

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**



THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2021 IEC, Geneva, Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester. If you have any questions about IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

Droits de reproduction réservés. Sauf indication contraire, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et les microfilms, sans l'accord écrit de l'IEC ou du Comité national de l'IEC du pays du demandeur. Si vous avez des questions sur le copyright de l'IEC ou si vous désirez obtenir des droits supplémentaires sur cette publication, utilisez les coordonnées ci-après ou contactez le Comité national de l'IEC de votre pays de résidence.

IEC Central Office
3, rue de Varembe
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
info@iec.ch
www.iec.ch

About the IEC

The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications

The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigendum or an amendment might have been published.

IEC publications search - webstore.iec.ch/advsearchform

The advanced search enables to find IEC publications by a variety of criteria (reference number, text, technical committee, ...). It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished

Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and once a month by email.

IEC Customer Service Centre - webstore.iec.ch/csc

If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: sales@iec.ch.

IEC online collection - oc.iec.ch

Discover our powerful search engine and read freely all the publications previews. With a subscription you will always have access to up to date content tailored to your needs.

Electropedia - www.electropedia.org

The world's leading online dictionary on electrotechnology, containing more than 22 000 terminological entries in English and French, with equivalent terms in 18 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

A propos de l'IEC

La Commission Electrotechnique Internationale (IEC) est la première organisation mondiale qui élabore et publie des Normes internationales pour tout ce qui a trait à l'électricité, à l'électronique et aux technologies apparentées.

A propos des publications IEC

Le contenu technique des publications IEC est constamment revu. Veuillez vous assurer que vous possédez l'édition la plus récente, un corrigendum ou amendement peut avoir été publié.

Recherche de publications IEC - webstore.iec.ch/advsearchform

La recherche avancée permet de trouver des publications IEC en utilisant différents critères (numéro de référence, texte, comité d'études, ...). Elle donne aussi des informations sur les projets et les publications remplacées ou retirées.

IEC Just Published - webstore.iec.ch/justpublished

Restez informé sur les nouvelles publications IEC. Just Published détaille les nouvelles publications parues. Disponible en ligne et une fois par mois par email.

Service Clients - webstore.iec.ch/csc

Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions contactez-nous: sales@iec.ch.

IEC online collection - oc.iec.ch

Découvrez notre puissant moteur de recherche et consultez gratuitement tous les aperçus des publications. Avec un abonnement, vous aurez toujours accès à un contenu à jour adapté à vos besoins.

Electropedia - www.electropedia.org

Le premier dictionnaire d'électrotechnologie en ligne au monde, avec plus de 22 000 articles terminologiques en anglais et en français, ainsi que les termes équivalents dans 16 langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (IEV) en ligne.

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.**

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*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- IEC Electropedia: available at <http://www.electropedia.org/>
- ISO Online browsing platform: available at <http://www.iso.org/obp>

3.1

class of an I&C system

one of three possible assignments (1, 2, 3) of I&C systems important to safety resulting from consideration of their requirement to implement I&C functions of different safety importance

Note 1 to entry: An unclassified assignment is made if the I&C system does not implement functions important to safety.

Note 2 to entry: See also "category of an I&C function", "items important to safety", "safety systems".

[SOURCE: IEC 61513:2011, 3.6, modified – last sentence of definition turned into Note 1 to entry.]

3.2

common cause failure, CCF

failure of two or more structures, systems or components due to a single specific event or cause

Note 1 to entry: Common causes can be internal or external to an I&C system.

[SOURCE: IAEA Safety Glossary: 2018, modified – Note 1 to entry has been added.]

3.3

component

one of the parts that make up a system

Note 1 to entry: A component can be hardware, software or HPD and can be subdivided into other components.

Note 2 to entry: See also "I&C system", "equipment".

Note 3 to entry: The terms "equipment", "component", and "module" are often used interchangeably. The relationship of these terms is not yet standardised.

Note 4 to entry: This IEC SC 45A definition is in principle compatible with the sub-definition of "Component" given in the frame of the 2018 edition of the IAEA Safety Glossary definition of "Structures Systems and Components (SSC)". Nevertheless, as only examples of hardware components are given, this can mislead the reader and IEC SC 45A prefer to use a definition which explicitly covers software components.

[SOURCE: IEC 61513:2011, 3.10, modified – last sentence of definition turned into Note 1 to entry and edition 2007 of IAEA Safety Glossary has been updated to edition 2018.]

3.4

computer-based item

item that relies on software instructions running on microprocessors or microcontrollers

Note 1 to entry: In this term and its definition, the term item can be replaced by the terms: system, or equipment, or device.

Note 2 to entry: A computer-based item is a kind of programmable digital item.

Note 3 to entry: This term is equivalent to software-based item.

Note 4 to entry: The definitions for the following terms: E/E/PE item, Electrical item, I&C systems, Programmable digital item, Computer-based item, Hardwired item, Programmable Logic Device, HPDs have to be considered in conjunction and are totally consistent and coherent. They are totally consistent and coherent with the general requirements established by IEC 61513 and IEC 63046 for instrumentation, control and electrical systems for nuclear power plants.

[SOURCE: IEC 62138:2018, 3.8, modified – Note 4 to entry has been added.]

3.5

electrical / electronic / programmable electronic item

E/E/PE item

item based on electrical (E) and/or electronic (E) and/or programmable electronic (PE) technology

Note 1 to entry: In this term and its definition, the word "item" can be replaced by the words: system, or equipment, or device.

Note 2 to entry: The definitions for the following terms: E/E/PE item, Electrical item, I&C systems, Programmable digital item, Computer-based item, Hardwired item, Programmable Logic Device, HDL Programmed Device (HDL Hardware Description Language), have to be considered in conjunction and are totally consistent and coherent. They are totally consistent and coherent with the general requirements established by IEC 61513 and IEC 63046 for instrumentation, control and electrical systems for nuclear power plants.

[SOURCE: IEC 62138:2018, 3.15, modified – Note 2 to entry has been added.]

3.6 electrical power system

EPS

system performing electrical power generation, transmission and distribution; performing supply functions to operate plant equipment (pumps, valves, heaters, etc.)

Note 1 to entry: An electrical system can integrate E/E/PE items to perform its internal electrical control and protection.

[SOURCE: IEC 63046:2020, 3.12]

3.7 equipment

one or more parts of a system

Note 1 to entry: An item of equipment is a single definable (and usually removable) element or part of a system.

Note 2 to entry: See also "component", "I&C system".

Note 3 to entry: Equipment may include software.

Note 4 to entry: The terms "equipment", "component", and "module" are often used interchangeably. The relationship of these terms is not yet standardised.

[SOURCE: IEC 61513:2011, 3.16, modified – last sentence of definition turned into Note 1 to entry and Note 4 to entry of IEC 61513 has been removed.]

3.8 firmware

software which is closely coupled to the hardware characteristics on which it is installed

Note 1 to entry: The presence of firmware is generally "transparent" to the user of the hardware component and, as such, can be considered to be effectively an integral part of the hardware design (a good example of such software being processor microcode).

Note 2 to entry: Generally, firmware can only be modified by a user by replacing the hardware components (for example, processor chip, card, EPROM) which contain this software with components which contain modified software (firmware). Where this is the case, configuration control of the hardware components by the users of the equipment effectively provides configuration control of the firmware. Firmware, as considered by this document, is effectively software that is built into the hardware

3.9 function

specific purpose or objective to be accomplished, that can be specified or described without reference to the physical means of achieving it

[SOURCE: IAEA Safety Glossary, 2018]

3.10 hardwired item

item that relies on relays, on analogue electronic or on discrete digital logic

Note 1 to entry: In this term and its definition, the term item can be replaced by the terms: system, or equipment, or device.

Note 2 to entry: This term used by IEC SC 45A is roughly equivalent to electronic item used by IEC 61508. Relays are electro-mechanical items, not electronic items, but they are included in the term hardwired-based item.

Note 3 to entry: Hardwired item are also usually called conventional items.

Note 4 to entry: The definitions for the following terms: E/E/PE item, Electrical item, I&C systems, Programmable digital item, Computer-based item, Hardwired item, Programmable Logic Device, HDL Programmed Device (HDL Hardware Description Language), have to be considered in conjunction and are totally consistent and coherent. They are totally consistent and coherent with the general requirements established by IEC 61513 and IEC 63046 for instrumentation, control and electrical systems for nuclear power plants.

3.11**Hardware Description Language****HDL**

language used to formally describe the functions and/or the structure of an electronic component for documentation, simulation or synthesis

Note 1 to entry: The most widely used HDLs are VHDL (IEEE 1076) and Verilog (IEEE 1364).

[SOURCE: IEC 62566:2012, 3.6]

3.12**HDL-Programmed Device****HPD**

integrated circuit configured with Hardware Description Languages and related software tools

Note 1 to entry: HDLs and related tools (e.g. simulator, synthesizer) are used to implement the requirements in a proper assembly of pre-developed micro-electronic resources.

Note 2 to entry: The development of HPDs can use Pre-Developed Blocks.

Note 3 to entry: HPDs are typically based on blank FPGAs, PLDs or similar micro-electronic technologies.

Note 4 to entry: HPD is a kind of programmable digital item.

Note 5 to entry: The definitions for the following terms: E/E/PE item, Electrical item, I&C systems, Programmable digital item, Computer-based item, Hardwired item, Programmable Logic Device, HDL Programmed Device (HDL Hardware Description Language), have to be considered in conjunction and are totally consistent and coherent. They are totally consistent and coherent with the general requirements established by IEC 61513 and IEC 63046 for instrumentation, control and electrical systems for nuclear power plants.

[SOURCE: IEC 62566:2012, 3.7, modified – Note 4 to entry and Note 5 to entry added.]

3.13**I&C system**

system, based on electrical and/or electronic and/or programmable electronic technology, performing I&C functions as well as service and monitoring functions related to the operation of the system itself

Note 1 to entry: The term is used as a general term which encompasses all elements of the system such as internal power supplies, sensors and other input devices, data highways and other communication paths, interfaces to actuators and other output devices. The different functions within a system may use dedicated or shared resources.

Note 2 to entry: See also "system, I&C function".

Note 3 to entry: The elements included in a specific I&C system are defined in the specification of the boundaries of the system.

Note 4 to entry: According to their typical functionality, IAEA distinguishes between automation / control systems, HMI systems, interlock systems and protection systems.

[SOURCE: IEC 61513:2011, 3.29, modified – last sentence of definition turned into Note 1 to entry.]

3.14**integration**

progressive aggregation and verification of components into a complete system

[SOURCE: IEC 62138:2018, 3.27]

3.15

periodic testing

performance of tests at predetermined time points to demonstrate that the functional capabilities of I&C systems and equipment important to safety are retained and that the characteristics relevant to the claims of the safety analysis are satisfied

[SOURCE: IEC 60671:2007, 3.7]

3.16

pre-existing items

hardware, hardwired or programmable digital items that already exist as a commercial or proprietary product, and are being considered for use

Note 1 to entry: This definition includes that of pre-developed software or HDL, see IEC 60880, IEC 62138, IEC 62566 and IEC 62566-2.

Note 2 to entry: Pre-existing items can be commercial off-the-shelf (also called "COTS") or proprietary products internally utilised by a manufacturer (see IEC 61513:2011, 6.2.3.2).

[SOURCE: IEC 61513:2011, 3.36, modified – definition and Notes to entry changed to address Electrical, Electronic, Programmable Electronic items and COTS.]

3.17

programmable digital item

item that relies on software instructions or programmable logic to accomplish a function

Note 1 to entry: In this term and its definition, the term item can be replaced by the terms: system or equipment or device.

Note 2 to entry: The main kinds of programmable digital items are computer-based items and programmable logic items.

Note 3 to entry: This term used by IEC SC 45A is equivalent to programmable electronic item (PE item) defined according to IEC 61508.

Note 4 to entry: The definitions for the following terms: E/E/PE item, Electrical item, I&C systems, Programmable digital item, Computer-based item, Hardwired item, Programmable Logic Device, HDL Programmed Device (HDL Hardware Description Language), have to be considered in conjunction and are totally consistent and coherent. They are totally consistent and coherent with the general requirements established by IEC 61513, IEC 60880, IEC 62138, IEC 62566 and IEC 62566-2 for instrumentation, control and electrical systems for nuclear power plants.

[SOURCE: IEC 62138:2018, 3.34, modified – Note 4 to entry has been added.]

3.18

Programmable Logic item

item that relies on logic components with an integrated circuit that consists of logic elements with an inter-connection pattern, parts of which are user programmable

Note 1 to entry: In this term and its definition, the term item can be replaced by the terms: system, or equipment, or device.

Note 2 to entry: A programmable logic item is a kind of programmable digital item.

Note 3 to entry: See also the definition of E/E/PE item and the associated notes.

[SOURCE: IEC 62138:2018, 3.35]

3.19

qualification

process of determining whether a system or component is suitable for operational use. The qualification is performed in the context of a specific class of the I&C system and a specific set of qualification requirements

Note 1 to entry: The qualification requirements are derived from the specific class of the I&C system and a specific application context.

Note 2 to entry: I&C systems are typically implemented on the basis of interacting sets of equipment. Such equipment may be developed as part of the project, or it may be pre-existing equipment. Typically, qualification of an "I&C system" is accomplished in stages: first by the qualification of individual pre-existing equipment (usually early in the system realization process); in a second step by the qualification of the integrated I&C system (i.e. the final realized design).

Note 3 to entry: Qualification of I&C systems is always a plant- and application-specific activity. However, it may rely to a large degree on qualification activities performed outside the framework of a specific plant design (these are called "generic qualification" or "pre-qualification"). Pre-qualification may reduce the plant-specific qualification effort significantly, however, the application-specific qualification requirements need to be demonstrated.

[SOURCE: IEC 61513:2011, 3.38, modified – embedded definition of Pre-existing equipment has been removed in Note 2 to entry and last sentence of Note 3 corrected.]

3.20

random fault

non-systematic fault of hardware components

Note 1 to entry: Faults of hardware components are a consequence of physical or chemical effects, which can occur at any time. A good description of the probability of the occurrence of random faults can be given using statistics (fault rate). Increased fault rates can be the consequence of systematic faults in hardware design or manufacture, if these occur without temporal correlation, for example as a consequence of premature ageing.

[SOURCE: IEC 62340:2007, 3.15]

3.21

safety function

specific purpose that must be accomplished for safety for a facility or activity to prevent or to mitigate radiological consequences of normal operation, anticipated operational occurrences and accident conditions

Note 1 to entry: Safety functions are required to fulfil the fundamental safety functions that are (i) control of reactivity, (ii) removal of heat from the reactor and from the fuel store, (iii) confinement of radioactive material, shielding against radiation and control of planned radioactive releases, as well as limitation of accidental radioactive releases [IAEA SSR-2/1, Requirement 4].

Note 2 to entry: Safety functions are primarily those that are credited in the safety analysis and include functions performed at all levels of defence in depth.

[SOURCE: IAEA Safety Glossary, 2018]

3.22

system

set of components which interact according to a design, where an element of a system can be another system, called a subsystem

Note 1 to entry: See also "I&C system".

Note 2 to entry: I&C systems are distinguished from mechanical systems and electrical systems of the NPP.

Note 3 to entry: This IEC SC 45A definition is totally compatible with the sub-definition of "system" given in the frame of the 2018 edition of the IAEA Safety Glossary definition of "Structures Systems and Components (SCC)".

[SOURCE: IEC 61513:2011, 3.56, modified – In Note 3 to entry, edition 2007 of IAEA Safety Glossary definition has been updated to edition 2018.]

3.23

system validation

confirmation by examination and provision of other evidence that a system fulfils in its entirety the requirement specification as intended (functionality, response time, fault tolerance, robustness)

[SOURCE: IEC 61513:2011, 3.59]

3.24

systematic fault

fault in the hardware or software which concerns systematically some or all components of a specific type

Note 1 to entry: Systematic faults may result from errors in the specification or design, from manufacturing defects or from errors which are introduced during maintenance activities.

Note 2 to entry: Components containing a systematic latent fault may fail randomly or coincidentally, depending on the kind of fault and the related mechanisms that trigger the fault.

[SOURCE: IEC 62340:2007, 3.24]

3.25

unrevealed hardware failure

hardware failure which is not detected by a system automatically and which only becomes apparent when an attempt is made to use a function which depends upon the failed hardware

Note 1 to entry: Such failures can be discovered by functional testing or when an operational demand is placed upon the system.

3.26

verification

confirmation by examination and by provision of objective evidence that the results of an activity meet the objectives and requirements defined for this activity

Note 1 to entry: The 2018 edition of the IAEA Safety Glossary gives the two following definitions:

Validation: The process of determining whether a product or service is adequate to perform its intended function satisfactorily. Validation (typically of a system) concerns checking against the specification of requirements, whereas verification (typically of a design specification, a test specification or a test report) relates to the outcome of a process. Validation may involve a greater element of judgment than verification.

Verification: The process of determining whether the quality or performance of a product or service is as stated, as intended or as required. Verification is closely related to quality management and quality control.

The IAEA definition of "verification" is very similar to the IAEA one of « validation », as both address the final product or service.

In IEC SC 45A standards, the terms "verification" and "validation" refer to the result of the lifecycle of specific products, namely I&C equipment and systems, but not to services in general.

Furthermore, "verification" and "validation" are used to identify two different and complementary types of assessments:

"Verification" indicates the assessment of the results of an individual activity against its inputs.

"Validation" indicates the assessment of the final product against its documented objectives and requirements.

[SOURCE: IEC 61513:2011, 3.62, modified –in Note 1 to entry, edition 2007 of IAEA Safety Glossary definition has been updated to edition 2018 and the content of the note adapted consistently.]

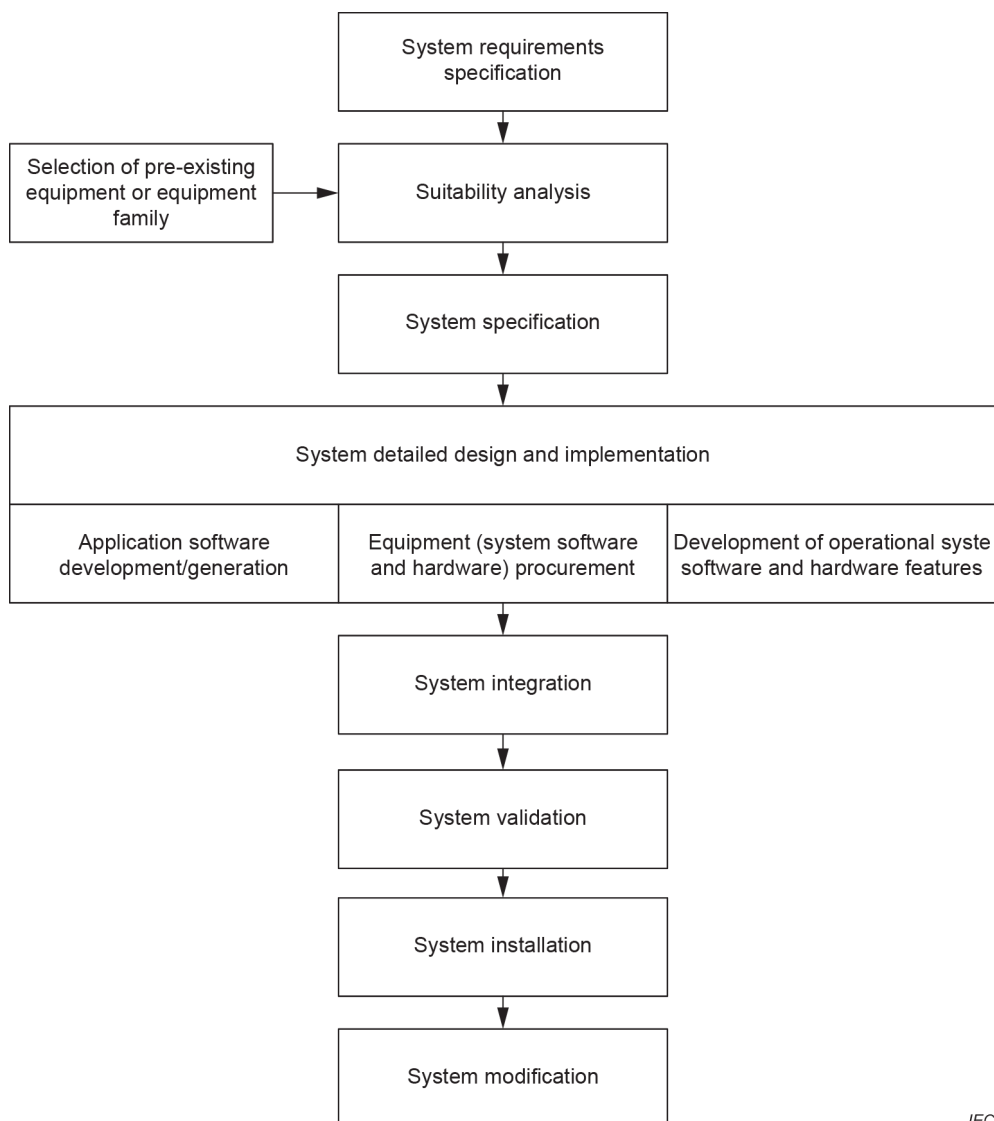
4 Symbols and abbreviated terms

ATE	Automated Test Equipment
BOM	Bill Of Materials
COTS	Commercial Off The Shelf
FMEA	Failure Modes and Effects Analysis
FMECA	Failure Mode Effects and Criticality Analysis
FPGA	Field Programmable Gate Array
FTA	Fault Tree Analysis
HDL	Hardware Description Languages
HPD	HDL-Programmed Device
ISA	International Society of Automation
NEMA	National Electrical Manufacturers Association
NPP	Nuclear Power Plant
OMM	Operation and Maintenance Manual

5 Hardware safety lifecycle

5.1 General

The process of producing I&C systems for use in nuclear power plants is given in IEC 61513 which introduces the concept of system safety lifecycle. This is a vehicle by which the development process can be controlled and whose adoption also results in evidence necessary to justify the correct operation of systems important to safety. It includes and places requirements on, but does not dictate the project arrangements to be used for the production of systems (see Figure 1).



IEC

Figure 1 – System safety lifecycle (informative, as defined by IEC 61513)

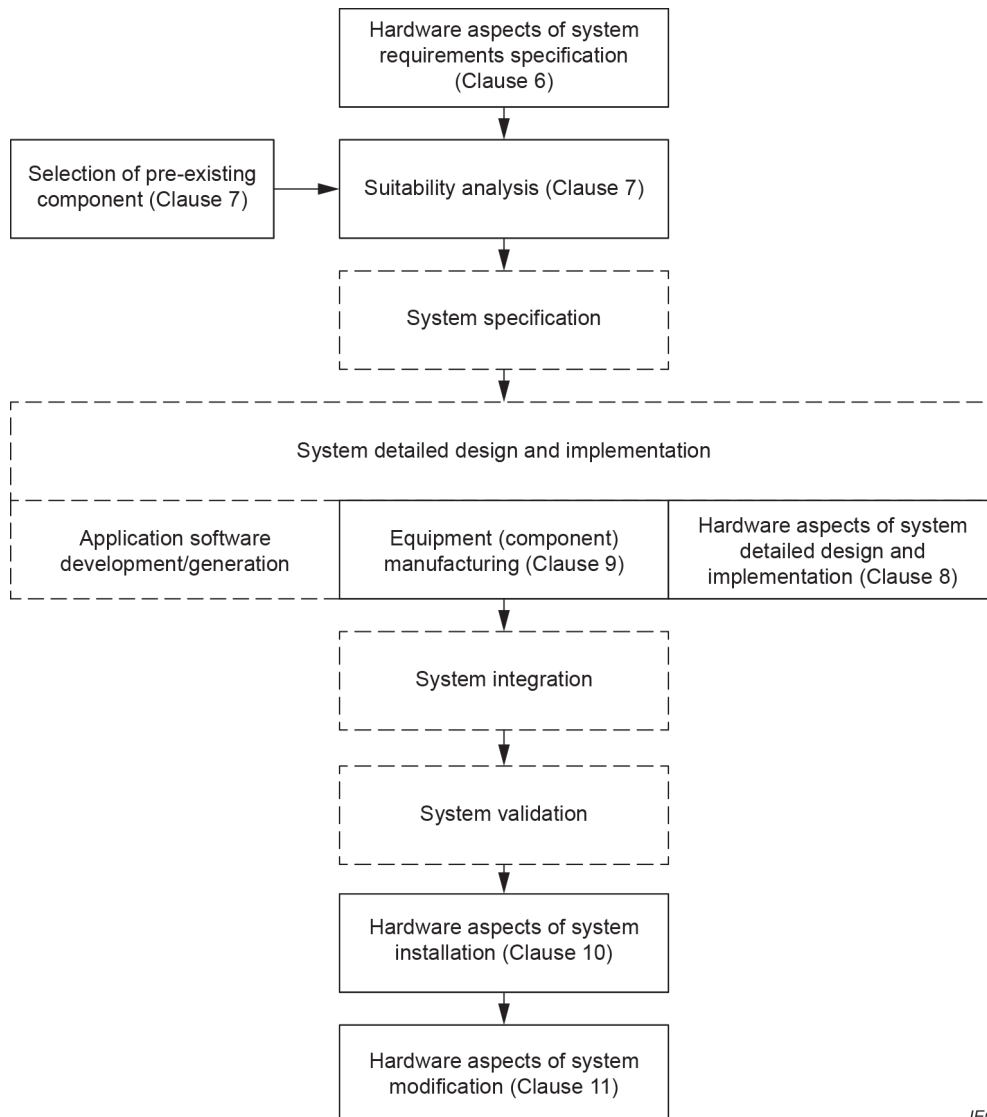
The system safety lifecycle of IEC 61513 is completed in IEC 60880 (for category A functions) and IEC 62138 (for category B and C functions) for software development, by IEC 62566 (for category A functions) and IEC 62566-2 (for category B and C functions) for HPD development and in IEC 60987 for hardware development of class 1, 2 and 3 I&C systems.

I&C equipment, including hardware components, are developed according to a cycle that includes development activities dedicated to requirements specification, design and implementation, qualification, manufacturing, integration and validation, together with quality assurance and verification activities.

In most cases, I&C suppliers use pre-existing components and the hardware safety lifecycle is strongly integrated within the system safety lifecycle. In particular, the hardware requirements specification is a part of, or is derived directly from, system requirements specification and system design.

If needed, development of specific new components may be done in parallel of the plant specific application. In such cases, development and qualification are run in advance or with some overlaps with the project.

Figure 2 illustrates the relationship between the activities of the hardware safety lifecycle and the activities of the system safety lifecycle.



NOTE Boxes in thin dotted lines represent system activities not addressed in this document.

Figure 2 – Hardware related activities in the system safety lifecycle

The following additional planning activities not represented in Figure 2 also support the hardware safety lifecycle:

- quality assurance;
- verification;
- configuration management.

Operation and maintenance which are not represented in Figure 2 are also addressed in this document.

The qualification to environmental conditions is not represented in Figure 2 and is not addressed by this document. I&C systems have to be tested and qualified for their environmental conditions in accordance with the applicable requirements of IEC/IEEE 60780-323 supplemented by IEC/IEEE 60980-344 when the I&C system needs to be seismic resistant.

The degree of immunity to electromagnetic interference needs to be specified as required by the operational environment and IEC 62003. The electromagnetic requirements need to be in accordance with realistic estimates of the operational conditions under all credible worst-case circumstances.

The degree of immunity to electromagnetic interference needs to be tested according to applicable IEC 61000 series standards.

5.2 Hardware safety lifecycle for class 1 and class 2

5.2.1 Project structure for class 1 and class 2

5.2.1.1 The hardware safety lifecycle shall be compatible with the whole system safety lifecycle.

The development project of a new module can be a standalone project and managed separately from the I&C equipment development where it is intended to be integrated. Nowadays this is a typical situation where most of the modules integrated in the I&C system are pre-existing modules as part of a generic equipment family provided by I&C suppliers.

5.2.1.2 Each phase of the hardware safety lifecycle shall consist of well-defined and documented activities.

5.2.1.3 Each phase should be to some extent self-contained but will depend on other phases for inputs and will, in turn, provide outputs for other phases.

NOTE The various project phases together are considered to form the overall safety lifecycle (see IEC 61513:2011, Clause 5, which provides requirements for system safety lifecycles). IEC 61513 allows project phases to be performed in parallel provided the integrity of the system safety lifecycle is not compromised.

5.2.1.4 Each phase shall include the production of documentation for commencing the next phase of development including any assumptions or limitations to be applied to the I&C equipment.

5.2.1.5 Each phase shall be concluded by performing verification (see 5.2.3).

5.2.1.6 All activities shall be scheduled to ensure that adequate time is allowed for:

- interactions between the hardware and HPD or software development phases required to ensure system hardware/software/HPD compatibility;
- production of documentation, and the performance of testing, verification and quality assurance activities.

5.2.2 Quality management for class 1 and class 2

5.2.2.1 A quality assurance plan for hardware aspects shall exist either as a separate document (or documents) or as part of a system quality assurance plan.

5.2.2.2 All hardware quality-related activities to be performed as part of the hardware safety lifecycle should be included in the quality assurance plan.

5.2.2.3 The quality assurance plan shall require that adequate resources (e.g. human resources, budgets), adequate means (i.e. spare parts, devices for test and maintenance, etc.) and adequate working environments (i.e. laboratories, workshops, working space) are provided to carry out the tasks associated with each phase of the hardware safety lifecycle.

5.2.2.4 The quality assurance plan shall require that the implementation of each activity is assigned to competent persons.

5.2.2.5 The quality assurance plan shall address the following phases, as they are applicable to any particular system or development:

- hardware aspects of system requirements specification;
- selection of pre-existing components;
- hardware aspects of system detailed design and implementation;
- equipment (component) manufacturing;
- hardware aspects of system installation;
- hardware aspects of system modification.

5.2.2.6 The quality assurance plan(s) should describe the organization, management and execution of quality-related activities, including, as relevant:

- the design process;
- the control of the documentation configuration;
- the control of build instructions, build procedures and drawings;
- the procurement process for goods and services;
- the control of materials and items to be used to build the system hardware;
- the quality control activities, such as formal inspections;
- the control of test equipment and tools;
- the control of hardware handling/storage/shipping;
- the testing process;
- the monitoring of non-conformances and related corrective actions;
- the procedure for storing quality assurance records;
- the procedure for internal and external audits.

5.2.3 Verification of hardware for class 1 and class 2

5.2.3.1 General requirements for class 1 and class 2

The detailed design and implementation process shall include formal checks that the hardware design deliverables from each phase meet the requirements imposed by the previous phase.

NOTE The hardware verification process is generally considered to begin with the verification of the hardware requirements specification against the system requirements specification and is considered to be complete when the HPDs and the system software are integrated into the hardware. IEC 60880 and IEC 62138, IEC 62566 and IEC 62566-2 provide relevant requirements for the hardware/software/HPDs integration phases.

5.2.3.2 Verification plan for class 1 and class 2

5.2.3.2.1 A verification plan shall be prepared to define the approach to be used to verify the hardware design and to control the correct application of verification activities. The plan may be part of an overall verification plan.

5.2.3.2.2 The plan shall be prepared prior to initiating verification actions.

5.2.3.2.3 The plan (or plans) should document the personnel/organization to be used, organizational structure, verification methods to be used, level of verification to be performed, schedules and other significant project activities related to verification.

5.2.3.2.4 Verification actions shall take place only when design products (e.g. documents, components) are released for verification by the design personnel and when related documentation is recorded under a formal configuration control.

Informal pre-verification might be performed in parallel with the design process so that errors can be detected and corrected as soon as possible (providing the adequate configuration control arrangements are ensured).

5.2.3.2.5 After release for verification, the design change process shall ensure that all subsequent changes to the hardware design are adequately verified (i.e., as required by Clause 11).

5.2.3.3 Independence of verification for class 1 and class 2

5.2.3.3.1 The verification plan shall be developed and implemented by individuals who did not participate in the design.

5.2.3.3.2 For class 1, verification personnel should be managerially independent from the hardware designers; for example, they may be in different departments of the same organization or from a different organization.

5.2.3.3.3 The verification personnel shall be technically competent persons.

5.2.3.3.4 Verification shall be performed according to documented procedures.

5.2.3.3.5 Any verification findings and responses to those findings by the design team shall be formally documented.

5.2.3.3.6 For class 1 when an ATE is used and automatically executes tests, independence shall be assured between:

- the hardware designers and the test scenario developers;
- the hardware designers and the personnel responsible for carrying out the tests and evaluating the results of the tests.

5.2.3.3.7 For class 2, when an ATE is used and automatically executes tests, independence shall be assured between:

- the hardware designers and the test scenario developers;
- the hardware designers and the personnel evaluating the results of the tests.

5.2.3.4 Verification methods for class 1 and class 2

5.2.3.4.1 The basis for the choice of verification method(s) to be used shall be documented in sufficient detail to allow auditing by personnel who are not directly involved in the design or verification activities.

NOTE Typical examples of verifications methods are critical reviews, audits, analysis, manual tests or tests performed using ATE.

5.2.3.4.2 When choosing the appropriate verification method, the following issues shall be considered:

- the safety classification of the system (i.e. with class 1 requiring the most rigorous techniques);
- the documented reviews and tests which will be performed on the integrated hardware, software and HPDs as part of the system verification and validation processes, i.e. to eliminate such activities from the hardware verification and validation processes, so as not to inefficiently utilise resources by duplicating work;
- previous verification activities performed on the hardware or on systems containing the hardware (i.e. where equipment has been effectively pre-qualified);

- system design characteristics, for example, size, maturity/novelty of design principles used, failure modes and complexity;
- supporting data which may be available from other sources, such as those obtained from quality assurance and environmental qualification processes.

5.2.3.4.3 Tools and methods shall be available to support the testing of subsystems and components to ensure that they can be thoroughly tested.

5.2.3.4.4 ATE should be used to improve the repeatability and thoroughness of testing where effective.

5.2.3.4.5 Test instruments used in the verification or testing process shall be calibrated to confirm accuracy, where the test success criteria is dependent on the measured value, in which case procedures shall ensure that only calibrated instruments are used.

5.2.3.4.6 Software-based testing tools shall be validated prior to use and shall be placed under configuration control.

NOTE The validation of software-based testing tools is based on the user documentation and the adequacy with regards to the testing requirements.

5.2.3.4.7 The results of all formal testing shall be recorded (informal testing may be performed during the design process as a precursor to formal testing). Auditable records of formal testing shall be available and be sufficient to demonstrate that all tests have been performed, and that any test discrepancies have been successfully reconciled.

5.2.3.5 Verification documentation for class 1 and class 2

5.2.3.5.1 Auditable records related to verification activities shall include the verification plan, test procedures, test results, design change records and documentation of any discrepancies which are discovered during the hardware verification process (together with records showing how each discrepancy was reconciled).

5.2.3.5.2 Test procedures shall be clearly written, provide step-by-step instructions for hardware verification and shall contain detailed information of the test set-up.

5.2.3.5.3 Test procedures shall contain unambiguous pass/fail criteria.

5.2.3.5.4 When test procedures are implemented by software then the software version shall be included in the documentation.

5.2.3.6 Discrepancies management for class 1 and class 2

5.2.3.6.1 Discrepancies found during the verification process shall be formally documented and transmitted to the relevant personnel for resolution.

5.2.3.6.2 The response shall be formally documented to provide a traceable path to assure that all discrepancies are assessed and that any identified design deficiencies are corrected or accepted.

5.2.3.6.3 Where design deficiencies are accepted, all impacts on system documentation shall be fully addressed.

5.3 Hardware safety lifecycle for class 3

5.3.1 Project structure and quality management for class 3

5.3.1.1 The hardware safety lifecycle shall be compatible with the whole system safety lifecycle.

The development project of a new module can be a standalone project and managed separately from the I&C equipment development where it is intended to be integrated. Nowadays this is a typical situation where most of the modules integrated in the I&C system are pre-existing modules as part of a generic equipment family provided by I&C suppliers.

5.3.1.2 Each phase should be to some extent self-contained but will depend on other phases for inputs and will, in turn, provide outputs for other phases.

NOTE The various project phases together are considered to form the overall safety lifecycle (see IEC 61513:2011, Clause 6, which provides requirements for system safety lifecycles). IEC 61513 allows project phases to be performed in parallel providing the integrity of the system safety lifecycle is not compromised.

5.3.1.3 Each phase should include the production of documentation for commencing the next phase of development including any assumption or limitations to be applied to the I&C equipment.

5.3.1.4 A quality assurance plan for hardware aspects shall exist either as a separate document (or documents) or as part of a system quality assurance plan.

5.3.1.5 The quality assurance plan shall address the following phases, as they are applicable to any particular system or development:

- hardware aspects of system requirements specification;
- selection of pre-existing components;
- hardware aspects of system detailed design and implementation;
- equipment (component) manufacturing;
- hardware aspects of system installation;
- hardware aspects of system modification.

5.3.2 Verification of hardware for class 3

5.3.2.1 The design and implementation process shall include checks that the hardware design deliverables from each phase of design and implementation meet the requirements imposed by the previous phase.

NOTE The hardware verification process is generally considered to begin with the verification of the hardware requirements specification against the system requirements specification and is considered to be complete when the HPDs and the system software are integrated into the hardware. IEC 60880 and IEC 62138, IEC 62566 and IEC 62566-2 provide relevant requirements for the hardware/software/HPDs integration phases.

5.3.2.2 Discrepancies found during the verification process should be formally documented and transmitted to the relevant personnel for resolution.

5.3.2.3 Auditable records related to verification activities should include the verification plan, test procedures, test results, design change records and discrepancies resolution.

6 Hardware aspects of system requirements specification

6.1 Hardware aspects of system requirements specification for class 1 and class 2

6.1.1 General requirements for class 1 and class 2

6.1.1.1 The hardware requirements shall be specified in the hardware requirements specification or as part of a broader scope specification.

6.1.1.2 The hardware requirements shall be consistent with the system requirements specification (see IEC 61513:2011, Clause 6).

The system requirements specification is a description of the combined hardware and hardware/software/HPDs aspects and states the design objectives for the system and the functions to be performed by the system. The system may be entirely developed for a particular application or may be based on a generic equipment family assembled for a specific project application.

The hardware requirements specification identifies the hardware functions and required performance, identifies the hardware design requirements, states hardware reliability requirements, and states the hardware environmental conditions requirements.

6.1.1.3 Hardware requirements shall be presented according to techniques or methods whose format shall not preclude readability.

6.1.1.4 Hardware requirements shall be unambiguous, testable and/or verifiable and achievable.

6.1.1.5 The hardware requirements should generally specify what has to be done and not how it has to be done.

However, the use of pre-existing components may result in a degree of bottom-up hardware design.

6.1.2 Functional and performance requirements for class 1 and class 2

6.1.2.1 The hardware functional and performance requirements shall be consistent with the functional and performance requirements of the system.

6.1.2.2 The hardware functional and performance requirements, combined with the hardwired item requirements or the programmable digital item requirements (to the extent necessary to address all hardware requirements), shall be verified for compliance with the system requirements.

6.1.2.3 The hardware functional requirements shall include, but are not restricted to, the definition of:

- the purpose of the overall system hardware and of each of the hardware sub-assemblies;
- the numbers and types of sensors and actuators to be connected to the system;
- the numbers and types of devices for the man/machine interface such as displays, printers and keyboards.

6.1.2.4 Each component or subsystem delivered by a supplier, and which is to be integrated into the system, shall either:

- be accompanied by a specification which addresses all safety aspects of the performance of that item; or
- be accompanied by an analysis that determines the hardware design characteristics of the component to the extent necessary to confirm its suitability.

6.1.2.5 The hardware performance requirements shall include (as applicable to any particular application):

- required data acquisition rate;
- required data handling capability;
- required computational capacity;
- required communications interfaces (protocols, transmission speeds);
- required computational and conversion accuracy;

- required signal noise rejection capability;
- required response times;
- physical size limitations;
- geographic requirements (for example, length of data transmission lines);
- required level of spare capacity (if required);
- environmental operating conditions;
- electrical power supply requirements.

6.1.2.6 The constraints on hardware interfaces with other systems shall be specified in the hardware requirements specification or in a broader scope document.

IEC 61513:2011, 6.2.2.3.2, 6.2.2.4, 6.2.2.5, 6.2.3.3.3 and 6.2.3.3.4 provide system interface requirements which aim to guarantee the correct integration and to prevent the propagation of failures across system interfaces.

6.1.2.7 Any constraints imposed upon the hardware design by the system or software/HPD design shall be stated.

6.1.3 Reliability requirements for class 1 and class 2

6.1.3.1 The hardware reliability requirements shall be defined and they shall be consistent with the overall reliability requirements of the system.

NOTE Hardware reliability in this context is concerned with random faults and excludes any consideration of systematic faults.

6.1.3.2 The hardware reliability/availability requirements should include a description of the types of failure which have to be tolerated without loss, or with a defined limited loss, of functions.

6.1.3.3 The hardware requirements should give target figures for the hardware reliability parameters, such as mean time between failures (revealed), mean time between failures (unrevealed), mean time to repair (for revealed failures).

6.1.3.4 Any requirement for reliability claims to be supported with detailed analysis of the hardware design should be stated, for example, sub-assembly, module or component-level analysis.

6.1.3.5 Maintenance requirements shall be defined to ensure the required reliability over the lifetime of the I&C system.

6.1.3.6 Maintenance requirements shall address (as applicable to any particular system):

- requirements for system operation during hardware maintenance activities;
- consumable replacement, for example, air filters, batteries;
- any requirements for the regular replacement of subsystems, modules and/or components;
- any requirements to perform periodic testing including periodicity;
- measures to prevent maintenance errors potentially leading to CCF;
- the extent of system revalidation (for example, testing) required following hardware maintenance activities.

6.1.3.7 Maintenance requirements should be defined during the hardware requirements specification, and if they cannot be defined in details during that phase, they should be finalised at a later stage, prior to the system installation.

6.1.4 Environmental conditions requirements for class 1 and class 2

6.1.4.1 The hardware environmental condition requirements shall identify the constraints the I&C system may undergo and address the related physical levels to take into account when applicable.

NOTE Typical constraints are climatic, ageing, seismic, chemical, electrical, EMC and radiation conditions.

6.1.4.2 The normal and extreme ranges of environmental conditions that the system is required to withstand shall be specified in accordance with the constraints imposed from the plant design framework (see IEC 61513:2011, 5.2.4).

6.1.4.3 Any particular requirements applicable during storage, installation and commissioning should be included.

6.1.5 Manufacturing requirements for class 1 and class 2

The hardware requirements shall identify, in particular:

- Any prohibited construction materials and any requirements for particular materials to be used;
- Particular types of manufacturing processes;
- Minimum IPC-A-610 acceptability criteria (see 9.1.6.4).

6.1.6 Documentation requirements for class 1 and class 2

The hardware documentation requirements shall be specified as part of the documentation requirements of the I&C system (see IEC 61513).

Annex A identifies typical documentation for each of the main clauses of this document.

6.2 Hardware aspects of system requirements specification for class 3

6.2.1 General requirements for class 3

6.2.1.1 The hardware requirements shall be specified in the hardware requirements specification or as part of a broader scope specification.

6.2.1.2 It shall be ensured that the hardware requirements specification meet the requirements expressed in the system requirements specification in terms of:

- functionality;
- reliability;
- environmental operating conditions;
- manufacturing (e.g. prohibited construction materials, minimum IPC-A-610 acceptability criteria (see 9.2.5), interchangeability).

6.2.1.3 Each component or subsystem delivered by a supplier, and which is to be integrated into the system, should be accompanied by an analysis that determines the hardware design characteristics of the component to the extent necessary to confirm its suitability as given in 7.2.

6.2.2 Reliability for class 3

If required to support the system-level reliability analysis, an analysis of the potential for hardware failures shall be required in the hardware requirements specification.

6.2.3 Environmental conditions requirements for class 3

The hardware environmental condition requirements shall identify the constraints the I&C system may undergo and address the related physical levels to take into account when applicable.

NOTE Typical constraints are climatic and electrical conditions.

6.2.4 Documentation requirements for class 3

The hardware documentation requirements shall be specified as part of the documentation requirements of the I&C system (see IEC 61513).

Annex A identifies typical documentation for each of the main clauses of this document.

7 Selection of pre-existing components

7.1 Selection of pre-existing components for class 1 and class 2

7.1.1 A suitability analysis shall be carried out and documented to demonstrate that the pre-existing components used in the equipment comply with the specified requirements defined in 6.1. The analysis may be part of an overall suitability analysis.

7.1.2 In addition to this suitability analysis, evidence of quality shall be provided and be based on:

- identification, versions;
- historical changes and related reports;
- quality management records;
- type tests conducted by the manufacturer;
- applied guides or standards;
- the manufacturer's operational experience.

7.1.3 If the suitability analysis or the evidence of quality have revealed lack of information then compensatory measures shall be put in place, for example testing, analysis, justification.

7.1.4 If the suitability analysis has revealed non-compliances, then they shall be addressed by modifying the hardware design or the system design (whilst ensuring that the requirements relating to nuclear safety are not compromised) or otherwise rejecting the component.

7.1.5 Pre-existing component design shall fulfil all of the specific maintenance requirements resulting from the hardware requirements specification.

NOTE These can include operational testing procedures, calibration, repair, periodic replacements and maintenance.

7.1.6 If the hardware reliability is not sufficient to fulfil the required targets, then compensatory measures shall be taken.

NOTE Such measures can include design improvements or changes related to in-service operation (such as increasing the frequency of periodic testing).

7.1.7 Care should be taken when it is decided to increase periodic testing, as all intrusive operations on the installed equipment incur an intrinsic risk of directly or indirectly introducing errors (for example the overall effect of periodic testing can negatively influence safety). Ideally, tests should be carried out when potential faults in the testing procedure cannot

impact safety, for example during outages or when tested equipment is isolated from the rest of the installation.

7.1.8 The design should be assessed against the risk of human errors during operation and maintenance activities (see 8.1.4.3).

7.2 Selection of pre-existing components for class 3

7.2.1 A suitability analysis shall be carried out and documented to demonstrate that the pre-existing components used in the equipment comply with the specified requirements defined in 6.2. The analysis may be part of an overall suitability analysis.

7.2.2 In addition to this suitability analysis, evidence of quality shall be provided and be based on:

- the manufacturer's operational experience;
- and/or data supplied by the electronic module manufacturers (nature and results of end-of-manufacture tests, operational experience, sample testing, audits, skills, certificates);
- and/or type tests conducted by the manufacturer.

7.2.3 When the evidence is based on the manufacturer's operational experience, it shall be formalised and based on:

- results from procurement inspections performed on successive batches and allowing verification of batch conformance and variation;
- and/or results from tests on samples;
- and/or operational results showing defects in equipment components of modules, detected through inspection performed during or at the end of manufacture, or through customer returns for repair.

8 Hardware aspects of system detailed design and implementation

8.1 Hardware aspects of system detailed design and implementation for class 1 and class 2

8.1.1 General requirement for class 1 and class 2

8.1.1.1 The phase hardware aspects of system detailed design and implementation shall take as an input the hardware requirements specification.

8.1.1.2 The design process should progress through design phases set out in the quality assurance plan (see 5.2.2), which result in the production of hardware which meets the hardware requirements specification.

The more general level of design activity may be termed the hardware general design, consisting of the analysis of different design alternatives in order to define the hardware system architecture in terms of subsystems and modules.

Hardware general design is generally followed by one or more detailed design levels.

8.1.1.3 The detailed design activities shall expand the general design to address the detailed design of subsystems, modules and components to the extent that the hardware design description is sufficiently complete to be implemented.

Prototype hardware can be built, not only to demonstrate successful interaction between hardware modules, but also to check hardware, software and HPD compatibility.

8.1.1.4 If the design takes place in a single phase, then this phase shall include the detailed hardware design.

8.1.2 Design activities for class 1 and class 2

8.1.2.1 System performance requirements which are dependent upon hardware performance shall be addressed by the hardware design, and evidence shall be made available, either through analysis or testing, to show that the hardware design meets these requirements (see 6.1.2.5).

8.1.2.2 Any discrepancy against hardware requirements shall be reconciled, by either changing the design or re-analysing the requirements (see 5.2.3.6).

8.1.2.3 The tests necessary to show that the required performance has been achieved shall be identified.

8.1.2.4 Such tests may be performed on the hardware alone, or performed when the hardware is integrated with the software and/or HPDs, i.e. as part of the system integration phase.

8.1.2.5 Maintenance activities required to provide confidence that the performance and reliability requirements are achieved during the operational life of the equipment shall be specified. These may include periodic tests, calibration, repairs, preventive and corrective maintenance. All these activities shall be documented in maintenance procedures.

8.1.2.6 Maintenance activities should be performed to an extent which provides sufficient confidence in correct operation of the equipment and yet reduces human interference and the performance of intrusive work with the systems to a minimum, so as to reduce the likelihood of faults being introduced through maintenance activities.

8.1.2.7 For equipment within a redundant system or several systems used to carry out a safety function, an analysis should take into account potential common cause failures due to hardware.

The potential causes resulting in the introduction of common cause failures related to the hardware are the following:

- Maintenance activities carried out simultaneously or sequentially on several items of equipment (particularly when these activities can introduce hardware failures);
- Periodic testing;
- Hidden hardware design faults that are not detected during the development lifecycle.

8.1.3 Reliability for class 1 and class 2

8.1.3.1 As required to support the system-level safety analysis, an analysis of the potential for hardware failures shall be made during design.

8.1.3.2 The method used for carrying out hardware reliability analyses shall be selected according to the pursued objectives.

Reliability requirements are specified in the hardware requirements specification as per 6.1.3.

The methods which may be used to analyse the system hardware reliability include:

- FTA (Fault Tree Analysis), which is concerned with the identification and analysis of conditions and factors which cause or contribute to the occurrence of a defined undesirable event (see IEC 61025 for advice concerning this technique);