IEC 60987

Edition 3.0 2021-02

INTERNATIONAL STANDARD

NORME INTERNATIONALE

Nuclear power plants – Instrumentation and control important to safety – Hardware requirements

Centrales nucléaires de puissance – Systèmes d'instrumentation et de contrôle-commande importants pour la sûreté – Exigences applicables au matériel

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

ICS 27.120.20

ISBN 978-2-8322-9319-5

Warning! Make sure that you obtained this publication from an authorized distributor.
Attention! Veuillez vous assurer que vous avez obtenu cette publication via un distributeur agréé.

® Registered trademark of the International Electrotechnical Commission
Marque déposée de la Commission Electrotechnique Internationale

CONTENTS

FOREWORD 4
INTRODUCTION 6
1 Scope 9
2 Normative references 9
3 Terms and definitions 10
4 Symbols and abbreviated terms 17
5 Hardware safety lifecycle 17
5.1 General 17
5.2 Hardware safety lifecycle for class 1 and class 2 20
5.2.1 Project structure for class 1 and class 2 20
5.2.2 Quality management for class 1 and class 2 20
5.2.3 Verification of hardware for class 1 and class 2 21
5.3 Hardware safety lifecycle for class 3 23
5.3.1 Project structure and quality management for class 3 23
5.3.2 Verification of hardware for class 3 24
6 Hardware aspects of system requirements specification 24
6.1 Hardware aspects of system requirements specification for class 1 and class 2 24
6.1.1 General requirements for class 1 and class 2 24
6.1.2 Functional and performance requirements for class 1 and class 2 25
6.1.3 Reliability requirements for class 1 and class 2 26
6.1.4 Environmental conditions requirements for class 1 and class 2 27
6.1.5 Manufacturing requirements for class 1 and class 2 27
6.1.6 Documentation requirements for class 1 and class 2 27
6.2 Hardware aspects of system requirements specification for class 3 27
6.2.1 General requirements for class 3 27
6.2.2 Reliability for class 3 27
6.2.3 Environmental conditions requirements for class 3 28
6.2.4 Documentation requirements for class 3 28
7 Selection of pre-existing components 28
7.1 Selection of pre-existing components for class 1 and class 2 28
7.2 Selection of pre-existing components for class 3 29
8 Hardware aspects of system detailed design and implementation 29
8.1 Hardware aspects of system detailed design and implementation for class 1 and class 2 29
8.1.1 General requirement for class 1 and class 2 29
8.1.2 Design activities for class 1 and class 2 30
8.1.3 Reliability for class 1 and class 2 30
8.1.4 Maintenance for class 1 and class 2 31
8.1.5 Power failure for class 1 and class 2 32
8.1.6 Design documentation for class 1 and class 2 32
8.2 Hardware aspects of system detailed design and implementation for class 3 33
8.2.1 General requirement for class 3 33
8.2.2 Reliability for class 3 33
8.2.3 Maintenance for class 3 33
9 Equipment (component) manufacturing 33

9.1 Equipment (component) manufacturing for class 1 and class 2 33
9.1.1 Manufacturing quality management for class 1 and class 2 33
9.1.2 Training of personnel for class 1 and class 2 34
9.1.3 Planning and organisation of the manufacturing activities for class 1 and class 2 35
9.1.4 Input data for class 1 and class 2 35
9.1.5 Purchasing and procurement for class 1 and class 2 35
9.1.6 Manufacturing for class 1 and class 2 36
9.2 Equipment (component) manufacturing for class 3 41
9.2.1 Manufacturing quality management for class 3 41
9.2.2 Training of personnel for class 3 41
9.2.3 Input data for class 3 41
9.2.4 Purchasing and procurement for class 3 42
9.2.5 Assessment of electronic modules for class 3 42
9.2.6 Identification and traceability for class 3 43
9.2.7 Protection and storage of product for class 3 43
9.2.8 Manufacturing of electronic modules for class 3 44
10 Hardware aspects of system installation 44
10.1 General 44
11 Hardware aspects of system modification 45
11.1 General 45
12 Operation and maintenance 45
12.1 General 45
12.2 Operation and maintenance requirements 46
12.3 Failure data 46
12.3.1 Failure data acquired during equipment operation constitutes a major source of information which can be used to improve: 46
12.4 Operation and maintenance documentation 47
Annex A (informative) Typical documentation 48
Bibliography 49

Figure 1 – System safety lifecycle (informative, as defined by IEC 61513) 18
Figure 2 – Hardware related activities in the system safety lifecycle 19

Table A.1 – Typical documentation 48

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

NUCLEAR POWER PLANTS – INSTRUMENTATION AND CONTROL IMPORTANT TO SAFETY – HARDWARE REQUIREMENTS

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 60987 has been prepared by subcommittee 45A: Instrumentation, control and electrical power systems of nuclear facilities, of IEC technical committee 45: Nuclear instrumentation.

This third edition cancels and replaces the second edition published in 2007, and its Amendment 1, published in 2013. This edition constitutes a technical revision.

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

a) Title modified;
b) Take account of the fact that hardware requirements apply to all I&C technologies, including conventional hardwired equipment, programmable digital equipment or by using a combination of both types of equipment;
c) Align the standard with the new revisions of IAEA documents SSR-2/1, which include as far as possible an adaptation of the definitions;

d) Replace, as far as possible, the requirements associated with standards published since the edition 2.1, especially IEC 61513, IEC 60880, IEC 62138, IEC 62566 and IEC 62566-2;

e) Review the existing requirements and update the terminology and definitions;

f) Extend the scope of the standard to all hardware (computerized and non-computerized) and to all safety classes 1, 2 and 3;

g) Complete, update the IEC and IAEA references and vocabulary;

h) Check possible impact of other IAEA requirements and recommendations considering extension of the scope of SC 45A;

i) Highlight the use of IEC 62566 and IEC 62566-2 for HPD development;

j) Introduce specific activities for pre-existing items (selection, acceptability and/or mitigation);

k) Introduce clearer requirements for electronic module-level design, manufacturing and control;

l) Complete reliability assessment methods;

m) Introduce requirements when using automated tests or control activities;

n) Complete description of manufacturing control activities (control process, assessment of manufactured equipment, preservation of products);

o) Define and ensure the inclusion of a graded approach for dealing with the 3 different classes of equipment and related requirements.

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

FDIS	Report on voting
45A/1365/FDIS	45A/1372/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.

INTRODUCTION

a) Technical background, main issues and organization of the standard

This International Standard provides requirements on the hardware aspects of E/E/PE items used in instrumentation and control (I&C) systems performing safety functions as defined by IEC 61226.

It is consistent with, and complementary to, IEC 61513. Activities that are mainly system level activities (for example, integration, validation and installation) are not addressed exhaustively by this document: requirements that are not specific to hardware are deferred to IEC 61513.

The basic principles for the design of nuclear instrumentation, as specifically applied to the systems important to safety 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 SSG-39.

IEC 60987 was first issued in 1989 to cover the hardware aspects of digital systems design for systems important to safety.

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:

– the use of different technologies that may include conventional hardwired equipment, programmable digital equipment or by using a combination of both types of equipment;
– IEC 61226 and IEC 61513 cover I&C systems performing 3 different categories of functions (A, B and C) and 3 classes of systems (class 1, 2 and 3);
– the use of pre-existing components, 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 I&C 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 I&C systems hardware requirements.

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 I&C systems hardware requirements.

IEC 62566 and IEC 62566-2 are second-level standards which together cover the development of HPDs used to perform functions important to safety in NPPs. IEC 62566 and IEC 62566-2 make direct reference to IEC 60987 for I&C systems hardware requirements.

The requirements of IEC/IEEE 60780-323 for equipment qualification are referenced within IEC 60987.

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 standard establishes no additional functional requirements for classified systems (see IEC 61226 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 the hardware safety lifecycle;
– an approach from the requirements specifications down to on-site operation and maintenance activities.

It is recognized that I&C technology is continuing to evolve 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 is possible to assess the suitability of such techniques by adapting and applying the design principles contained within this standard.

The scope of this document covers I&C systems hardware for all classes of systems important to safety. This includes conventional hardwired equipment, programmable digital equipment or by using a combination of both types of equipment; it covers the assessment and use of pre-existing items, for example, commercial off-the-shelf items (COTS), and the development of new hardware.

This document does not explicitly address how to protect systems against those threats arising from malicious attacks, i.e. cybersecurity, for programmable digital item. IEC 62645 provides requirements for security programmes for programmable digital item for all their development phases and on-site operation.

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, defence 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 part 2 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, IEC 60964 is the entry document for the IEC/SC 45A control rooms standards and IEC 62342 is the entry document for the ageing management standards.

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, chemical hazards, process energy hazards) international or national standards would be applied.

NUCLEAR POWER PLANTS – INSTRUMENTATION AND CONTROL IMPORTANT TO SAFETY – HARDWARE REQUIREMENTS

1 Scope

I&C systems important to safety may be implemented using conventional hardwired equipment, programmable digital equipment or by using a combination of both types of equipment.

This document provides requirements and recommendations for the hardware aspects of I&C systems whatever the technology and applies for all safety classes in a graded manner (as defined by IEC 61513).

The requirements defined within this document guide, in particular, the selection of pre-existing components, hardware aspects of system detailed design and implementation and equipment manufacturing.

This document does not explicitly address how to protect systems against those threats arising from malicious attacks, i.e. cybersecurity, for programmable digital item. IEC 62645 provides requirements for security programmes for programmable digital item for all their development phases and on-site operation.

Pre-existing items may include microcontrollers or HPDs and, where firmware or programming files are deeply-embedded, be effectively "transparent" to the user. In such cases, this document can 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 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 document.

Software which is not deeply-embedded, as described above, is 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 and 3 systems).

In the same manner, HPDs which are not deeply-embedded, as described above, are developed or assessed according to the requirements of the relevant HPD standard (for example, IEC 62566 for class 1 systems and IEC 62566-2 for class 2 and 3 systems).

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

IEC 60812, *Failure modes and effects analysis (FMEA and FMECA)*

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

IEC/IEEE 60980-344, *Nuclear facilities – Equipment important to safety – Seismic qualification*

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

IEC 61025, *Fault tree analysis (FTA)*

IEC 61513:2011, *Nuclear power plants – Instrumentation and control important to safety – General requirements for systems*

IEC 61709, *Electrical components – Reliability – Reference conditions for failure rates and stress models for conversion*

IEC 62003, *Nuclear power plants – Instrumentation, control and electrical power systems – Requirements for electromagnetic compatibility testing*

IEC 62138:2018, *Nuclear power plants – Instrumentation and control systems important to safety – Software aspects for computer-based systems performing category B or C functions*

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

IEC 62566-2, *Nuclear power plants – Instrumentation and control systems important to safety – Development of HDL-programmed integrated circuits – Part 2: HDL-programmed integrated circuits for systems performing category B or C functions*

ISO 28590, *Sampling procedures for inspection by attributes — Introduction to the ISO 2859 series of standards for sampling for inspection by attributes*

IPC-A-610, *Acceptability of Electronic Assemblies*

SOMMAIRE

AVANT-PROPOS 52
INTRODUCTION 54
1 Domaine d'application 57
2 Références normatives 57
3 Termes et définitions 58
4 Symboles et termes abrégés 66
5 Cycle de vie et de sûreté du matériel 66
5.1 Généralités 66
5.2 Cycle de vie et de sûreté du matériel pour la classe 1 et la classe 2 69
5.2.1 Structure du projet pour la classe 1 et la classe 2 69
5.2.2 Gestion de la qualité pour la classe 1 et la classe 2 70
5.2.3 Vérification du matériel pour la classe 1 et la classe 2 70
5.3 Cycle de vie et de sûreté du matériel pour la classe 3 73
5.3.1 Structure du projet et gestion de la qualité pour la classe 3 73
5.3.2 Vérification du matériel pour la classe 3 74
6 Aspects matériels de la spécification des exigences système 74
6.1 Aspects matériels de la spécification des exigences système pour la classe 1 et la classe 2 74
6.1.1 Exigences générales pour la classe 1 et la classe 2 74
6.1.2 Exigences fonctionnelles et de performances pour la classe 1 et la classe 2 75
6.1.3 Exigences de fiabilité pour la classe 1 et la classe 2 76
6.1.4 Exigences relatives aux conditions d'environnement pour la classe 1 et la classe 2 76
6.1.5 Exigences de fabrication pour la classe 1 et la classe 2 77
6.1.6 Exigences documentaires pour la classe 1 et la classe 2 77
6.2 Aspects matériels de la spécification des exigences système pour la classe 3 77
6.2.1 Exigences générales pour la classe 3 77
6.2.2 Fiabilité pour la classe 3 77
6.2.3 Exigences relatives aux conditions d'environnement pour la classe 3 77
6.2.4 Exigences documentaires pour la classe 3 77
7 Sélection des composants préexistants 78
7.1 Sélection de composants préexistants pour la classe 1 et la classe 2 78
7.2 Sélection de composants préexistants pour la classe 3 78
8 Aspects matériels de la conception détaillée et de la mise en œuvre du système 79
8.1 Aspects matériels de la conception détaillée et de la mise en œuvre du système pour les classes 1 et 2 79
8.1.1 Exigences générales pour la classe 1 et la classe 2 79
8.1.2 Activités de conception pour la classe 1 et la classe 2 79
8.1.3 Fiabilité pour la classe 1 et la classe 2 80
8.1.4 Maintenance pour la classe 1 et la classe 2 81
8.1.5 Perte d'alimentation électrique pour la classe 1 et la classe 2 82
8.1.6 Documentation de conception pour la classe 1 et la classe 2 82
8.2 Aspects matériels de la conception détaillée et de la mise en œuvre du système pour la classe 3 83
8.2.1 Exigence générale pour la classe 3 83

8.2.2 Fiabilité pour la classe 3 83
8.2.3 Maintenance pour la classe 3 83
9 Fabrication d'équipements (composants) 84
9.1 Fabrication d'équipements (composants) pour la classe 1 et la classe 2 84
9.1.1 Gestion de la qualité de fabrication pour la classe 1 et la classe 2 84
9.1.2 Formation du personnel pour la classe 1 et la classe 2 85
9.1.3 Planification et organisation des activités de fabrication pour la classe 1 et la classe 2 85
9.1.4 Données d'entrée pour la classe 1 et la classe 2 85
9.1.5 Achat et approvisionnement pour la classe 1 et la classe 2 86
9.1.6 Fabrication pour la classe 1 et la classe 2 87
9.2 Fabrication d'équipements (composants) pour la classe 3 92
9.2.1 Gestion de la qualité de fabrication pour la classe 3 92
9.2.2 Formation du personnel pour la classe 3 92
9.2.3 Données d'entrée pour la classe 3 92
9.2.4 Achat et approvisionnement pour la classe 3 93
9.2.5 Évaluation des modules électroniques pour la classe 3 93
9.2.6 Identification et traçabilité pour la classe 3 94
9.2.7 Protection et stockage des produits pour la classe 3 95
9.2.8 Fabrication des modules électroniques pour la classe 3 95
10 Aspects matériels de l'installation du système 95
10.1 Généralités 95
11 Aspects matériels de la modification du système 96
11.1 Généralités 96
12 Exploitation et maintenance 97
12.1 Généralités 97
12.2 Exigences d'exploitation et de maintenance 97
12.3 Données relatives aux défaillances 98
12.3.1 Les données relatives aux défaillances acquises durant l'exploitation du matériel constituent une des sources principales d'information pouvant être utilisées pour améliorer 98
12.4 Documentation de l'exploitation et de la maintenance 98
Annexe A (informative) Documentation type 100
Bibliographie 101

Figure 1 – Cycle de vie et de sûreté du système (informative, comme cela est défini par l'IEC 61513) 67
Figure 2 – Activités liées au matériel dans le cycle de vie et de sûreté des systèmes 68

Tableau A.1 – Documentation type 100

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

CENTRALES NUCLÉAIRES DE PUISSANCE – SYSTÈMES D'INSTRUMENTATION ET DE CONTRÔLE-COMMANDE IMPORTANTS POUR LA SÛRETÉ – EXIGENCES APPLICABLES AU MATÉRIEL

AVANT-PROPOS

1) La Commission Électrotechnique 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. À 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 60987 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 troisième édition annule et remplace la deuxième édition parue en 2007, et son Amendement 1 paru en 2013. Cette édition constitue une révision technique.

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

a) Modification du titre;
b) Prise en compte du fait que les exigences en matière de matériel s'appliquent à toutes les technologies d'I&C, y compris des équipements câblés conventionnels, des équipements numériques programmables ou une combinaison de ces deux types d'équipements;
c) Alignement de la norme sur les nouvelles révisions des documents de l'AIEA SSR-2/1, incluant autant que possible une adaptation des définitions;
d) Remplacement, autant que possible, des exigences associées aux normes publiées depuis la parution de l'édition 2.1, plus particulièrement l'IEC 61513, l'IEC 60880, l'IEC 62138, l'IEC 62566 et l'IEC 62566-2;
e) Révision des exigences existantes et mise à jour des définitions et de la terminologie;
f) Élargissement du domaine d'application de la norme à tout le matériel (informatisé et non informatisé) et à toutes les classes de sûreté 1, 2 et 3;
g) Complément et mise à jour des références et du vocabulaire de l'IEC et de l'AIEA;
h) Vérification de l'impact éventuel d'autres exigences et recommandations de l'AIEA envisageant l'extension du domaine d'application du SC 45A;
i) Mise en évidence de l'utilisation de l'IEC 62566 et de l'IEC 62566-2 pour le développement du HPD;
j) Introduction d'activités spécifiques pour les constituants prédéveloppés (sélection, acceptabilité et/ou compensation);
k) Introduction d'exigences plus claires pour la conception, la fabrication et le contrôle au niveau des modules électroniques;
l) Méthodes complètes d'évaluation de la fiabilité;
m) Introduction d'exigences lors de l'utilisation d'essais automatisés ou d'activités de contrôle;
n) Complément concernant les activités de contrôle de la fabrication (processus de contrôle, évaluation des équipements fabriqués, préservation des produits);
o) Définition et incorporation d'une approche graduelle pour traiter les 3 différentes classes d'équipements et les exigences qui s'y rapportent.

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

FDIS	Rapport de vote
45A/1365/FDIS	45A/1372/RVD

Le rapport de vote indiqué dans le tableau ci-dessus donne toute information sur le vote ayant abouti à l'approbation de la présente Norme internationale.

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. À cette date, le document sera

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

INTRODUCTION

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

La présente Norme internationale fournit des exigences sur les aspects matériels des éléments E/E/PE utilisés dans les systèmes d'instrumentation et de contrôle (I&C) remplissant des fonctions de sûreté telles que définies par l'IEC 61226.

Elle est conforme à l'IEC 61513 et la complète. Les activités qui sont principalement des activités au niveau du système (par exemple, l'intégration, la validation et l'installation) ne sont pas traitées de manière exhaustive par le présent document: les exigences qui ne sont pas spécifiques au matériel sont reportées à l'IEC 61513.

Les principes de base de conception de l'instrumentation nucléaire tels qu'ils sont spécifiquement appliqués aux systèmes importants pour la sûreté des centrales nucléaires de puissance (CNP) ont d'abord été 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 SSG-39.

La première édition de l'IEC 60987 a été publiée en 1989 pour couvrir les aspects matériels de la conception des systèmes informatisés des systèmes importants pour 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 présente révision de l'IEC 60987, et en particulier:

– l'utilisation de différentes technologies qui peuvent comprendre des équipements câblés conventionnels, des équipements numériques programmables ou une combinaison de ces deux types d'équipements;
– l'IEC 61226 et l'IEC 61513 couvrent les systèmes d'I&C qui remplissent 3 catégories de fonctions différentes (A, B et C) et 3 classes de systèmes (classe 1, 2 et 3);
– l'utilisation de composants préexistants, plutôt que de développements spécifiques, a significativement augmenté.

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

La norme de premier niveau du SC 45A concernant les systèmes d'I&C importants pour la sûreté utilisés dans les centrales nucléaires de puissance (CNP) est l'IEC 61513. L'IEC 60987 est la norme du SC 45A de deuxième niveau qui traite de la question générique des exigences matériel des systèmes d'I&C.

L'IEC 60880 et l'IEC 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. L'IEC 60880 et l'IEC 62138 font directement référence à l'IEC 60987 pour les exigences matériel des systèmes d'I&C.

L'IEC 62566 et l'IEC 62566-2 sont des normes de deuxième niveau qui, ensemble, couvrent le développement des HPD utilisés pour remplir des fonctions importantes pour la sûreté des centrales nucléaires. L'IEC 62566 et l'IEC 62566-2 font directement référence à l'IEC 60987 pour les exigences matériel des systèmes d'I&C.

L'IEC 60987 fait référence aux exigences de l'IEC/IEEE 60780-323 en matière de qualification du matériel.

Pour de plus amples informations sur la collection de normes du SC 45A de l'IEC, voir le paragraphe d) de la présente introduction.

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

Il est important de noter que la présente norme n'établit pas d'exigence fonctionnelle supplémentaire pour les systèmes de sûreté (voir l'IEC 61226 pour ce qui concerne les exigences de classement des systèmes).

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

– une approche générale du cycle de vie et de sûreté du matériel;
– une approche allant des spécifications des exigences jusqu'aux activités d'exploitation et de maintenance sur site.

Il est reconnu que la technologie d'I&C évolue continuellement et qu'il n'est pas possible pour une norme telle que celle-ci de faire référence aux technologies et techniques de conception modernes. Afin d'assurer la pertinence de la présente norme pour les années à venir, l'accent est mis sur les questions de principe plutôt que sur des technologies particulières. Si de nouvelles techniques de conception sont développées alors il est possible d'évaluer l'aptitude de telles techniques à être employées en adaptant et en appliquant les principes de conception contenus dans la présente norme.

Le domaine d'application de la présente norme couvre le matériel des systèmes d'I&C pour toutes les classes de systèmes importants pour la sûreté. Ceci comprend des équipements câblés conventionnels, des équipements numériques programmables ou une combinaison de ces deux types d'équipements; il couvre l'évaluation et l'utilisation des constituants prédéveloppés, par exemple des constituants commercialement disponibles sur étagère (COTS) et le développement de nouveaux matériels.

La présente norme ne traite pas explicitement de la protection des systèmes contre les menaces liées à des attaques malveillantes des éléments numériques programmables, c'est-à-dire la cybersécurité. L'IEC 62645 définit les exigences relatives aux programmes de sécurité pour les éléments numériques programmables, pour toutes leurs phases de développement et leur fonctionnement sur site.

d) Description de la structure de la série de 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 haut niveau de la série de normes du SC 45A de l'IEC sont l'IEC 61513 et l'IEC 63046. L'IEC 61513 traite des exigences générales relatives aux systèmes et équipements d'I&C utilisés pour accomplir les fonctions importantes pour la sûreté des centrales nucléaires. L'IEC 63046 traite des exigences générales relatives aux systèmes d'alimentation électrique des centrales nucléaires; elle couvre les systèmes d'alimentation électrique jusqu'à et y compris les alimentations des systèmes d'I&C. L'IEC 61513 et l'IEC 63046 doivent être prises en considération conjointement et au même niveau. L'IEC 61513 et l'IEC 63046 structurent la série de normes du SC 45A de l'IEC et forment un cadre complet établissant des exigences générales pour l'instrumentation, le contrôle et les systèmes électriques des centrales nucléaires.

L'IEC 61513 et l'IEC 63046 renvoient directement à d'autres normes du SC 45A de l'IEC pour les sujets généraux liés à la catégorisation des fonctions et à la classification des systèmes, la qualification, la séparation, la défense contre les défaillances de cause commune, la conception des salles de contrôle, la compatibilité électromagnétique, la cybersécurité, les aspects logiciels et matériels des systèmes numériques programmables, 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 l'IEC 61513 et l'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 l'IEC 61513 ou l'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.

La série de normes du SC 45A de l'IEC met en œuvre et détaille de manière cohérente les principes et les aspects fondamentaux de la sûreté et de la sécurité fournis dans les normes de sûreté de l'AIEA et dans les documents pertinents de la collection Sécurité nucléaire de l'AIEA. Il s'agit en particulier du document d'exigences SSR-2/1 qui établit les exigences de sûreté liées à la conception des centrales nucléaires, du guide de sûreté SSG-30 qui traite de la classification de sûreté des structures, systèmes et composants des centrales nucléaires, du guide de sûreté SSG-39 qui traite de la conception des systèmes d'instrumentation et de contrôle des centrales nucléaires, du guide de sûreté SSG-34 qui traite de la conception des systèmes d'alimentation électrique des centrales nucléaires et du guide d'application NSS17 pour la sécurité informatique dans 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.

L'IEC 61513 et l'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, l'IEC 61513 et l'IEC 63046 sont l'interprétation des exigences générales de l'IEC 61508-1, 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. L'IEC 61513 et l'IEC 63046 font référence aux normes ISO ainsi qu'aux documents AIEA GSR partie 2 et AIEA GS-G-3.1 et AIEA GS-G-3.5 pour ce qui concerne l'assurance qualité. Au second niveau, l'IEC 62645 est le document chapeau du SC 45A de l'IEC portant sur la sécurité nucléaire. Elle est élaborée à partir des principes de haut niveau et des concepts principaux des normes de sécurité génériques, en particulier 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 série de normes IEC 62443. Au second niveau, l'IEC 60964 est le document chapeau des normes du SC 45A de l'IEC portant sur les salles de commande et l'IEC 62342 est le document chapeau des normes du SC 45A de l'IEC portant sur la gestion du vieillissement.

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

CENTRALES NUCLÉAIRES DE PUISSANCE – SYSTÈMES D'INSTRUMENTATION ET DE CONTRÔLE-COMMANDE IMPORTANTS POUR LA SÛRETÉ – EXIGENCES APPLICABLES AU MATÉRIEL

1 Domaine d'application

Les systèmes d'I&C importants pour la sûreté peuvent être mis en œuvre en utilisant des équipements câblés conventionnels, des équipements numériques programmables ou une combinaison de ces deux types d'équipements.

Le présent document fournit des exigences et des recommandations pour les aspects matériels des systèmes d'I&C, quelle que soit la technologie, et s'applique à toutes les classes de sûreté de manière graduelle (comme cela est défini par l'IEC 61513).

Les exigences définies dans le présent document guident en particulier la sélection des composants préexistants, les aspects matériels de la conception détaillée et de la mise en œuvre du système et la fabrication des équipements.

Le présent document ne traite pas explicitement de la protection des systèmes contre les menaces liées à des attaques malveillantes des éléments numériques programmables, c'est-à-dire la cybersécurité. L'IEC 62645 définit les exigences relatives aux programmes de sécurité pour les éléments numériques programmables, pour toutes leurs phases de développement et leur fonctionnement sur site.

Les constituants prédéveloppés peuvent contenir des microcontrôleurs ou des HPD et, lorsque les microprogrammes ou des fichiers de programmation sont profondément intégrés, être entièrement "transparents" pour l'utilisateur. Dans ce cas, le présent document peut être utilisé comme guide pour le processus d'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 appliquant le présent document.

Un logiciel qui n'est pas profondément intégré comme cela est décrit ci-dessus est développé ou évalué conformément aux exigences des normes logiciel applicables (par exemple l'IEC 60880 pour les systèmes de classe 1 ou l'IEC 62138 pour les systèmes de classe 2 et 3).

De la même manière, les HPD qui ne sont pas profondément intégrés comme cela est décrit ci-dessus, sont développés ou évalués conformément aux exigences des normes HPD applicables (par exemple l'IEC 62566 pour les systèmes de classe 1 ou l'IEC 62566-2 pour les systèmes de classe 2 et 3).

2 Références normatives

Les documents suivants sont cités dans le texte de sorte qu'ils 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/IEEE 60780-323, *Installations nucléaires – Équipements électriques importants pour la sûreté – Qualification*

IEC 60812, *Analyse des modes de défaillance et de leurs effets (AMDE et AMDEC)*

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

IEC/IEEE 60980-344, *Installations nucléaires – Équipements importants pour la sécurité – Qualification sismique*

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

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

IEC 61513:2011, *Centrales nucléaires de puissance – Instrumentation et contrôle-commande importants pour la sûreté – Exigences générales pour les systèmes*

IEC 61709, *Composants électriques – Fiabilité – Conditions de référence pour les taux de défaillance et modèles de contraintes pour la conversion*

IEC 62003, *Centrales nucléaires de puissance – Systèmes d'instrumentation, de contrôle-commande et d'alimentation électrique – Exigences relatives aux essais de compatibilité électromagnétique*

IEC 62138:2018, *Centrales nucléaires de puissance – Systèmes d'instrumentation et de contrôle commande importants pour la sûreté – Aspects logiciels des systèmes informatisés réalisant des fonctions de catégorie B ou C*

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*

IEC 62566-2, *Centrales nucléaires de puissance – Instrumentation et contrôle commande importants pour la sûreté – Développement des circuits intégrés programmés en HDL – Partie 2: Circuits intégrés programmés en HDL pour les systèmes réalisant des fonctions de catégorie B ou C*

ISO 28590, *Règles d'échantillonnage pour les contrôles par attributs — Introduction au système d'échantillonnage pour les contrôles par attributs de l'ISO 2859*

IPC-A-610, *Acceptabilité des Assemblages Électroniques*