IEC 60987

Edition 3.0 2020-11

PRE-RELEASE VERSION (FDIS)

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

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 27.120.20

45A/1365/FDIS

FINAL DRAFT INTERNATIONAL STANDARD (FDIS)

PROJECT NUMBER:	
IEC 60987 ED3	
DATE OF CIRCULATION:	CLOSING DATE FOR VOTING:
2020-11-13	**2020-12-25**
SUPERSEDES DOCUMENTS:	
45A/1305/CDV, 45A/1338A/RVC	

IEC SC 45A : INSTRUMENTATION, CONTROL AND ELECTRICAL POWER SYSTEMS OF NUCLEAR FACILITIES	
SECRETARIAT:	SECRETARY:
France	Mr Jean-Paul Bouard
OF INTEREST TO THE FOLLOWING COMMITTEES:	HORIZONTAL STANDARD:
	☐
FUNCTIONS CONCERNED:	
☐ EMC ☐ ENVIRONMENT	☐ QUALITY ASSURANCE ☒ SAFETY
☐ SUBMITTED FOR CENELEC PARALLEL VOTING	☒ NOT SUBMITTED FOR CENELEC PARALLEL VOTING

This document is a draft distributed for approval. It may not be referred to as an International Standard until published as such.

In addition to their evaluation as being acceptable for industrial, technological, commercial and user purposes, Final Draft International Standards may on occasion have to be considered in the light of their potential to become standards to which reference may be made in national regulations.

Recipients of this document are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

TITLE:

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

PROPOSED STABILITY DATE: 2025

NOTE FROM TC/SC OFFICERS:

CONTENTS

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/XX/FDIS	45A/XX/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*