the requirements of the individual systems important to safety.

The life cycles illustrated in, and followed by, this standard are not the only ones possible; other life cycles may be followed, provided that the objectives stated in this standard are satisfied.

NOTE 1 I&C systems may also use electronic modules based on complex electronic components such as ASICs or FPGA. Depending on the scope and functionality of these components, they may be treated according to the guidance for conventional electronic equipment, or similar to CB equipment. A significant part of the guidance for CB equipment is also applicable to the design of equipment with complex electronic components, including e.g. the concepts of re-using pre-existing designs, and the evaluation of design errors in software or complex hardware designs.

NOTE 2 In the following, “requirement” is used as a comprehensive term for both requirements and recommendations. The distinction appears at the level of the specific provisions where requirements are expressed by “shall” and recommendations by “should”.

1.2 Application: new and pre-existing plants

This standard applies to the I&C of new nuclear power plants as well as to I&C up-grading or back-fitting of existing plants.

For existing plants, only a subset of requirements is applicable and this subset should be identified at the beginning of any project.

1.3 Framework

The standard comprises four normative clauses (an overview is provided in Figure 1):

- Clause 5 addresses the overall architecture of the I&C systems important to safety:
  - defining requirements for the I&C functions, and associated systems and equipment derived from the safety analysis of the NPP, the categorisation of I&C functions, and the plant lay-out and operational context;
  - structuring the overall I&C architecture, dividing it into a number of systems and assigning the I&C functions to systems. Design criteria are identified, including those to give defence in depth and to minimize the potential for common cause failure (CCF);

– planning the overall architecture of the I&C systems.

- Clause 6 addresses the requirements for the individual I&C systems important to safety, particularly the requirements for computer-based systems. This includes differentiation of requirements according to the safety category of the I&C functions which are implemented;
- Clauses 7 and 8 address the overall integration, commissioning, operation and maintenance of the I&C systems.

NOTE Figure 1 outlines the structure of the standard. It does not necessarily present the timely order of activities which may be in reality partially executed in parallel, or include iterations.

Additionally, the standard provides informative annexes:

- Annex A highlights the relations between IAEA and basic safety concepts that are used throughout this standard;
- Annex B provides information on the categorisation/classification principles;
- Annex C gives examples of I&C sensitivity to CCF;
- Annex D provides guidance to support comparison of this standard with parts 1, 2 and 4 of IEC 61508. This annex surveys the main requirements of IEC 61508 to verify that the issues relevant to safety are adequately addressed, considers the use of common terms and explains the reason for adopting different or complementary techniques or terms;
- Annex E indicates modifications to be made in future revisions of daughter standards of IEC 61513 to make them consistent and to minimize overlapping contents.

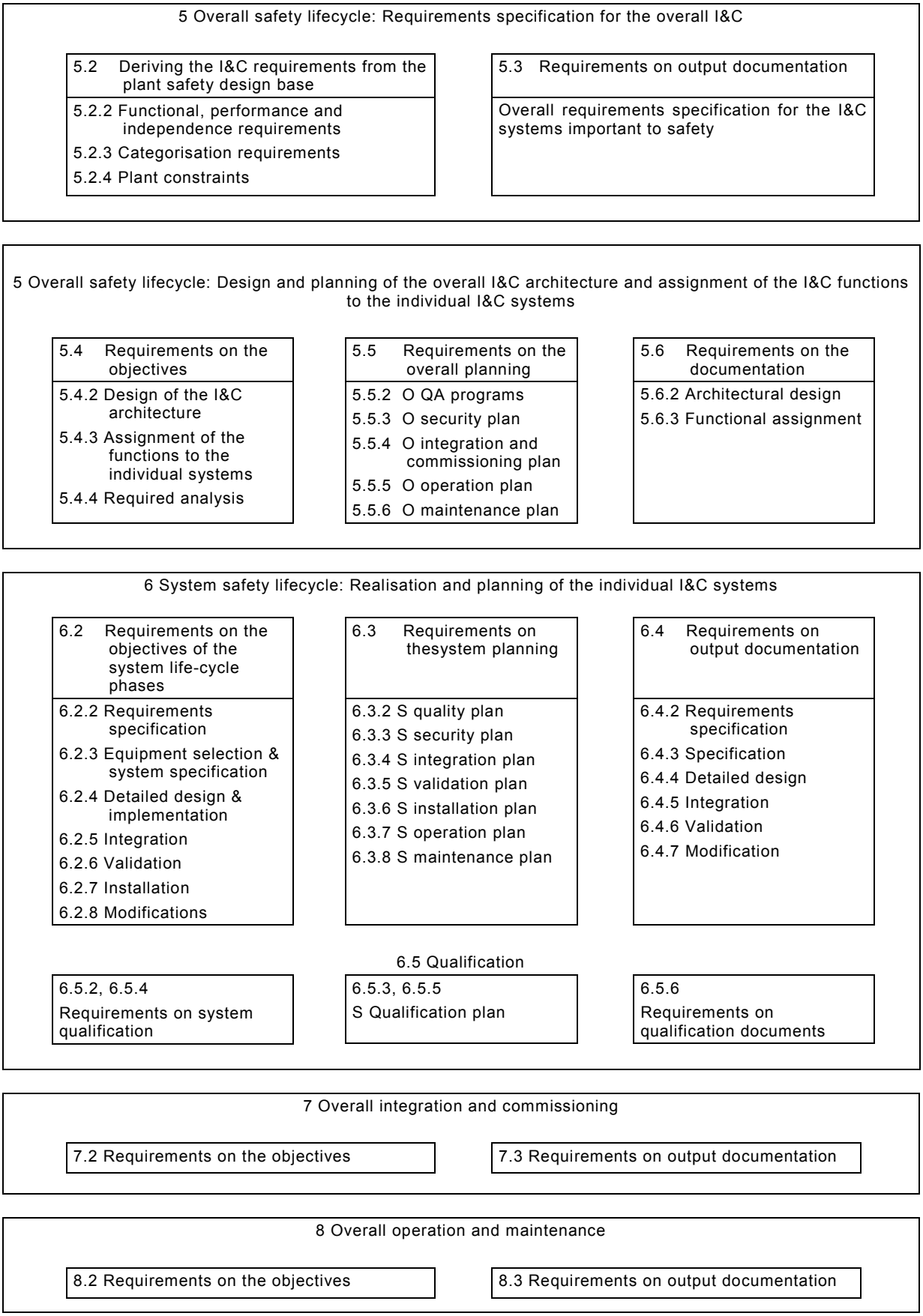


Figure 1 – Overall framework of this standard

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 60880:2006, *Nuclear power plants – Instrumentation and control systems important to safety – Software aspects for computer-based systems performing category A functions*

IEC 60964:2009, *Nuclear power plants – Control rooms – Design*

IEC 60965, *Nuclear power plants – Control rooms – Supplementary control points 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 60987:2007, *Nuclear power plants – Instrumentation and control important to safety – Hardware design requirements for computer-based systems*

IEC 61000-4-1, *Electromagnetic compatibility (EMC) – Part 4-1: Testing and measurement techniques – Overview of IEC 61000-4 series*

IEC 61000-4-2, *Electromagnetic compatibility (EMC) – Part 4-2: Testing and measurement techniques – Electrostatic discharge immunity test*

IEC 61000-4-3, *Electromagnetic compatibility (EMC) – Part 4-3: Testing and measurement techniques – Radiated, radio-frequency, electromagnetic field immunity test*

IEC 61000-4-4, *Electromagnetic compatibility (EMC) – Part 4-4: Testing and measurement techniques – Electrical fast transient/burst immunity test*

IEC 61000-4-5, *Electromagnetic compatibility (EMC) – Part 4-5: Testing and measurement techniques – Surge immunity test*

IEC 61000-4-6, *Electromagnetic compatibility (EMC) – Part 4-6: Testing and measurement techniques – Immunity to conducted disturbances, induced by radio-frequency fields*

IEC 61226:2009, *Nuclear power plants – Instrumentation and control systems important to safety – Classification of instrumentation and control functions*

IEC 61500, *Nuclear power plants – Instrumentation and control important to safety – Data communication in systems performing category A functions*

IEC 61508-2:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems*

IEC 61508-4:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 4: Definitions and abbreviations*

IEC 62138:2004, *Nuclear power plants – Instrumentation and control important for safety – Software aspects for computer-based systems performing category B or C functions*

IEC 62340, *Nuclear power plants – Instrumentation and control systems important to safety – Requirements for coping with common cause failure (CCF)*

ISO 9001:2008, *Quality management systems – Requirements*

IAEA INSAG-10:1996, *Defence in Depth in Nuclear Safety*

IAEA NS-R-1:2000, *Safety of Nuclear Power Plants: Design*

IAEA GS-R-3:2006, *The Management System for Facilities and Activities Safety – Requirements*

IAEA GS-G-3.1:2006, *Application of the Management System for Facilities and Activities – Safety Guide*

IAEA NS-G-1.3:2002, *Instrumentation and Control Systems Important to Safety in Nuclear Power Plants*

IAEA 75-INSAG-3 Rev. 1 – INSAG 12:1999, *Basic Safety Principles for Nuclear Power Plants*

SOMMAIRE

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

CENTRALES NUCLÉAIRES DE PUISSANCE – INSTRUMENTATION ET CONTRÔLE-COMMANDE IMPORTANTS POUR LA SÛRETÉ – EXIGENCES GÉNÉRALES POUR LES SYSTÈMES

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 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 la CEI. La CEI 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 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 brevet. La CEI 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 CEI 61513 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.

Cette deuxième édition annule et remplace la première édition publiée en 2001, dont elle constitue une révision technique.

Les principaux changements techniques par rapport à l'édition précédente sont les suivants:

- mettre en cohérence la norme avec les nouvelles révisions des documents de l'AIEA, NS-R-1 et NS-G-1.3; passer en revue les exigences et mettre à jour la terminologie et les définitions;

- prendre en compte, autant que possible, les exigences associées aux normes publiées depuis la parution de la première édition, en particulier les CEI 60880, CEI 61226, CEI 62138, CEI 62340 et CEI 60987;
- prendre en compte le fait que les techniques de génie logiciel ont réalisé des progrès significatifs durant ces années;
- intégrer les exigences relatives à la formation du personnel.

Le texte de cette norme est issu des documents suivants:

FDIS	Rapport de vote
45A/838/FDIS	45A/848/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 stabilité 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

La présente Norme Internationale établit des exigences applicables aux matériels et systèmes d'instrumentation et de contrôle commande (systèmes d'I&C) utilisés pour réaliser des fonctions importantes pour la sûreté dans les centrales nucléaires de puissance (CNP).

Cette norme met l'accent sur la relation existant entre:

- les objectifs de sûreté de la CNP et les exigences applicables à l'ensemble de l'architecture des systèmes d'I&C importants pour la sûreté.
- l'ensemble de l'architecture des systèmes d'I&C et les exigences relatives aux systèmes individuels importants pour la sûreté.

L'objectif de la présente norme est d'être utilisée par les concepteurs, les exploitants de centrales nucléaires, les évaluateurs de système et par les régulateurs.

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

La CEI 61513 est le document du SC 45A de la CEI de premier niveau qui traite des exigences générales pour les systèmes. Elle est le point d'entrée de la collection des normes du SC 45A de la CEI.

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

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

Il est important de noter que la présente norme n'établit pas d'exigence fonctionnelle supplémentaire pour les systèmes de sûreté.

Afin d'assurer la pertinence de la présente norme pour les années à venir, l'accent est mis sur les questions de principes plutôt que sur les technologies particulières.

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 publication fondamentale de sécurité CEI 61508, avec un cycle de vie de sûreté d'ensemble et un cycle de vie de sûreté des systèmes. Au niveau sûreté nucléaire, elle est l'interprétation des exigences générales de la CEI 61508-1 [1][1], de la CEI 61508-2 et de la CEI 61508-4 pour le secteur nucléaire. Dans ce domaine, la CEI 60880 et la CEI 62138 correspondent à la CEI 61508-3 [2] pour le secteur nucléaire.

La CEI 61513 fait référence aux normes ISO ainsi qu'aux documents AIEA GS-R-3 et AIEA GS-G-3.1 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.

NOTE Il est fait l'hypothèse que pour la conception des systèmes d'I&C dans les CNP 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 et la prévention contre les risques liés au procédé énergétique) on applique des normes nationales ou internationales, dont les exigences sont comparables à des normes telle que la série CEI 61508.

---

1 Les chiffres entre crochets se réfèrent à la bibliographie.

CENTRALES NUCLÉAIRES DE PUISSANCE – INSTRUMENTATION ET CONTRÔLE-COMMANDE IMPORTANTS POUR LA SÛRETÉ – EXIGENCES GÉNÉRALES POUR LES SYSTÈMES

1 Domaine d'application

1.1 Généralités

Les systèmes d'I&C importants pour la sûreté peuvent être réalisés à l'aide de composants traditionnels câblés, de composants informatiques ou d'une combinaison des deux (voir Note 1). La présente Norme internationale fait état des exigences et des recommandations (voir Note 2) relatives à l'architecture d'ensemble de l'I&C incluant l'une ou l'autre de ces technologies ou les deux.

La présente norme souligne aussi la nécessité d'avoir des exigences complètes et précises, issues des objectifs de sûreté de la centrale, comme condition préalable à l'établissement des exigences relatives à l'architecture d'ensemble de l'I&C, et ensuite à l'établissement de celles portant sur chaque système d'I&C individuel important pour la sûreté.

La présente norme introduit les concepts de cycle de vie de sûreté pour l'ensemble de l'architecture d'I&C, et de cycle de vie de sûreté pour chaque système d'I&C individuel. Ainsi, elle met en exergue les relations existant entre les objectifs de sûreté de la CNP et les exigences relatives à l'architecture d'ensemble des systèmes importants pour la sûreté, et les relations existant entre l'architecture d'ensemble de l'I&C et les exigences relatives aux systèmes individuels importants pour la sûreté.

Les cycles de vie présentés et détaillés dans la présente norme ne sont pas les seuls possibles; d'autres cycles de vie peuvent être adoptés, sous réserve que les objectifs de la présente norme soient atteints.

NOTE 1 Les systèmes d'I&C peuvent aussi utiliser des modules électroniques réalisés à base de composants électroniques complexes tels que des ASICs ou des FPGA. Suivant le domaine d'application et les fonctionnalités de ces composants, ils peuvent être traités conformément aux recommandations relatives aux matériels électroniques conventionnels, ou à des matériels informatiques comparables. Une partie significative des recommandations relatives aux équipements numériques est aussi applicable lors de la conception d'équipements intégrant des composants électroniques complexes, y compris par exemple les concepts liés à réutilisation de conceptions préexistantes, ainsi que l'évaluation des erreurs de conception lors de la conception de logiciels ou de composants matériel complexe.

NOTE 2 Dans la suite de la présente norme, le terme « exigences » est utilisé comme terme général pour les « exigences et recommandations » de la norme. La distinction apparaît au niveau des exigences spécifiques, lorsque les exigences sont exprimées par «doit» et les recommandations par «il est recommander de» ou «il convient que».

1.2 Application: nouvelles centrales et centrales existantes

La présente norme s'applique à l'I&C des nouvelles centrales nucléaires, ainsi qu'à l'amélioration ou à la rénovation de l'I&C des centrales existantes.

Pour les centrales existantes, seul un sous-ensemble des exigences est applicable. Il convient de définir ce sous-ensemble au début de chaque projet.

1.3 Cadre général

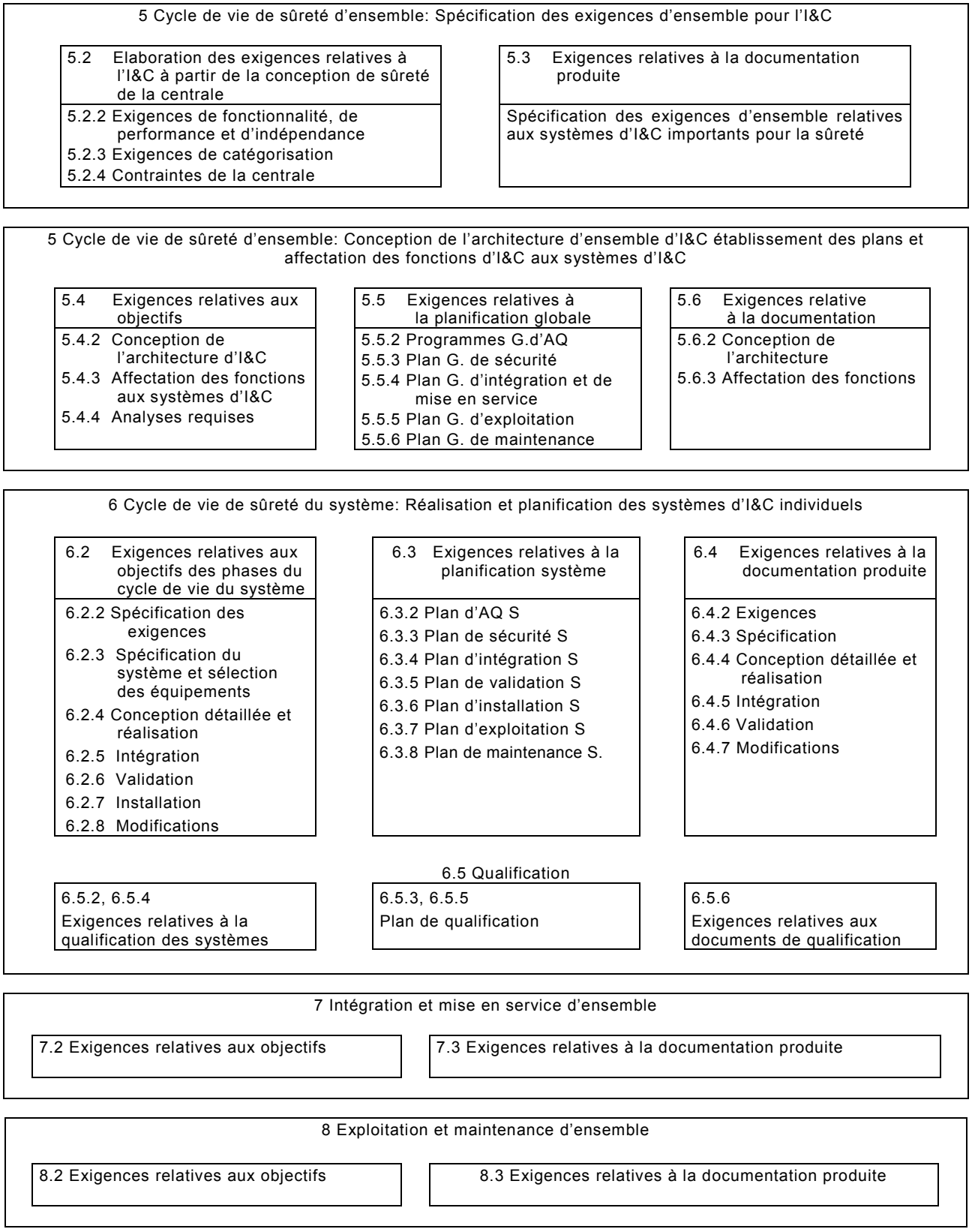
La présente norme comprend quatre articles normatifs (dont la vue d'ensemble est fournie par la Figure 1):

- l'Article 5 traite de l'architecture d'ensemble des systèmes d'I&C importants pour la sûreté:
  - définition des exigences relatives aux fonctions d'I&C et aux systèmes et équipements associés, déduites de l'analyse de sûreté de la centrale, de la catégorisation des fonctions d'I&C, de la disposition de la centrale et du contexte opérationnel,
  - découpage de l'architecture d'ensemble de l'I&C en plusieurs systèmes et affectation des fonctions d'I&C à ces systèmes. Les critères de conception y sont identifiés, y compris ceux nécessaires à la défense en profondeur et à la minimisation du risque de défaillance de cause commune (DCC),
  - établissement des plans relatifs à l'architecture d'ensemble des systèmes d'I&C.
- l'Article 6 traite des exigences relatives à chacun des systèmes d'I&C importants pour la sûreté, en particulier celles relatives aux systèmes programmés. Ceci comprend la différentiation des exigences en fonction des catégories de sûreté des fonctions d'I&C qui sont mises en œuvre;
- les Articles 7 et 8 traitent de l'intégration, de la mise en service, de l'exploitation et la maintenance des systèmes d'I&C;

NOTE La Figure 1 met en exergue la structure de la norme. Elle ne présente pas nécessairement les activités de façon chronologique qui peuvent être en réalité exécutées en parallèle ou comprendre des itérations.

De plus, la présente norme comprend les annexes informatives suivantes:

- l'Annexe A présente les relations entre les concepts de sûreté de base de l'AIEA et ceux utilisés dans la présente norme,
- l'Annexe B fournit des informations sur les principes de catégorisation et de classement,
- l'Annexe C présente des exemples illustrant les niveaux de sensibilité de l'I&C aux DCC,
- l'Annexe D est un guide pour pouvoir comparer la présente norme avec les parties 1, 2 et 4 de la CEI 61508. Elle examine les principales exigences de la CEI 61508 afin de vérifier que les questions liées à la sûreté sont abordées correctement. Elle rappelle les termes communément employés et elle justifie s'il y a lieu l'adoption de techniques ou de termes différents ou complémentaires;
- l'Annexe E indique les modifications qui devront être réalisées lors des futures révisions des normes filles de la CEI 61513 pour que celles ci soient consistantes avec la présente version et que cela minimise les chevauchements entre les contenus de documents.



Légende AQ: Assurance Qualité; G: Global; S: Système

Figure 1 – Cadre général de la présente norme

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 60880:2006, *Centrales nucléaires de puissance – Instrumentation et contrôle-commande importants pour la sûreté – Aspects logiciels des systèmes programmés réalisant des fonctions de catégorie A*

CEI 60964:2009, *Centrales nucléaires de puissance – Salles de commande – Conception*

CEI 60965, *Centrales nucléaires de puissance – Salles de commande – Points de commande supplémentaires pour l'arrêt des réacteurs sans accès à la salle de commande principale (salle de commande de repli)*

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

CEI 60987:2007, *Centrales nucléaires de puissance – Instrumentation et contrôle-commande importants pour la sûreté – Exigences applicables à la conception du matériel des systèmes informatisés*

CEI 61000-4-1, *Compatibilité électromagnétique (CEM) – Partie 4-1: Techniques d'essai et de mesure – Vue d'ensemble de la série CEI 61000-4*

CEI 61000-4-2, *Compatibilité électromagnétique (CEM) – Partie 4-2: Techniques d'essai et de mesure – Essai d'immunité aux décharges électrostatiques*

CEI 61000-4-3, *Compatibilité électromagnétique (CEM) – Partie 4-3: Techniques d'essai et de mesure – Essai d'immunité aux champs électromagnétiques rayonnés aux fréquences radioélectriques*

CEI 61000-4-4, *Compatibilité électromagnétique (CEM) – Partie 4-4: Techniques d'essai et de mesure – Essais d'immunité aux transitoires électriques rapides en salves*

CEI 61000-4-5, *Compatibilité électromagnétique (CEM) – Partie 4-5: Techniques d'essai et de mesure – Essai d'immunité aux ondes de choc*

CEI 61000-4-6, *Compatibilité électromagnétique (CEM) – Partie 4-6: Techniques d'essai et de mesure – Immunité aux perturbations conduites, induites par les champs radioélectriques*

CEI 61226:2009, *Centrales nucléaires de puissance – Instrumentation et contrôle-commande importants pour la sûreté – Classement des fonctions d'instrumentation et de contrôle-commande*

CEI 61500, *Centrales nucléaires de puissance – Instrumentation et contrôle-commande importants pour la sûreté – Communication de données dans les systèmes réalisant des fonctions de catégorie A*

CEI 61508-2:2010, *Sécurité fonctionnelle des systèmes électriques/ électroniques/électroniques programmables relatifs à la sécurité – Partie 2: Exigences pour les systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité*

CEI 61508-4:2010, *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 4: Définitions et abréviations*

CEI 62138:2004, *Centrales nucléaires – Instrumentation et contrôle-commande importants pour la sûreté – Aspects logiciels des systèmes informatisés réalisant des fonctions de catégorie B ou C*

CEI 62340, *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)*

ISO 9001:2008, *Systèmes de management de la qualité – Exigences*

AIEA INSAG N° 10:1997, *La Défense en Profondeur en Sûreté Nucléaire*

AIEA NS-R-1:2000, *Sûreté des Centrales Nucléaires: Conception*

IAEA GS-R-3:2006, *The Management System for Facilities and Activities Safety – Requirements*
(disponible en anglais seulement)

GS-G-3.1:2006, *Application of the Management System for Facilities and Activities – Safety Guide*
(disponible en anglais seulement)

AIEA NS-G-1.3:2005, *Systèmes d'instrumentation et de contrôle-commande importants pour la sûreté des centrales nucléaires*

AIEA 75-INSAG-3, Rev. 1 – INSAG 12:1999, *Principes de sûreté fondamentaux pour les centrales nucléaires*