IEC 60987

Edition 2.0 2007-08

INTERNATIONAL STANDARD

NORME INTERNATIONALE

Nuclear power plants – Instrumentation and control important to safety – Hardware design requirements for computer-based systems

Centrales nucléaires de puissance – Instrumentation et contrôle-commande importants pour la sûreté – Exigences applicables à la conception du matériel des systèmes informatisés

INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMISSION ELECTROTECHNIQUE INTERNATIONALE

PRICE CODE
CODE PRIX

V

ICS 27.120.20

ISBN 2-8318-9285-6

CONTENTS

FOREWORD 4
INTRODUCTION 6

1 Scope 8
1.1 General 8
1.2 Use of this standard for pre-developed (for example, COTS) hardware assessment 8
1.3 Applicability of this standard to programmable logic devices development 9
2 Normative references 9
3 Terms and definitions 10
4 Project structure 12
4.1 General 12
4.2 Project subdivision 12
4.3 Quality assurance 12
5 Hardware requirements 13
5.1 General 13
5.2 Functional and performance requirements 14
5.3 Reliability/Availability requirements 15
5.4 Environmental withstand requirements 16
5.5 Documentation requirements 16
6 Design and development 17
6.1 General 17
6.2 Design activities 17
6.3 Reliability 18
6.4 Maintenance 18
6.5 Interfaces 19
6.6 Modification 19
6.7 Power failure 19
6.8 Component selection 19
6.9 Design documentation 19
7 Verification and validation 20
7.1 General 20
7.2 Verification plan 20
7.3 Independence of verification 21
7.4 Methods 21
7.5 Documentation 22
7.6 Discrepancies 22
7.7 Changes and modifications 22
7.8 Installation verification 22
7.9 Validation 22
7.10 Verification of pre-existing equipment platforms 22
8 Qualification 23
9 Manufacture 23
10 Installation and commissioning 23
11 Maintenance 23
11.1 Maintenance requirements 24

11.2 Failure data 24
11.3 Maintenance documentation 25
12 Modification 26
13 Operation 26

Annex A (informative) Overview of system life cycle 27
Annex B (informative) Outline of qualification 28
Annex C (informative) Example of maintenance procedure 29

Bibliography 30

INTERNATIONAL ELECTROTECHNICAL COMMISSION

NUCLEAR POWER PLANTS – INSTRUMENTATION AND CONTROL IMPORTANT TO SAFETY – HARDWARE DESIGN REQUIREMENTS FOR COMPUTER-BASED 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 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 60987 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 1989. This edition includes the following significant technical changes with respect to the previous edition:

- account has been taken of the fact that computer design engineering techniques have advanced significantly in the intervening years;
- update of the format to align with the current IEC/ISO directives on the style of standards;
- alignment of the standard with the new revisions of IAEA documents NS-R-1 and NS-G-1.3, which includes as far as possible an adaptation of the definitions;

- replacement, as far as possible, of the requirements associated with standards published since the first edition, especially IEC 61513, IEC 60880, edition 2, and IEC 62138;
- review of the existing requirements and updating of the terminology and definitions.

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

FDIS	Report on voting
45A/662/FDIS	45A/666/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) Technical background, main issues and organization of the standard

The basic principles for the design of nuclear instrumentation, as specifically applied to the safety systems of nuclear power plants, were first interpreted in nuclear standards with reference to hardwired systems in IAEA Safety Guide 50-SG-D3 which has been superseded by IAEA Guide NS-G-1.3.

IEC 60987 was first issued in 1989 to cover the hardware aspects of digital systems design for systems important to safety, i.e. safety systems and safety-related systems.

Although many of the requirements within the original issue continue to be relevant, there were significant factors which justified the development of this revised edition of IEC 60987, in particular:

– a new standard has been produced which addresses in detail the general requirements for nuclear systems important to safety (IEC 61513);
– the use of pre-developed system platforms, rather than bespoke developments, has increased significantly.

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

The first-level IEC SC 45A standard for computer-based systems important to safety in nuclear power plants (NPPs) is IEC 61513. IEC 60987 is a second-level IEC SC 45A standard which addresses the generic issue of hardware design of computerized systems.

IEC 60880 and IEC 62138 are second-level standards which together cover the software aspects of computer-based systems used to perform functions important to safety in NPPs. IEC 60880 and IEC 62138 make direct reference to IEC 60987 for hardware design.

The requirements of IEC 60780 for equipment qualification are referenced within IEC 60987. For modules to be used in the design of a specific system important to safety, relevant and auditable operating experience from nuclear or other applications as described in IEC 60780, in combination with the application of rigorous quality assurance programmes, may be an acceptable method of qualification.

For more details on the structure of the 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 standard establishes no additional functional requirements for Class 1 or Class 2 systems (see IEC 61513 for system classification requirements).

Aspects for which special recommendations have been produced (so as to assure the production of highly reliable systems), are:

– a general approach to computing hardware development;
– a general approach to hardware verification and to the hardware aspects of computer system validation.

It is recognized that computer technology is continuing to develop and that it is not possible for a standard such as this to include references to all modern design technologies and techniques. 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 hardware design technologies. If new design techniques are developed then it should be possible to assess the suitability of such techniques by adapting and applying the design principles contained within this standard.

The scope of this standard covers digital systems hardware for Class 1 and Class 2 systems. This includes multiprocessor distributed systems and single processor systems; it covers the assessment and use of pre-developed items, for example, commercial off-the-shelf items (COTS), and the development of new hardware.

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

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 direct 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 direct 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 referenced direct 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 documents.

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 9001 as well as to IAEA 50-C-QA (now replaced by IAEA 50-C/SG-Q) 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 of NS-R-1, establishing safety requirements related to the design of NPPs, and Safety Guide NS-G-1.3 dealing with instrumentation and control systems important to safety in NPPs. The terminology and definitions used by SC 45A standards are consistent with those used by the IAEA.

NUCLEAR POWER PLANTS – INSTRUMENTATION AND CONTROL IMPORTANT TO SAFETY – HARDWARE DESIGN REQUIREMENTS FOR COMPUTER-BASED SYSTEMS

1 Scope

1.1 General

This International Standard is applicable to NPP computer-system hardware for systems of Class 1 and 2 (as defined by IEC 61513).

The structure of this standard has not changed significantly from the original 1989 issue; however, some issues are now covered by standards which have been issued in the interim (for example, IEC 61513 for system architecture design) and references to new standards have been provided where applicable. The text of the standard has also been modified to reflect developments in computer system hardware design, the use of pre-developed (for example, COTS) hardware and changes in terminology.

Computer hardware facilities used for software loading and checking are not considered to form an intrinsic part of a system important to safety and, as such, are outside the scope of this standard.

NOTE 1 Class 3 computer-system hardware is not addressed by this standard, and it is recommended that such systems should be developed to commercial grade standards.

NOTE 2 In 2006 the development of a new standard to address hardware requirements for “very complex” hardware was discussed within IEC SC 45A. If such a standard is developed then that standard would be used for the development of “very complex” hardware in preference to IEC 60987.

1.2 Use of this standard for pre-developed (for example, COTS) hardware assessment

Although the primary aim of this standard is to address aspects of new hardware development, the processes defined within this standard may also be used to guide the assessment and use of pre-developed hardware, such as COTS hardware. Guidance has been provided in the text concerning the interpretation of the requirements of this standard when used for the assessment of such components. In particular, the quality assurance requirements of 4.3, concerning configuration control, apply.

Pre-developed components may contain firmware (as defined in 3.8), and, where firmware software is deeply imbedded, and effectively “transparent” to the user, then IEC 60987 should be used to guide the assessment process for such components. An example of where this approach is considered appropriate is in the assessment of modern processors which contain a microcode. Such a code is generally an integral part of the “hardware”, and it is therefore appropriate for the processor (including the microcode) to be assessed as an integrated hardware component using this standard.

Software which is not firmware, as described above, should be developed or assessed according to the requirements of the relevant software standard (for example, IEC 60880 for Class 1 systems and IEC 62138 for Class 2 systems).

1.3 Applicability of this standard to programmable logic devices development

I&C components may include programmable logic devices that are given their specific application logic design by the designer of the I&C component, as opposed to the chip manufacturer. Examples of such devices include complex programmable logic devices (CPLD) and field programmable gate arrays (FPGA).

While the programmable nature of these devices gives the development processes used for these devices, some of the characteristics of a software development process and the design processes used for such devices, are very similar to those used to design logic circuits implemented with discrete gates and integrated circuit packages. Therefore, the design processes and design verification applied to programmable logic devices should comply with the relevant requirements of this standard (i.e. taking into account the particular features of the design processes of such devices). To the extent that software-based tools are used to support the design processes for programmable logic devices, those software tools should generally follow the guidance provided for software-based development tools in the appropriate software standard, i.e. IEC 60880 (Class 1 systems) or IEC 62138 (Class 2 systems).

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

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

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

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

IEC 61025, *Fault tree analysis (FTA)*

IEC 61513:2001, *Nuclear power plants – Instrumentation and control for systems important to safety – General requirements for systems*

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

ISO 9001, *Quality management systems – Requirements*

IAEA NS-G 1.3, *Instrumentation and control systems important to safety in nuclear power plants*

IAEA 50-C/SG-Q:1996, *Quality assurance for safety in nuclear power plants and other nuclear installations*

SOMMAIRE

AVANT-PROPOS 34
INTRODUCTION 36

1 Domaine d'application 38
1.1 Généralités 38
1.2 Utilisation de cette norme pour l'évaluation des matériels prédéveloppés (par exemple les COTS) 38
1.3 Application de cette norme au développement des composants logiques programmables 39
2 Références normatives 39
3 Termes et définitions 40
4 Structure du projet 42
4.1 Généralités 42
4.2 Subdivision du projet 42
4.3 Assurance qualité 43
5 Exigences applicables au matériel 43
5.1 Généralités 43
5.2 Exigences fonctionnelles et de performances 44
5.3 Exigences de fiabilité/disponibilité 45
5.4 Exigences relatives à la résistance aux conditions d'environnement 46
5.5 Exigences documentaires 47
6 Conception et développement 47
6.1 Généralités 47
6.2 Activités de conception 48
6.3 Fiabilité 48
6.4 Maintenance 49
6.5 Interfaces 49
6.6 Modifications 49
6.7 Perte d'alimentation électrique 49
6.8 Sélection des composants 50
6.9 Documentation de conception 50
7 Vérification et validation 51
7.1 Généralités 51
7.2 Plan de vérification 51
7.3 Indépendance de la vérification 51
7.4 Méthodes 52
7.5 Documentation 52
7.6 Non-conformités 53
7.7 Changements et modifications 53
7.8 Vérification de l'installation 53
7.9 Validation 53
7.10 Vérification de plateformes matériel préexistantes 53
8 Qualification 53
9 Fabrication 54
10 Installation et mise en service 54
11 Maintenance 54

11.1 Exigences de maintenance 55
11.2 Données relatives aux défaillances 55
11.3 Documentation de maintenance 56
12 Modifications 57
13 Exploitation 57

Annexe A (informative) Vue générale du cycle de vie système 58
Annexe B (informative) Tracé du contour de la qualification 59
Annexe C (informative) Exemple de procédure de maintenance 60

Bibliographie 61

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

CENTRALES NUCLÉAIRES DE PUISSANCE – INSTRUMENTATION ET CONTRÔLE-COMMANDE IMPORTANTS POUR LA SÛRETÉ – EXIGENCES APPLICABLES À LA CONCEPTION DU MATÉRIEL DES SYSTÈMES INFORMATISÉS

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 60987 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 parue en 1989. Cette édition inclut les modifications techniques majeures suivantes par rapport à l'édition précédente:

- prise en compte du fait que les techniques de conception du matériel des systèmes informatisés ont progressé de façon significative ces dernières années;
- mise à jour du format de la norme pour être conforme aux directives ISO/CEI portant sur le style des normes;
- mise en cohérence de la norme avec les nouvelles révisions des documents de l'AIEA NS-R-1 et NS-G-1.3, cela comprenant autant que possible une adaptation des définitions;

- remplacement, autant que faire se peut, des exigences associées aux normes publiées depuis la parution de la première édition de la CEI 60880, plus particulièrement la CEI 61513, la CEI 60880, édition 2, et la CEI 62138;
- revue des exigences existantes et mise à jour des définitions et de la terminologie.

Le texte de cette norme est issu des documents suivants:

FDIS	Rapport de vote
45A/662/FDIS	45A/666/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 cette norme

Les principes de base de conception de l'instrumentation nucléaire tels que particulièrement appliqués aux systèmes de sûreté des centrales nucléaires de puissance (CNP) furent interprétés dans les normes du secteur nucléaire en référence aux systèmes câblés, en particulier dans le «Guide de sûreté 50-SG-D3» de l'AIEA qui a été remplacé par le guide de l'AIEA NS-G-1.3.

La première édition de la CEI 60987 a été publiée en 1989 pour couvrir les aspects matériels de la conception des systèmes informatisés des systèmes importants pour la sûreté, c'est-à-dire, des systèmes de sûreté et des systèmes liés à la sûreté.

Bien que beaucoup des exigences contenues dans la première édition de la norme restent pertinentes, des facteurs significatifs ont justifié du développement de la révision de la CEI 60987, et en particulier:

– une nouvelle norme est parue qui traite en détail des exigences générales applicables au systèmes nucléaires importants pour la sûreté (la CEI 61513);
– l'utilisation de plateformes système prédéveloppées, plutôt que de développements faits sur commande, a significativement augmentée.

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

La norme de premier niveau du SC 45A concernant les systèmes informatisés importants pour la sûreté utilisés dans les centrales nucléaires de puissance (CNPs) est la CEI 61513. La CEI 60987 est un document du SC 45A de deuxième niveau qui traite de la question générique de la conception du matériel des systèmes informatisés.

La CEI 60880 et la CEI 62138 sont des normes de second niveau de la collection de normes du SC 45A qui couvrent ensemble les aspects logiciels relatifs aux systèmes informatisés utilisés pour réaliser des fonctions importantes pour la sûreté des CNP. Les CEI 60880 et CEI 62138 font directement référence à la CEI 60987 pour la conception du matériel.

La CEI 60987 fait référence aux exigences de la CEI 60780 en matière de qualification du matériel. Concernant les modules utilisés pour la conception de systèmes particuliers importants pour des applications de sûreté, les retours d'expérience pertinents et qui peuvent faire l'objet d'audits dans le domaine du nucléaire ou pour d'autres applications, peuvent, comme cela est décrit dans la CEI 60780, en combinaison avec l'exécution d'un programme rigoureux d'assurance qualité, constituer une méthode acceptable de qualification.

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

Il est important de noter que cette norme n'établit pas d'exigence fonctionnelle supplémentaire pour les systèmes de Classe 1 ou de Classe 2 (voir la CEI 61513 pour ce qui concerne les exigences de classement des systèmes).

Pour assurer la production de systèmes d'une grande fiabilité, cette norme fournit des recommandations particulières pour les aspects suivants:

– une approche générale du développement du matériel informatique;
– une approche générale de la vérification du matériel et des aspects liés au matériel de la validation des systèmes informatisés.

Il est reconnu que la technologie informatique est continuellement en développement et qu'il n'est pas possible pour une norme telle que celle-ci de faire référence aux technologies et techniques de conception modernes. L'accent a été mis sur les questions de principes plutôt que sur celles spécifiques aux technologies liées à la conception du matériel, pour assurer que la norme soit pertinente dans les années à venir. Si de nouvelles techniques de conception sont développées alors il devrait être possible d'évaluer l'aptitude de telles techniques à être employées en adaptant et en appliquant les principes de conception contenus dans cette norme.

Le domaine d'application de cette norme couvre le matériel des systèmes informatisés utilisés par des systèmes de Classe 1 et de Classe 2. Ceci comprend les systèmes multiprocesseurs répartis et les systèmes monoprocesseurs; elle couvre l'évaluation et l'utilisation des éléments commercialement disponibles sur étagère (COTS) et le développement de nouveaux matériels.

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

Le document de niveau supérieur de la collection de normes produites par le SC 45A de la CEI est la 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 CNPs, 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 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 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 des CEI 61508-1, CEI 61508-2 et 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 à l'ISO 9001 ainsi qu'au document AIEA 50-C-QA (remplacé depuis par le document AIEA 50-C/SG-Q) 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 CNPs, ainsi qu'avec les guides de sûreté de l'AIEA, en particulier le document d'exigences NS-R-1 qui établit les exigences de sûreté relatives à la conception des CNPs et 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 – INSTRUMENTATION ET CONTRÔLE-COMMANDE IMPORTANTS POUR LA SÛRETÉ – EXIGENCES APPLICABLES À LA CONCEPTION DU MATÉRIEL DES SYSTÈMES INFORMATISÉS

1 Domaine d'application

1.1 Généralités

La présente Norme internationale est applicable au matériel des systèmes informatisés des CNPs de Classes 1 et 2 (telles que définies dans la CEI 61513).

La structure de cette norme n'a pas évoluée de façon significative depuis la version originale publiée en 1989, néanmoins certaines éléments apparus entre-temps sont maintenant pris en compte par celle-ci (par exemple la CEI 61513 pour la conception de l'architecture des systèmes) et des références aux nouvelles normes sont fournies lorsque cela est pertinent. Le texte de cette norme a aussi évolué pour refléter les développements survenus dans le domaine de la conception du matériel des systèmes informatisés, l'utilisation de matériels prédéveloppés commercialement disponibles sur étagère (par exemple, les COTS) et l'évolution de la terminologie.

Les ensembles de matériel informatique utilisés pour le chargement et la vérification du logiciel ne sont pas considérés comme faisant partie intrinsèque du système important pour la sûreté et comme tel sont hors du domaine d'application de cette norme.

NOTE 1 Le matériel des systèmes informatisés de Classe 3 n'est pas couvert par cette norme et il est recommandé que de tels systèmes soient développés conformément à des normes commerciales.

NOTE 2 En 2006, des discussions ont eu lieu au SC 45A de la CEI pour le développement d'une nouvelle norme concernant les exigences relatives au matériel très complexe. Si cette norme est développée, alors on l'utilisera de préférence à la CEI 60987.

1.2 Utilisation de cette norme pour l'évaluation des matériels pré-développés (par exemple les COTS)

Bien que le but principal de cette norme soit de traiter du sujet du développement du nouveau matériel, le processus défini dans la norme peut aussi servir de guide dans l'évaluation du matériel prédéveloppé tel que COTS. Le texte fournit des recommandations pour interpréter les exigences de la norme lorsque celle-ci est employée pour évaluer de tels composants. En particulier, les exigences d'assurance qualité de 4.3 concernant la gestion de configuration s'appliquent.

Les composants prédéveloppés peuvent contenir des microprogrammes (tels que définis en 3.8) et, lorsque les microprogrammes sont profondément intégrés et que la présence de tels logiciels est effectivement « transparente » pour l'utilisateur, alors il convient d'utiliser la CEI 60987 comme guide pour l'évaluation de tels composants. Un exemple pour lequel cette approche est considérée comme adaptée est l'évaluation des processeurs modernes qui comprennent du microcode. Un tel code fait généralement partie intégrante du matériel, ainsi il est donc acceptable d'évaluer le processeur (comprenant le microcode) en tant que composant matériel intégré en se servant de la présente norme.

Il convient de développer ou d'évaluer le logiciel qui ne peut être considéré comme un microprogramme tel que décrit ci-dessus, conformément aux exigences des normes logiciel applicables (par exemple la CEI 60880 pour les systèmes de Classe 1 ou la CEI 62138 pour les systèmes de Classe 2).

1.3 Application de cette norme au développement des composants logiques programmables

Des composants d'I&C (instrumentation et contrôle-commande) peuvent contenir des composants logiques programmables dont la conception logique applicative particulière est assurée par le concepteur du composant d'I&C, et non par le fabricant de composants électroniques, par exemple les « complex programmable logic devices (CPLD) » et les « field programmable gate arrays (FPGA) ».

Alors que la nature programmable de ces composants confère aux processus de développement utilisés pour ceux-ci, certaines caractéristiques propres aux processus de développement logiciel, les processus de développement utilisés pour de tels composants sont très proches de ceux suivis pour la conception des circuits logiques mettant en œuvre des composants discrets et des circuits intégrés. Ainsi, les processus de conception et de vérification de la conception retenus pour ces dispositifs programmables logiques doivent être conformes aux exigences applicables de la présente norme (par exemple en prenant en compte les caractéristiques particulières des processus de développement de tels dispositifs). Dans la mesure où des outils logiciels sont utilisés en support des processus de conception des composants logiques programmables, il convient que ces outils logiciels suivent les recommandations applicables au développement d'outils logiciels fournies par les normes pertinentes, par exemple la CEI 60880 (systèmes de Classe 1) ou la CEI 62138 (système de Classe 2).

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

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

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

CEI 61025, *Analyse par arbre de panne (AAP)*

CEI 61513:2001, *Centrales nucléaires – Instrumentation et contrôle commande des systèmes importants pour la sûreté – Prescriptions générales pour les systèmes*

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

ISO 9001, *Système de management de la qualité – Exigences*

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

AIEA 50-C/SG-Q:1996, *Assurance de la qualité pour la sûreté des centrales nucléaires de puissance et les autres installations nucléaires*