IEC 60987

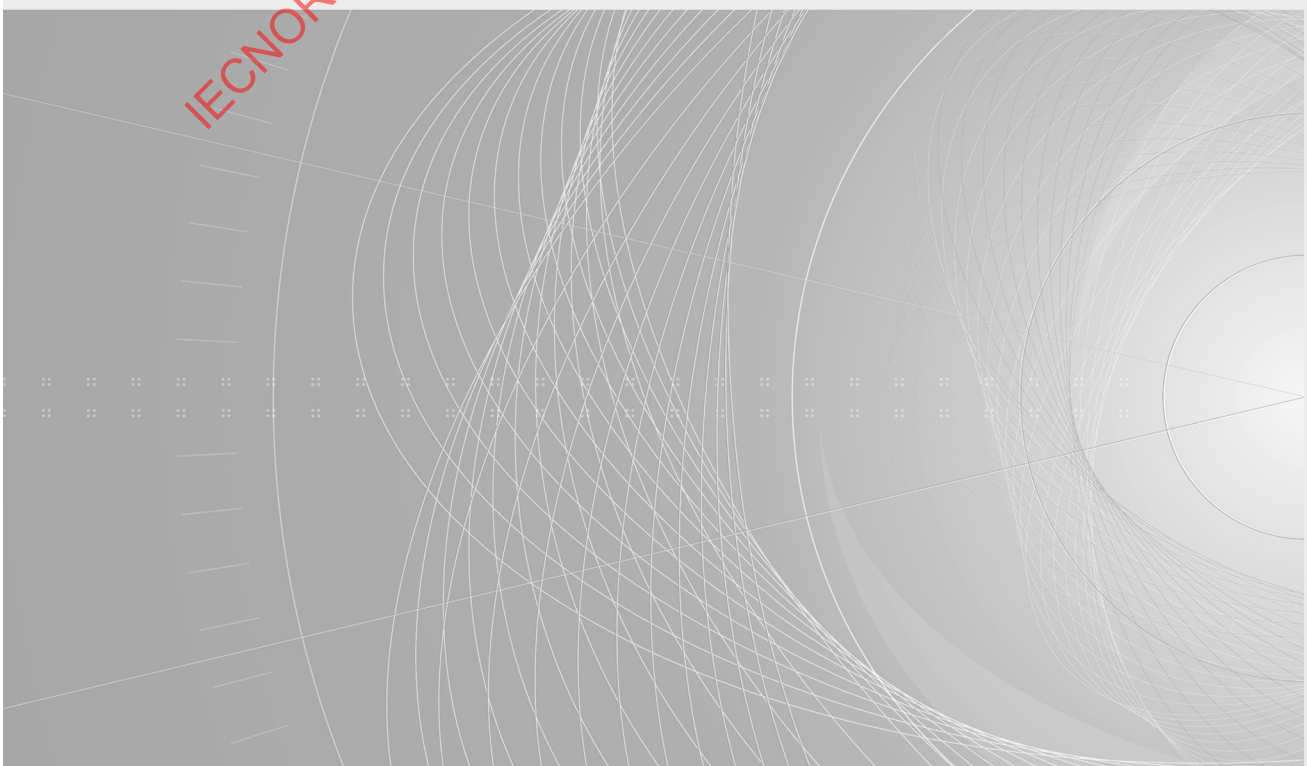
Edition 3.0 2021-02

INTERNATIONAL STANDARD

NORME INTERNATIONALE

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

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



IEC 60987:2021-02(en-fr)

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

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

IEC 60987

Edition 3.0 2021-02

INTERNATIONAL STANDARD

NORME INTERNATIONALE

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

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

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

ICS 27.120.20

ISBN 978-2-8322-9319-5

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/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).

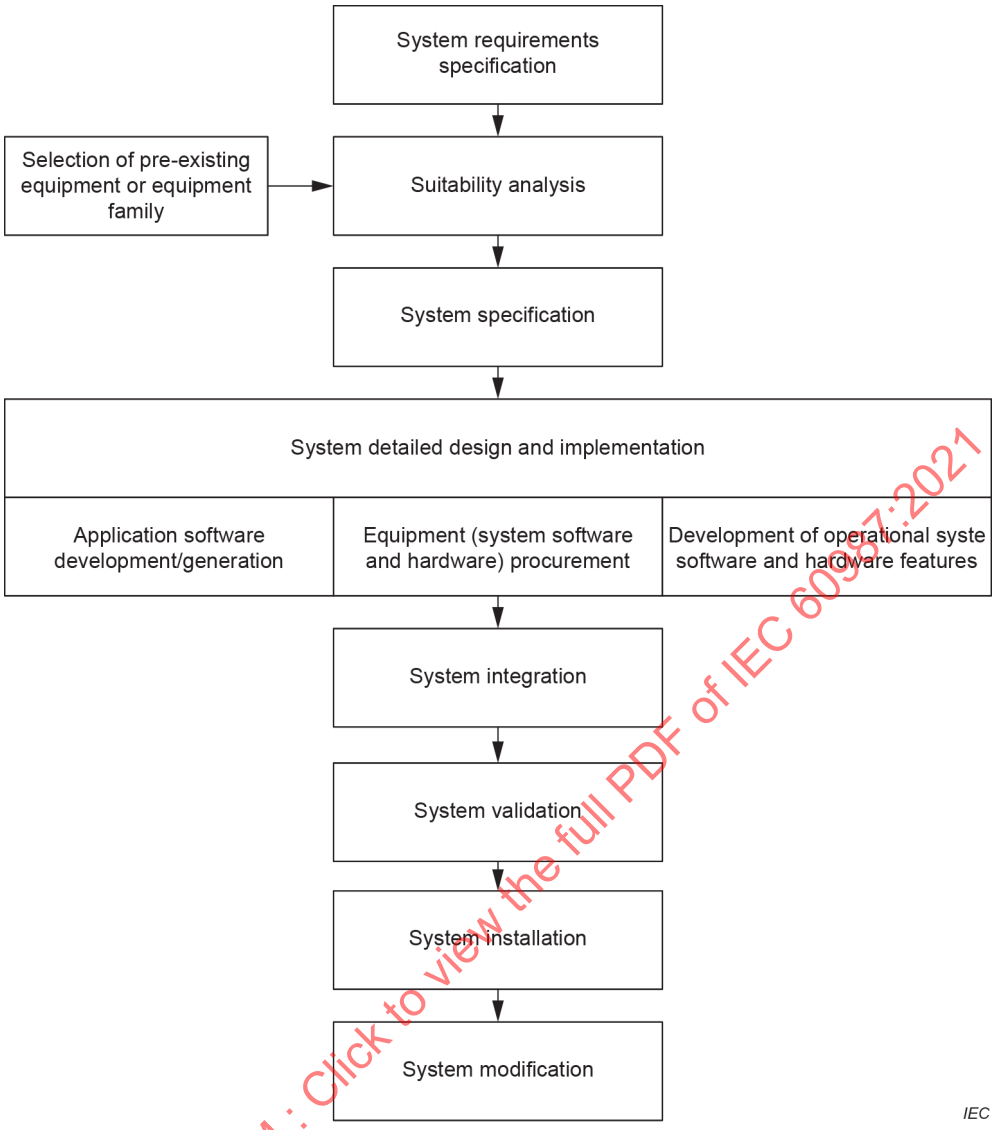


Figure 1 – System safety lifecycle (informative, as defined by IEC 61513)

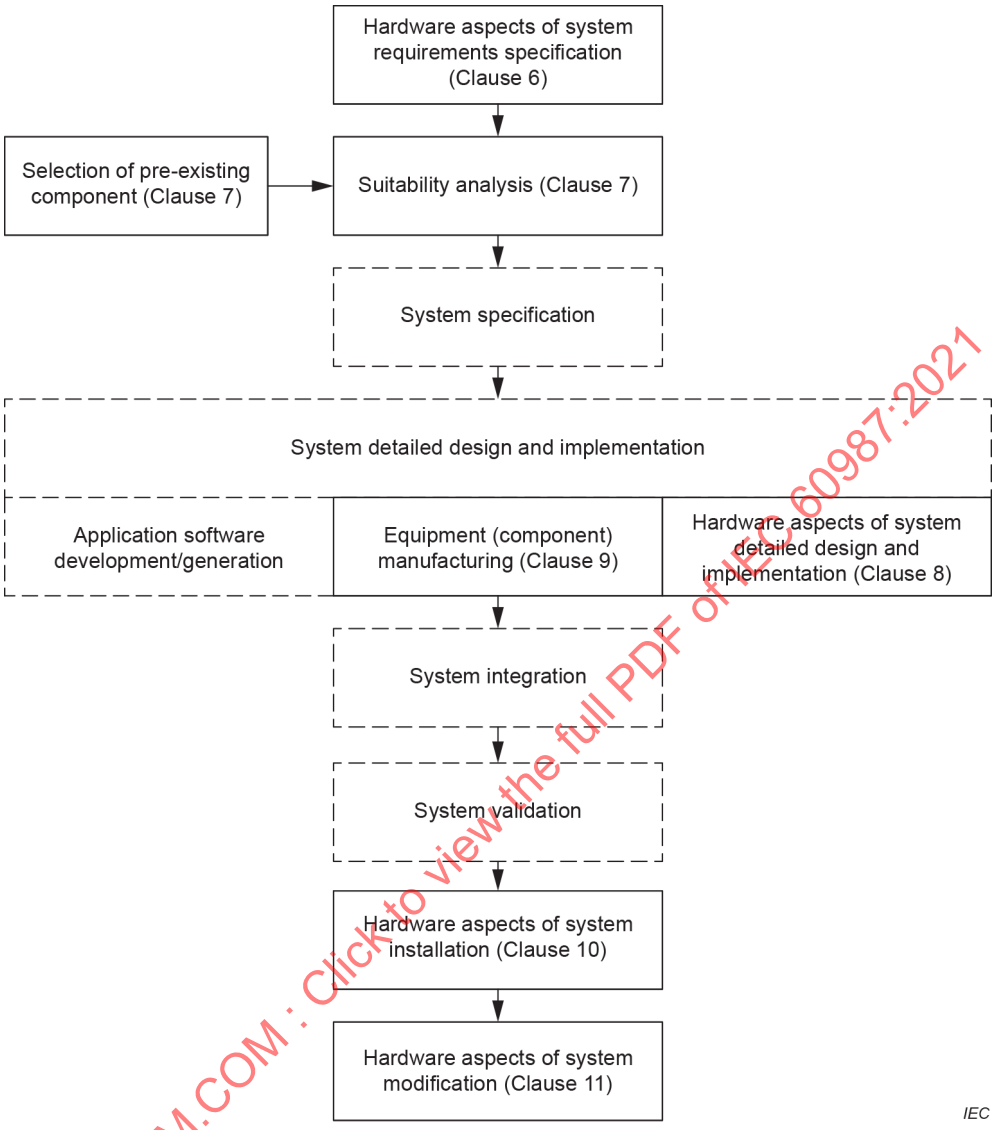
The system safety lifecycle of IEC 61513 is completed in IEC 60880 (for category A functions) and IEC 62138 (for category B and C functions) for software development, by IEC 62566 (for category A functions) and IEC 62566-2 (for category B and C functions) for HPD development and in IEC 60987 for hardware 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);

– FMEA (Failure Mode and Effects Analysis), which identifies failures which have significant consequences affecting the system performance, for example, reliability, safety; see IEC 60812 which describes a number of techniques for carrying out FMEAs and FMECAs (Failure Mode Effects and Criticality Analysis), and gives advice regarding the application of these methods according to the pursued objectives;
– For the failures rates estimates used as input data for the FMEA/FMECA, when differences exist between the final environmental conditions and the reference conditions, then guidance can be found to correct these data, for example in IEC 61709.

8.1.3.3 For class 1 equipment, an FTA or FMEA combined with component failure data shall be used to provide calculated values for system hardware reliability (see IEC 61513), unless sufficient operating experience is available to give high confidence that the hardware reliability targets are achieved.

8.1.3.4 For class 2 equipment, system hardware reliability shall be established either:

– by FTA or FMEA combined with component failure data;
– by a justification of adequate reliability provided on the basis of qualitative reasoning particularly if system hardware reliability is not overly demanding (for example, quality of components, hardware redundancy, operating experience, proportion of revealed hardware failures versus unrevealed hardware failures).

8.1.3.5 The hardware design should minimize the potential impact on nuclear safety of the following factors:

– maintenance activities;
– system failure due to random faults;
– hardware failure due to environmental conditions.

8.1.3.6 If the estimated hardware reliability is inadequate for the expected targets then compensating actions shall be taken, either in the form of design improvements or operational changes (such as an increase in the frequency of periodic testing).

When the option of increased periodic testing is chosen, care needs to be taken as any intrusive activities on operational plant carries an intrinsic degree of risk as faults can be induced or introduced (i.e. the net overall effect upon safety of periodic testing can be negative). Ideally, all testing is to be performed when potential faults in the testing process would not have a nuclear safety impact, for example, during station outages or when the equipment to be tested is isolated from operational plant.

Where a probabilistic safety assessment is used to support the safety case of an NPP, the estimated hardware reliability values (for example, as developed from FTA) may be fed into the NPP analysis, and so contributes to the accuracy of the overall station reliability calculations.

8.1.4 Maintenance for class 1 and class 2

8.1.4.1 The hardware design shall address any specific maintenance requirements contained within the hardware requirements specification.

8.1.4.2 Among all the electronic modules constituting an equipment those that are reparable and those that are not reparable shall be identified as such.

8.1.4.3 In addition, where practicable, the design should include features to reduce the risk of faults being introduced due to maintenance activities as follows:

– easy access to components which are likely to be replaced as consumables or following failures;

- clear identification of replaceable components to ensure that maintenance personnel can easily verify that the correct replacement components are used;
- use of components which can be replaced without intrusion on plant-process cabling;
- allow sufficient spacing between terminal blocks;
- adequate provision of dedicated terminals for use during calibration/testing activities (so that plant wiring does not have to be disconnected to facilitate such activities);
- hardware design supported by a structured layout with clear labelling to reduce the potential for maintenance errors.

8.1.5 Power failure for class 1 and class 2

8.1.5.1 To the extent required by the hardware requirements specification, the I&C system shall be designed to be insensitive to the consequences of short-term power failures and to potential variations of the power supply (voltage/frequency).

8.1.5.2 System features shall be provided to notify operators and maintenance staff of such power fluctuations (this role might not have been allocated to hardware, and hence may be out of scope of this document).

8.1.6 Design documentation for class 1 and class 2

8.1.6.1 The hardware design documentation shall describe the hardware design and the means by which the hardware requirements have been addressed.

8.1.6.2 Standardized forms of hardware design documentation and automated hardware design tools should be used.

8.1.6.3 A hierarchy of design documents addressing the I&C system hardware should be produced which consist of a number of documentation 'levels'.

8.1.6.4 The hardware design documentation at each level should specify the design aspects relevant to that level and define the hardware requirements for the lower levels or take into account the hardware characteristics from the lower level.

8.1.6.5 The hardware design documentation shall define the hardware architecture, i.e. the structure and relationship between the different parts of the system.

8.1.6.6 The hardware design documentation should include the general layout of hardware, with block diagrams of the subsystems and modules of the lower levels.

8.1.6.7 The hardware design documentation should also include hardware requirements for the hardware detailed design, such as:

- the number and types of central processor units and other processors;
- computer memory hardware requirements;
- the number and types of HPDs;
- the number and types of interfaces;
- the number and types of data links and busses.

8.1.6.8 At the conclusion of the design and implementation of the hardware, hardware design documentation shall be produced which contains a full and final description that conveys both the design details down to the lower level and the capabilities, limitations and other characteristics of the hardware.

8.1.6.9 This final hardware design documentation shall provide the following information:

- a design overview;
- cross-references to supporting design documents;
- a description of the subdivision of the hardware in terms of hardware subsystems;
- a description of each subsystem in terms of its major modules and components (using for example, block diagrams, circuit diagrams);
- a description of subsystem hardware interfaces; Interfaces shall be described as appropriate in logical, physical, electrical or other terms;
- a description of the I&C system hardware interfaces; Interfaces with any other systems, either within or outside the nuclear plant, shall be identified showing the specific interfaces and related hardware requirements;
- the physical layout; a description with diagrams of the physical layout of the equipment;
- a description of the environmental operating conditions of use and storage conditions;
- maintenance instructions, including the definition of any necessary actions (such as exchange of components) required to maintain the specified qualification lifetime;
- a description of hardware reliability and fail-safe properties;
- maintenance requirements.

8.2 Hardware aspects of system detailed design and implementation for class 3

8.2.1 General requirement for class 3

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

8.2.1.2 The hardware design documentation shall describe the hardware design and the means by which the hardware requirements have been addressed.

8.2.1.3 At the end of the design, the required hardware design documentation shall be produced and include a complete finalised description which contains all design details and which covers the functionalities, limitations and other hardware characteristics.

8.2.2 Reliability for class 3

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

8.2.3 Maintenance for class 3

8.2.3.1 The hardware design should address any specific maintenance requirements contained within the hardware requirements specification.

8.2.3.2 Among all the electronic modules constituting an equipment those that are reparable and those that are not reparable shall be identified as such.

9 Equipment (component) manufacturing

9.1 Equipment (component) manufacturing for class 1 and class 2

9.1.1 Manufacturing quality management for class 1 and class 2

9.1.1.1 Manufacturing activities shall be included in the quality assurance plan or, if not, shall be addressed by a separate manufacturing quality assurance plan.

9.1.1.2 Manufacturing-related activities during the design process (such as manufacturing assessments during product qualification) shall be included in the quality assurance plan.

NOTE Hardware produced during the manufacturing phase, and addressed in this clause, includes individual modules, sub-assemblies or equipment as a whole.

9.1.1.3 The primary consideration when defining manufacturing processes to which the quality assurance plan applies shall be to ensure that the manufacturing does not compromise the delivery of the safety functions by the product.

9.1.1.4 Procedures and work instructions shall be established for the manufacturing activities. These activities include manufacturing processes and their control, inspection and testing, independent quality surveillance and inspection, identification, handling, packaging, storage and delivery.

9.1.1.5 The extent and details of procedures and work instructions necessary for manufacturing activities shall be defined:

– to ensure the manufactured items meet the product description and specification generated during the design and implementation phases;

– to ensure the manufactured items meet the requirements demonstrated by the initial model during the qualification programme.

9.1.1.6 When the hardware contains components provided by external suppliers, the suppliers shall be evaluated and selected based on their ability to manufacture and supply these items in accordance with the product description and specification, including the requirements in 9.1 and defined quality assurance plan requirements.

9.1.1.7 When the designer of the I&C system chooses to outsource any process that affects product conformity to requirements, control over such processes shall be ensured. The type and extent of control to be applied to these outsourced processes shall be defined within the quality assurance plan.

9.1.1.8 Criteria for the selection, evaluation and re-evaluation of either external suppliers or sub-contractors shall be established and documented (e.g. general information such as business areas, scope of supply, technical capability and manufacturing capacity, quality organization, system and technical audits, financial health, market behaviour).

9.1.1.9 Quality management of manufacturing processes should be independently certified to recognised international standards by accredited bodies (e.g. the International Register for Certificated Assessors scheme for ISO 9001).

9.1.1.10 It shall be defined how the use of expired products in their manufacturing process is prevented.

9.1.2 Training of personnel for class 1 and class 2

9.1.2.1 The necessary competencies for personnel performing any kind of work involved in the manufacturing and control activities:

– shall be established, documented and maintained;

– or otherwise, training or relevant other actions shall be provided to achieve the necessary competence. The effectiveness of the training and actions taken shall be evaluated and recorded.

9.1.2.2 The personnel shall be trained to be aware of the relevance and importance of their activities and how they contribute to the achievement of the quality and safety objectives. In addition, appropriate records of education, training, skills and experience shall be established and maintained.

9.1.3 Planning and organisation of the manufacturing activities for class 1 and class 2

9.1.3.1 The manufacturing quality assurance plan shall be available at the start of the manufacturing phase and shall be kept up to date throughout the project.

9.1.3.2 Interfaces between different groups involved in the design, implementation and manufacturing activities shall be managed to ensure effective communication, clear definition of and assignment of responsibility for all aspects of the equipment relevant to the manufacturing process.

9.1.3.3 Effective arrangements for communicating with customers or inspectors shall be established to define and schedule manufacturing steps and the associated inspections, audits or controls.

9.1.4 Input data for class 1 and class 2

9.1.4.1 Manufacturing inputs shall be established during the design and implementation phase in order to provide appropriate information for manufacturing, testing and quality controls including product acceptance criteria.

9.1.4.2 The input data shall include the following information:

– the need for independence between manufacturing activities and a formal description of their content;

– any requirements for the customer approval of changes during manufacture to the sourcing of components or manufacturing consumables (e.g. solder);

– any requirements for the customer approval of the substitution during manufacture of components or manufacturing consumables (e.g. solder);

– any special training as a consequence of the equipment having a nuclear application.

9.1.4.3 Any requirements specified during the design process which have an impact on the manufacturing process shall be taken into account. This includes any statutory or regulatory requirements applicable to the product as well as physical and technical characteristics.

NOTE Commonly used manufacturing standards can be considered based on the safety class of the functions being performed by the hardware components. (e.g. ISO and ISA manufacturing standards, NEMA enclosures and protections standards, fire ratings standards, material processes standards, wiring techniques standards, etc.).

9.1.4.4 Input documents shall be reviewed prior to initiating manufacturing activities.

9.1.4.5 An input documents review shall ensure that product requirements are defined and that the defined requirements can be met.

9.1.4.6 The findings of the input documents review shall be recorded.

9.1.5 Purchasing and procurement for class 1 and class 2

9.1.5.1 Procurement process of commercially available components for class 1 and class 2

9.1.5.1.1 Demonstration or other suitable evidence shall be provided, that all the equipment components, including electronic components boards and housings, meet the specified requirements (e.g. functionality, environmental withstand, reliability and lifetime).

9.1.5.1.2 Demonstration shall be provided that the selected components fulfil the expected characteristics and quality and have been selected as described in 7.1.

9.1.5.2 Procurement process of items used in the I&C equipment for class 1 and class 2

9.1.5.2.1 The type and extent of control applied to the supplier or the sub-contractor and the purchased item shall be defined and contractually established with the supplier.

9.1.5.2.2 When the purchased item embeds or consist of programmable electronic components, specific additional requirements shall be in place to ensure strict configuration management and version control on hardware, software and HPDs revisions as per approved qualification and manufacturing records. Any and all changes shall be reported by the manufacturer and a safety impact assessment provided.

9.1.5.2.3 Records of the results of controls and any necessary actions arising from the evaluation shall be maintained.

9.1.5.2.4 Purchasing information shall describe the item to be purchased or sub-contracted, including, where appropriate:

– technical specification, (e.g. as schematics, drawings, control programs, test programs),
– requirements for approvals (e.g. processes, procedures, product and equipment),
– requirements for qualification of personnel,
– quality management system requirements.

9.1.5.3 Verification of purchased or sub-contracted items for class 1 and class 2

9.1.5.3.1 Inspection or other activities shall be established and performed to ensure that the purchased item, including the related expected documentation, meets the specified purchase requirements (see 5.2.3).

9.1.5.3.2 Where verification at the supplier's or the sub-contractor's premises is intended to be performed, verification arrangements and verification methods used shall be stated in the purchasing information. Requirements for preparation and acceptance of factory acceptance test plan(s), requirements for supervision and witnessing of acceptance testing, and requirements for final factory surveillance and inspection activities (i.e. to address any previously identified non-conformance issues and to confirm they have been resolved prior to shipment to site) shall be established.

9.1.5.3.3 The verification arrangements shall contain statements related to follow-up and control steps such as sampling tests, on-site observation or breakpoints.

9.1.5.3.4 Strict quality control shall be ensured of the incoming items, including the use of bonded stores where appropriate. The controls on the incoming goods shall include non-intrusive controls (e.g. visual inspection) and, where appropriate, intrusive controls, such as electrical tests and functional behaviour.

9.1.5.3.5 Control reports shall be written indicating the findings of the inspections carried out. These reports shall also ensure the traceability of all components (e.g. manufacturer, batch number).

9.1.6 Manufacturing for class 1 and class 2

9.1.6.1 Control of manufacturing for class 1 and class 2

9.1.6.1.1 Manufacturing shall be planned and carried out under controlled conditions.

Controlled conditions shall include, as applicable:

– availability of information that describes the characteristics of the product;

– availability of work instructions;
– availability of quality instruction;
– use and availability of suitable equipment and tools;
– traceability of component parts towards the BOM;
– recording of the dates and personnel responsible for the manufacturing operations;
– implementation of product release, delivery and post-delivery activities.

9.1.6.1.2 The processes used for the assembly of electronic modules shall be precisely described.

9.1.6.1.3 For each step, the following information shall be provided at a minimum:

– the operation carried out;
– the tools and products used;
– the verifications of tools (e.g. criteria, processes, means, frequency);
– the verifications carried out (e.g. sample sizes, sanctions in case of non-conformities);
– the level of training provided to operators;
– the premises where manufacturing takes place (e.g. level of cleanliness, temperature, humidity, protection against electro-static discharge);
– the standards used.

9.1.6.2 Specification and control of manufacturing environmental conditions for class 1 and class 2

9.1.6.2.1 Requirements for the environmental conditions for manufacturing and control areas shall be defined and documented.

9.1.6.2.2 Area access conditions such as rights to enter, procedures to follow and clothing to be worn shall be defined and documented.

9.1.6.2.3 Control plans for the environmental conditions of, and the access control to, the manufacturing facilities shall be established and documented (e.g. dust in the atmosphere, creating an inert atmosphere, humidity or temperature regulation, control of chemical composition of water, control of electrostatic discharges).

9.1.6.3 Validation of processes for manufacturing for class 1 and class 2

9.1.6.3.1 Specific processes for production provision shall be validated where the resulting output cannot be verified by subsequent monitoring or measurement and where, as a consequence, deficiencies become apparent only after the product has been in use or delivered.

9.1.6.3.2 The ability of these processes to be robust in order to achieve planned and repeatable results shall be demonstrated.

Arrangements shall be established for these processes including, as applicable:

– defined criteria for review and approval of the processes;
– approval of equipment and qualification of personnel;
– use of specific methods and procedures;
– requirements for records and validation;
– handling of defective parts including possible consequences for the manufacturing process.

9.1.6.4 Assessment of the manufactured I&C equipment acceptance and reproducibility for class 1 and class 2

9.1.6.4.1 The equipment produced shall be assessed and stated to be accepted by the customer.

9.1.6.4.2 The acceptance shall be based on the quality assurance management, the overall hardware qualification process and successful qualification results of the component, modules or equipment which usually are the first of a kind.

9.1.6.4.3 The designer of the I&C system shall be able to reproduce its equipment either by means of internal manufacture and assembly, or by means of sub-contract manufacture and assembly.

9.1.6.4.4 The evaluation of manufacturing should be based on surveys focusing on the I&C system manufacturer's organization and the technical means to manufacture the products.

9.1.6.4.5 When changes occur in the manufacturing process after the qualification of the initial item, an impact analysis shall be performed by the designer of the I&C equipment and conclusions shall be evaluated to decide if a new qualification has to be done or if the results of the previous qualification remain unchanged.

9.1.6.4.6 Dimensional controls and sampling plans for inspection shall conform to those specified in ISO 28590.

9.1.6.4.7 IPC-A-610 shall be applied for electronic assemblies acceptance criteria.

9.1.6.4.8 The minimum acceptability criteria shall be those of IPC-A-610 class 2.

9.1.6.4.9 For safety class 1 electronic assemblies, the acceptability criteria corresponding to IPC-A-610 class 3 should be applied.

This clause is a recommendation allowing handling situations where existing electronic boards may need to be used as designed formerly. On the other hand, any new electronic design does not usually face difficulties to fulfil IPC-A-610 class 3 criteria.

9.1.6.4.10 The IPC-A-610 level that the electronic assemblies comply with shall be documented.

9.1.6.4.11 The personnel shall be trained to be acquainted with IPC-A-610.

The formal accreditation of the personnel carrying out the manufacturing and controls to the IPC-A-610 standard is not required by this document.

9.1.6.4.12 The electronic components shall be subject to controls comprised of:

– A verification of the identification of the delivered components (markings on components or on coils);
– A verification of the conformity of the components with regards to the order (manufacturer, commercial reference, date code or date of manufacture);
– A verification of the absence of component deterioration (e.g. impact damage, oxidation, etc.).

9.1.6.4.13 For components that are available on the market but no longer through official distributors or components produced by manufacturers having negative feedback or components with poor documentation, the components shall be subject to functional tests and

characterised to ensure that they will be apt to fulfil their required functions under all the intended conditions (e.g. temperature, voltage, current, etc.), including limiting conditions.

NOTE 1 Controls of components can be carried out by characterization and test on each batch (e.g. same date code).

NOTE 2 Components that are no longer available through official distributors are commonly distributed by brokers. A broker is an independent seller having no contractual agreement with the original manufacturer of the component and carrying out no design activities on the component.

9.1.6.4.14 Brokers should be called upon only for components that are no longer available through official distributors.

9.1.6.4.15 For class 1 equipment, the quality of the components bought by brokers shall be evidenced by a justification of adequate reputation and quality measures.

9.1.6.4.16 The electronic assemblies shall be subject to controls comprised of:

– a verification of the identification of the delivered items;
– a verification of the IPC-A-610 certificate of compliance and of the associated class (can be replaced by a visual inspection of the compliance of the electronic assembly);
– a verification of the conformity of the dimensions, varnish, positioning of connectors and fixings and of the primary components of the electronic assembly with regards to its specification;
– a verification of the correct operation of the electronic assembly compared to its specification through functional testing. The functional tests shall at a minimum verify all of the primary functions of the electronic assembly and its critical characteristics. These tests can be carried out on individual electronic assemblies or on series of electronic assemblies;
– a verification by suitable means of the presence of the correct hardware, software and HPD versions.

9.1.6.4.17 Verifications shall be carried out in compliance with tests procedures and, where applicable, precisely identified test software.

9.1.6.4.18 These test procedures shall allow in particular the verification of:

– set values;
– the operation of electromechanical components;
– correct operation of all operating modes;
– when possible, the correct operation of self-tests and signalling circuitry;
– conformity of the primary static and dynamic electrical characteristics.

9.1.6.5 Control of manufacturing tools, monitoring and measuring devices for class 1 and class 2

9.1.6.5.1 The tools necessary to manufacture the product shall be determined.

9.1.6.5.2 Monitoring and measurement processes to be undertaken on the product shall be determined to provide evidence that the product conforms to its requirements.

9.1.6.5.3 Processes shall be established to ensure that manufacturing, monitoring and measurement are carried out in a manner that is consistent with the manufacturing, monitoring and measurement requirements.

9.1.6.5.4 Where necessary to ensure valid results, tools and measuring devices shall:

– be calibrated or verified, at specified intervals or prior to use, against measurement standards or established basis used for calibration or verification which are recorded;

– be adjusted or re-adjusted when necessary;

– have identification in order to determine their calibration status;

– be safeguarded from adjustments that would invalidate the measurement result;

– be protected from damage and deterioration during handling, maintenance and storage.

9.1.6.5.5 Quality assurance processes shall ensure that if manufactured equipment is found not to conform to requirements due to faults in the manufacturing process that adequate corrective action is taken.

9.1.6.5.6 Records of the results of manufacturing tools calibration, verification and corrective actions shall be maintained.

9.1.6.5.7 When software based devices are used in the monitoring and measurement activities, the ability of the device to satisfy the intended application shall be confirmed. This shall be undertaken prior to initial use and reconfirmed as necessary.

NOTE Confirmation of the ability of computer software to satisfy the intended application would typically include its verification and configuration management to maintain its suitability for use.

9.1.6.6 Identification and traceability for class 1 and class 2

9.1.6.6.1 The manufactured system shall be identified, as well as the parts and materials used to manufacture the system, by suitable means throughout product realization.

9.1.6.6.2 The manufactured system status shall be monitored throughout the overall manufacturing process.

9.1.6.6.3 A unique identification of the system, and of the included parts, shall be ensured and records of changes shall be maintained for traceability purposes.

9.1.6.6.4 An end of manufacturing report shall be established for each equipment and/or subassembly in order to define the configuration including the description of the equipment, the internal assemblies, components and versions. These files may typically include a list of sub-assemblies, plans, drawings, diagrams, data sheets, references to sub-tier detailed files, operators in order give an exhaustive description of a version of the system and/or sub-assemblies.

9.1.6.7 Protection and storage of products for class 1 and class 2

9.1.6.7.1 The system, and the included parts, shall be protected during internal processing in order to maintain conformity to requirements. Protection shall include identification and as applicable, handling, packaging, storage and protection conditions given before the acceptance test of the equipment.

9.1.6.7.2 The storage of components in order to manufacture electronic modules shall aim to avoid the decrease in the components reliabilities.

9.1.6.7.3 Protection against electro-static discharges shall be ensured by:

– dedicated packaging of sensitive components (antistatic packaging), featuring a clear indication warning of the danger of electro-static discharges;

– dedicated protection of electronic modules;

– the reduction in potential sources of electrostatic discharge (for example: through the use of antistatic bracelets, suitably protected workstations for the packaging and unpacking of components, conductive flooring);

– raising awareness and training of personnel.

9.1.6.7.4 The storage conditions (duration, environmental conditions) shall be compatible with:

– packaging and component protection specifications (e.g. antistatic strips, dry pack sachets);
– component manufacturer recommendations, in particular for components with expiration dates (for example electrolytic capacitors) or sensitive to taking on humidity.

9.1.6.8 Sustainability of tools and skills for class 1 and class 2

9.1.6.8.1 Requirements for the maintenance of tools and other means used during the manufacturing, testing, and validation activities shall be defined during the planning of the manufacturing activity and commensurate with the safety class of the functions being performed by the components.

9.1.6.8.2 Requirements shall be defined for maintaining the skills involved in manufacturing, testing and validation activities.

9.1.6.9 Resolution and control of non-conformities for class 1 and class 2

9.1.6.9.1 Non-conformities of manufacturing detected during environmental qualification tests, verification activities or manufacturing shall be identified and recorded according to the quality assurance plan (see 5.2.2).

9.1.6.9.2 Corrections and solutions shall be identified and recorded in such a way that they can be easily auditable by external parties. The related records shall indicate the nature of the changes, include impact analysis and associated justifications and approval.

9.1.6.9.3 Controls shall be ensured on the manufacturing line to check that the modifications have correctly been taken into account and that controls and test procedures have been correctly adapted (manufacture, identification and acceptance tests).

9.2 Equipment (component) manufacturing for class 3

9.2.1 Manufacturing quality management for class 3

9.2.1.1 Criteria for the selection, evaluation and re-evaluation of either external suppliers or sub-contractors should be established (e.g. general information such as business areas, scope of supply, technical capability and manufacturing capacity, quality organization, system and technical audits, financial health, market behaviour, etc.).

9.2.1.2 Quality management of manufacturing processes should be independently certified to recognised international standards by accredited bodies (e.g. the International Register for Certificated Assessors scheme for ISO 9001).

9.2.2 Training of personnel for class 3

The necessary competencies for personnel performing any kind of work involved in the manufacturing and control activities should be established, documented and maintained.

9.2.3 Input data for class 3

9.2.3.1 Manufacturing inputs should be established during the design and implementation phase in order to provide appropriate information for manufacturing and quality controls including product acceptance criteria.

9.2.3.2 The input data should include the following information:

– the need for independence between manufacturing activities and a formal description of their content;
– any requirements for the customer approval of changes during manufacture to the sourcing of components or manufacturing consumables (e.g. solder);
– any requirements for the customer approval of the substitution during manufacture of components or manufacturing consumables (e.g. solder).

9.2.3.3 Input documents should be reviewed prior to initiating manufacturing activities.

9.2.3.4 Input document review should ensure that product requirements are defined and that the defined requirements can be met.

9.2.3.5 The findings of the input document review and responses to those findings should be recorded.

9.2.4 Purchasing and procurement for class 3

9.2.4.1 Procurement process of commercially available components for class 3

Suitable evidence should be provided, that all the equipment components, including electronic components boards and housings, meet the specified requirements (e.g. functionality, environmental withstand, reliability and lifetime) and have been selected as described in 7.2.

9.2.4.2 Procurement process of items used in the I&C equipment for class 3

9.2.4.2.1 The type and extent of control applied to the supplier or the sub-contractor and the purchased item should be defined and contractually established with the supplier.

9.2.4.2.2 When the purchased item embeds or consists of programmable electronic components, specific additional requirements should be in place to ensure configuration management and version control on hardware, software and HPDs revisions as per approved qualification and manufacturing records. Any and all changes should be reported by the manufacturer.

9.2.4.3 Verification of purchased or sub-contracted items for class 3

Inspection or other activities shall be established and performed to ensure that the purchased item, including the related expected documentation, meets the specified purchase requirements (see 5.3.2).

9.2.5 Assessment of electronic modules for class 3

9.2.5.1 IPC-A-610 shall be applied for electronic assemblies acceptance criteria.

9.2.5.2 The minimum acceptability criteria shall be those of IPC-A-610 class 2.

9.2.5.3 The IPC-A-610 level that the electronic assemblies complies with shall be documented.

9.2.5.4 The personnel shall be trained to be acquainted with IPC-A-610.

The formal accreditation of the personnel carrying out the manufacturing and controls to the IPC-A-610 standard is not required by this document.

9.2.5.5 The electronic components shall be subject to controls comprised of:

– a verification of the identification of the delivered components (markings on components or on coils);

– a verification of the conformity of the components with regards to the order (manufacturer, commercial reference, date code or date of manufacture);
– a verification of the absence of component deterioration (e.g. impact damage, oxidation, etc.).

9.2.5.6 For components that are available on the market but no longer through official distributors or components produced by manufacturers having negative feedback, or components with poor documentation, the components shall be subject to functional tests and characterised to ensure that they will be apt to fulfil their required functions under all the intended conditions (e.g. temperature, voltage, current, etc.), including limiting conditions.

NOTE 1 Controls of components can be carried out by characterization and test on each batch (e.g. same date code).

NOTE 2 Components that are no longer available through official distributors are commonly distributed by brokers. A broker is an independent seller having no contractual agreement with the original manufacturer of the component and carrying out no design activities on the component.

9.2.5.7 Brokers should be called upon only for components that are no longer available through official distributors.

9.2.5.8 The electronic assemblies shall be subject to controls comprised of:

– a verification of the identification of the delivered items;
– a verification of the IPC-A-610 certificate of compliance and of the associated class (can be replaced by a visual inspection of the compliance of the electronic assembly);
– a verification of the conformity of the dimensions, varnish, positioning of connectors and fixings and of the primary components of the electronic assembly with regards to its specification;
– a verification of the correct operation of the electronic assembly compared to its specification through functional testing. The functional tests shall at a minimum verify all of the primary functions of the electronic assembly and its critical characteristics. These tests can be carried out on individual electronic assemblies or on series of electronic assemblies;
– a verification by suitable means of the presence of the correct hardware, software and HPD versions.

Controls of electronic assemblies can be carried out by survey.

9.2.5.9 Control reports shall be written indicating the findings of the inspections carried out. These reports shall also ensure the traceability of all components (e.g. manufacturer, batch number).

9.2.6 Identification and traceability for class 3

9.2.6.1 The manufactured system should be identified, as well as the parts and materials used to manufacture the system, by suitable means throughout product realization.

9.2.6.2 The manufacturing documentation should describe the manufacturing, storage, inspection and test activities and provide evidence that the requirements given in 9.2 are respected.

9.2.7 Protection and storage of product for class 3

9.2.7.1 The storage of components in order to manufacture electronic modules shall aim to avoid the decrease in the components reliabilities.

9.2.7.2 Protection against electro-static discharges shall be ensured by:

– dedicated packaging of sensitive components (antistatic packaging), featuring a clear indication warning of the danger of electro-static discharges;

– dedicated protection of electronic modules;

– the reduction in potential sources of electrostatic discharge (for example: through the use of antistatic bracelets, suitably protected workstations for the packaging and unpacking of components, conductive flooring);

– raising awareness and training of personnel.

9.2.7.3 The storage conditions (duration, environmental conditions) shall be compatible with:

– packaging and component protection specifications (e.g. antistatic strips, dry pack sachets);

– component manufacturer recommendations, in particular for components with expiration dates (for example electrolytic capacitors) or sensitive to taking on humidity).

9.2.8 Manufacturing of electronic modules for class 3

9.2.8.1 The processes used for the assembly of electronic modules shall be precisely described.

9.2.8.2 For each step, the following information shall be provided at a minimum:

– the operation carried out;

– the tools and products used;

– the verifications of tools (e.g. criteria, processes, means, frequency);

– the verifications carried out (e.g. sample sizes, sanctions in case of non-conformities);

– the level of training provided to operators;

– the premises where manufacturing takes place (e.g. level of cleanliness, temperature, humidity, protection against electro-static discharge);

– the standards used.

9.2.8.3 It shall be defined how the use of expired products in their manufacturing process is prevented.

9.2.8.4 When changes occur in the manufacturing process after the qualification of the initial item, an impact analysis shall be performed by the designer of the I&C equipment and conclusions shall be evaluated to decide if a new qualification has to be done or if the results of the previous qualification remain unchanged.

10 Hardware aspects of system installation

10.1 General

This Clause 10 applies to all safety classes.

The installation and commissioning requirements of this Clause 10 are consistent with and complete the requirements of the overall system installation, on site integration and commissioning as given in IEC 61513:2011, 6.2.7 and Clause 7.

10.2 Hardware aspects of installation activities shall be included in the system installation plan.

10.3 Packing, handling, transport, storage and unpacking shall be such as to prevent any damage to the system.

10.4 Before the system is unpacked and installed, the environment in which the system is to be installed shall be verified to conform to the hardware environmental conditions requirements, as covered by 6.1.4.

10.5 Adequate procedures and information shall be available to enable the system to be installed, cabled and wired in accordance with the design requirements (including, for example, qualification related requirements such as mechanical anchoring, earthing requirements).

10.6 Identification of items of equipment shall form part of this information.

10.7 The equipment shall be installed, tested individually and set to work in accordance with defined procedures before connected to the process.

10.8 The interconnection of the equipment shall be performed, tested and set to work as a system in accordance with defined procedures before being connected to the process.

10.9 The system as a whole shall be connected to the process and shall be checked by planned and specified commissioning tests, as required by IEC 61513.

On the completion of installation and commissioning, and when it has been confirmed that all acceptance criteria have been addressed (or concessions agreed), ownership of the system may be transferred to the user, as described in IEC 61513.

11 Hardware aspects of system modification

11.1 General

This Clause 11 applies to all safety classes.

Hardware design modification may be required to correct defective performance or to address new or revised performance requirements. The modification requirements of this Clause 11 are consistent with and complete the requirements of the overall system modification as given in IEC 61513:2011, 6.2.8 and 6.4.7.

11.2 Hardware design changes which have an impact beyond a single design phase (i.e. excluding any changes made by the designers while in the process of creating the design) shall be controlled by a documented procedure.

11.3 This design change procedure should take account of any potential impacts to other aspects of the system design, such as other hardware, software and HPD components.

11.4 The design change procedure shall ensure that the impact of all hardware changes on the hardware and system verification, validation and qualification processes is identified and any required re-work is performed.

11.5 Modified parts shall be identified in accordance with the relevant quality control procedures.

12 Operation and maintenance

12.1 General

This Clause 12 applies to all safety classes.

The operation and maintenance requirements of this clause are consistent with and complete the requirements of the overall operation and maintenance as given in IEC 61513:2011, Clause 8.

12.2 Operation and maintenance requirements

12.2.1 A formal procedure (or procedures) shall be available and applied to control the execution and the documentation of operation and maintenance activities. This shall take into account:

– preventative actions required to reduce the potential for faults to be introduced and the potential for personal injuries to occur;
– organizational and operational preparations required if the operation and maintenance activities have the potential to affect plant operation, or the availability of functions important to safety.

12.2.2 Operation and maintenance shall be undertaken by qualified and authorized personnel. It shall be performed according to specified procedures.

12.2.3 The procedures shall make provisions for approval (by an authorized person, or by automated test) to the effect that, where tasks can have a direct impact upon safety, each task has been completed satisfactorily.

12.2.4 All relevant information, such as time and date, replacements fitted, shall be recorded.

12.2.5 The records arising from maintenance work shall be made available for audit if required.

12.2.6 For identified components, rather than performing component replacement only when failure occurs, a preventative maintenance regime may be adopted. In this case, controls should be applied to ensure that components are replaced before their lifetime based on observed aging mechanisms.

12.2.7 Spare parts held by the operating organization shall be kept in a store which meets any environmental conditions adapted to this kind of parts.

12.2.8 The shelf life of spare parts shall be controlled and modified as necessary with the passage of time in accordance with the ageing characteristics of the hardware.

12.2.9 Any activities needed to preserve the state of readiness of the spares, such as periodic energization, shall be addressed.

12.2.10 All spares shall be under configuration control and shall have adequate identification marking or labelling.

12.2.11 The future supply of spare parts should be secured to the extent practicable (for example, either through the holding of spares, availability assurances from suppliers or by having access to manufacturing capability).

12.3 Failure data

12.3.1 Failure data acquired during equipment operation constitutes a major source of information which can be used to improve:

– component reliability data knowledge (by taking into account real operating environment conditions);

– equipment reliability evaluations (by determining actual field failure data in operating conditions);
– maintenance policy (through better spare parts optimization, better preventative maintenance schedules and better maintenance personnel training requirements).

12.3.2 Accordingly, field failure data (from information available from maintenance reports) should be logged in a failure data bank.

12.3.3 The maintenance records shall contain (if relevant and if known):

– identification of the system with the failed component;
– failure circumstances and failure effects;
– failed component identification;
– component location within the system;
– description of the fault which caused the failure;
– date of intervention;
– age of failed component;
– identification of person(s) who raised the report;
– identification of person(s) who diagnosed the fault.

12.3.4 Failure data for systems important to safety shall be subject to periodic review to ensure that the frequency of component failure remains within acceptable limits.

12.3.5 Any statistically significant negative trends in the data should be extrapolated to ensure, to the extent practicable, that the equipment will continue to operate satisfactorily in the future period up to the next assessment of the failure data of the equipment or until the equipment may be replaced (whichever is the shortest period).

12.3.6 Maintenance records should include data regarding real operating conditions: temperature and humidity.

12.4 Operation and maintenance documentation

12.4.1 Instructions for operation and maintenance shall be provided in an Operation and Maintenance Manual (OMM) that typically addresses the I&C system as a whole.

12.4.2 The OMM shall describe the hardware maintenance policy for the equipment in use, including identification of hardware components which require regular checking, re-calibration or replacement.

12.4.3 The OMM shall describe any relevant diagnostic processes which have to be used to detect the failure of specific modules.

12.4.4 The OMM shall describe the repair policy, i.e:

– the methods of repair or substitution of different subsystems, modules and components;
– any restrictions which the system shall be subjected to during repair time (for example, the system or parts of the system which shall be switched off);
– the extent to which equipment shall be revalidated after a repair.

12.4.5 In addition to the procedures for scheduled periodic maintenance, diagnostic procedures should be provided, where relevant and practicable, which may be used to assist in the investigation of anomalous system behaviour and to identify failed components.

Annex A
(informative)

Typical documentation

This annex identifies in Table A.1 typical documentation for each of the main clauses of this document. The choice and information arrangement among and within the documents may be done in relation with a graded approach for the class of the I&C system.

Table A.1 – Typical documentation

Documents concerning the hardware safety lifecycle	References
Quality assurance plan*	5.2.2, 5.3.1
Verification plan*	5.2.3.2
Documents concerning hardware aspects of system requirements specification	
Hardware requirements specification*	6.1, 6.2
Documents concerning selection of pre-existing components	
Pre-existing components suitability analysis and evidence of quality*	7.1.1, 7.1.2, 7.2.1, 7.2.2
Documents concerning hardware aspects of system detailed design and implementation	
Hardware design documentation	8.1.6, 8.2.1
Hardware reliability analyses	8.1.3
Recordings of verification/testing activities	5.2.3.5
Documents concerning the follow-up of discrepancies	5.2.3.6, 5.3.2
Documents concerning equipment (component) manufacturing	
Manufacturing quality assurance plan*	9.1.1
Procedures and work instructions	9.1.1
Recording of competencies of personnel	9.1.2, 9.2.2
Criteria for the selection, evaluation and re-evaluation of either external suppliers or sub-contractors	9.1.1
Review records of input documents coming from the design phase	9.1.4, 9.2.3
Control reports	9.2.5.9
Requirements for the environmental conditions for manufacturing and control areas	9.1.6.2
Records of the results of manufacturing tools calibration, verification and corrective actions	9.1.6.5
End of manufacturing report	9.1.6.6.4
Records of non-conformities of manufacturing	9.1.6.9
Documents concerning hardware aspects of system installation	
Installation plans*	10.2
Installation, cabling and wiring procedures*	10.5
On-site testing procedure*	10.7, 10.8
Documents concerning operation and maintenance	
Operation and Maintenance manual*	12.4
Records arising from maintenance*	12.2
Failure data bank	12.3
* These documents may be omitted when their content is included in system documents.	

Bibliography

IEC 60671:2007, *Nuclear power plants – Instrumentation and control systems important to safety – Surveillance testing*

IEC 61226, *Nuclear power plants – Instrumentation, control and electrical power systems important to safety – Categorization of functions and classification of systems*

IEC 61508 (all parts), *Functional safety of electrical/electronic/programmable electronic safety-related systems*

IEC 62340:2007, *Nuclear power plants – Instrumentation and control systems important to safety – Requirements for coping with common cause failure (CCF)*

IEC 62645, *Nuclear power plants – Instrumentation, control and electrical power systems – Cybersecurity requirements*

IEC 63046:2020, *Nuclear power plants – Electrical power systems – General requirements*

ISO 9001, *Quality management systems – Requirements*

IAEA Safety Glossary:2018

IAEA SSG-39, *Design of Instrumentation and Control Systems for Nuclear Power Plants*

IAEA SSR-2/1, *Safety of Nuclear Power Plants: Design*

AFCEN, RCC-E Ed. 2016, *Design and construction rules for Electrical and I&C systems and equipment*

Acknowledgement

The IEC thanks AFCEN for permission to use and/or reproduce information from its RCC-E 2016 edition. All extracts are copyrights of AFCEN. AFCEN takes no responsibility for the use and modification of the original text copied from RCC-E 2016 code.

SOMMAIRE

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

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

AVANT-PROPOS

1) La Commission Électrotechnique Internationale (IEC) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de l'IEC). L'IEC a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. À cet effet, l'IEC – entre autres activités – publie des Normes internationales, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de l'IEC"). Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'IEC, participent également aux travaux. L'IEC collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
2) Les décisions ou accords officiels de l'IEC concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de l'IEC intéressés sont représentés dans chaque comité d'études.
3) Les Publications de l'IEC se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de l'IEC. Tous les efforts raisonnables sont entrepris afin que l'IEC s'assure de l'exactitude du contenu technique de ses publications; l'IEC ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.
4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de l'IEC s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de l'IEC dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de l'IEC et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
5) L'IEC elle-même ne fournit aucune attestation de conformité. Des organismes de certification indépendants fournissent des services d'évaluation de conformité et, dans certains secteurs, accèdent aux marques de conformité de l'IEC. L'IEC n'est responsable d'aucun des services effectués par les organismes de certification indépendants.
6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.
7) Aucune responsabilité ne doit être imputée à l'IEC, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de l'IEC, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de l'IEC ou de toute autre Publication de l'IEC, ou au crédit qui lui est accordé.
8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.
9) L'attention est attirée sur le fait que certains des éléments de la présente Publication de l'IEC peuvent faire l'objet de droits de brevet. L'IEC ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de brevets et de ne pas avoir signalé leur existence.

La Norme internationale IEC 60987 a été établie par le sous-comité 45A: Systèmes d'instrumentation, de contrôle-commande et d'alimentation électrique des installations nucléaires, du comité d'études 45 de l'IEC: Instrumentation nucléaire.

Cette troisième édition annule et remplace la deuxième édition parue en 2007, et son Amendement 1 paru en 2013. Cette édition constitue une révision technique.

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

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

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

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

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

Ce document a été rédigé selon les Directives ISO/IEC, Partie 2.

Le comité a décidé que le contenu de ce document ne sera pas modifié avant la date de stabilité indiquée sur le site web de l'IEC sous "http://webstore.iec.ch" dans les données relatives au document recherché. À cette date, le document sera

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

INTRODUCTION

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

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

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

Les principes de base de conception de l'instrumentation nucléaire tels qu'ils sont spécifiquement appliqués aux systèmes importants pour la sûreté des centrales nucléaires de puissance (CNP) ont d'abord été interprétés dans les normes du secteur nucléaire en référence aux systèmes câblés, en particulier dans le "Guide de sûreté 50 SG D3" de l'AIEA qui a été remplacé par le guide de l'AIEA SSG-39.

La première édition de l'IEC 60987 a été publiée en 1989 pour couvrir les aspects matériels de la conception des systèmes informatisés des systèmes importants pour la sûreté.

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

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

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

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

L'IEC 60880 et l'IEC 62138 sont des normes de second niveau de la collection de normes du SC 45A qui couvrent ensemble les aspects logiciels relatifs aux systèmes informatisés utilisés pour réaliser des fonctions importantes pour la sûreté des CNP. L'IEC 60880 et l'IEC 62138 font directement référence à l'IEC 60987 pour les exigences matériel des systèmes d'I&C.

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

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

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

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

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

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

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

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

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

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

d) Description de la structure de la série de normes du SC 45A de l'IEC et relations avec d'autres documents de l'IEC, et d'autres organisations (AIEA, ISO)

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

L'IEC 61513 et l'IEC 63046 renvoient directement à d'autres normes du SC 45A de l'IEC pour les sujets généraux liés à la catégorisation des fonctions et à la classification des systèmes, la qualification, la séparation, la défense contre les défaillances de cause commune, la conception des salles de contrôle, la compatibilité électromagnétique, la cybersécurité, les aspects logiciels et matériels des systèmes numériques programmables, la coordination des exigences de sûreté et de sécurité et la gestion du vieillissement. Il convient de considérer que ces normes, de second niveau, forment, avec l'IEC 61513 et l'IEC 63046, un ensemble documentaire cohérent.

Au troisième niveau, les normes du SC 45A de l'IEC, qui ne sont généralement pas référencées directement par l'IEC 61513 ou l'IEC 63046, sont relatives à des matériels particuliers, à des méthodes ou à des activités spécifiques. Généralement ces documents, qui font référence aux documents de deuxième niveau pour les activités génériques, peuvent être utilisés de façon isolée.

Un quatrième niveau qui est une extension de la collection de normes du SC 45A de l'IEC correspond aux rapports techniques qui ne sont pas des documents normatifs.

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

L'IEC 61513 et l'IEC 63046 ont adopté une présentation similaire à celle de l'IEC 61508, avec un cycle de vie d'ensemble et un cycle de vie des systèmes. Au niveau sûreté nucléaire, l'IEC 61513 et l'IEC 63046 sont l'interprétation des exigences générales de l'IEC 61508-1, l'IEC 61508-2 et de l'IEC 61508-4 pour le secteur nucléaire. Dans ce domaine, l'IEC 60880, l'IEC 62138 et l'IEC 62566 correspondent à l'IEC 61508-3 pour le secteur nucléaire. L'IEC 61513 et l'IEC 63046 font référence aux normes ISO ainsi qu'aux documents AIEA GSR partie 2 et AIEA GS-G-3.1 et AIEA GS-G-3.5 pour ce qui concerne l'assurance qualité. Au second niveau, l'IEC 62645 est le document chapeau du SC 45A de l'IEC portant sur la sécurité nucléaire. Elle est élaborée à partir des principes de haut niveau et des concepts principaux des normes de sécurité génériques, en particulier des normes ISO/IEC 27001 et ISO/IEC 27002; elle les adapte et les complète pour qu'ils deviennent pertinents pour le secteur nucléaire; elle est coordonnée étroitement avec la série de normes IEC 62443. Au second niveau, l'IEC 60964 est le document chapeau des normes du SC 45A de l'IEC portant sur les salles de commande et l'IEC 62342 est le document chapeau des normes du SC 45A de l'IEC portant sur la gestion du vieillissement.

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

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

1 Domaine d'application

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

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

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

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

Les constituants prédéveloppés peuvent contenir des microcontrôleurs ou des HPD et, lorsque les microprogrammes ou des fichiers de programmation sont profondément intégrés, être entièrement "transparents" pour l'utilisateur. Dans ce cas, le présent document peut être utilisé comme guide pour le processus d'évaluation de tels composants. Un exemple pour lequel cette approche est considérée comme adaptée est l'évaluation des processeurs modernes qui comprennent du microcode. Un tel code fait généralement partie intégrante du matériel, ainsi il est donc acceptable d'évaluer le processeur (comprenant le microcode) en tant que composant matériel intégré en appliquant le présent document.

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

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

2 Références normatives

Les documents suivants sont cités dans le texte de sorte qu'ils constituent, pour tout ou partie de leur contenu, des exigences du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

IEC/IEEE 60780-323, *Installations nucléaires – Équipements électriques importants pour la sûreté – Qualification*

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

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

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

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

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

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

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

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

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

IEC 62566:2012, *Centrales nucléaires de puissance – Instrumentation et contrôle commande importants pour la sûreté – Développement des circuits intégrés programmés en HDL pour les systèmes réalisant des fonctions de catégorie A*

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

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

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

3 Termes et définitions

Pour les besoins du présent document, les termes et définitions suivants s'appliquent.

L'ISO et l'IEC tiennent à jour des bases de données terminologiques destinées à être utilisées en normalisation, consultables aux adresses suivantes:

- IEC Electropedia: disponible à l'adresse http://www.electropedia.org/
- ISO Online browsing platform: disponible à l'adresse http://www.iso.org/obp

3.1
classe d'un système d'I&C
l'une des trois affectations possibles (1,2,3) des systèmes d'I&C importants pour la sûreté, résultant de la nécessité pour ces systèmes d'exécuter des fonctions d'I&C d'importances pour la sûreté différentes

Note 1 à l'article: Une affectation "non classé" est délivrée si le système d'I&C n'exécute pas de fonction importante pour la sûreté.

Note 2 à l'article: Voir également "catégorie d'une fonction d'I&C", "système important pour la sûreté", "systèmes de sûreté".

[SOURCE: IEC 61513:2011, 3.6, modifié – La dernière phrase de la définition est devenue la Note 1 à l'article.]

3.2
défaillance de cause commune, DCC
défaillance de plusieurs structures, systèmes ou composants due à un événement ou à une cause spécifique unique

Note 1 à l'article: Les causes communes peuvent être internes ou externes à un système d'I&C.

[SOURCE: Glossaire de sûreté de l'AIEA: 2018, modifié – La Note 1 à l'article a été ajoutée.]

3.3
composant
l'une des pièces constituant un système

Note 1 à l'article: Un composant peut être matériel, logiciel ou HPD et peut être subdivisé en plusieurs autres composants

Note 2 à l'article: Voir également "système d'I&C", "équipement".

Note 3 à l'article: Les termes "équipement", "composant", et "module" sont souvent utilisés de manière interchangeable. La relation entre ces termes n'a pas encore été normalisée.

Note 4 à l'article: Cette définition du SC 45A de l'IEC est dans le principe compatible avec la sous-définition de "Composant" donnée dans la définition de "SSC, Structures, Systèmes et Composants" du Glossaire de sûreté de l'AIEA Édition 2018. Néanmoins comme il est seulement donné des exemples de composants matériel, ceci peut induire en erreur le lecteur, aussi le SC 45A de l'IEC a préféré utiliser une définition qui explicitement couvre les composants logiciel.

[SOURCE: IEC 61513:2011, 3.10, modifié – La dernière phrase de la définition est devenue la Note 1 à l'article et l'édition 2007 du Glossaire de sûreté de l'AIEA a été mise à jour en regard de l'édition 2018.]

3.4
élément informatisé
élément qui s'appuie sur des instructions logicielles s'exécutant sur des microprocesseurs ou des microcontrôleurs

Note 1 à l'article: Dans ce terme et sa définition le mot "élément" peut être remplacé par les mots "système", "équipement" ou "dispositif".

Note 2 à l'article: Un élément informatisé est un type d'élément numérique programmable.

Note 3 à l'article: Ce terme équivaut au terme "élément programmé".

Note 4 à l'article: Les définitions des termes suivants: élément E/E/PE, élément électrique, systèmes d'I&C, élément programmable numérique, élément informatisé, élément câblé, dispositif à logique programmable, HPD doivent être prises en considération conjointement et sont totalement consistantes et cohérentes. Elles sont totalement cohérentes et conformes aux exigences générales établies par l'IEC 61513 et l'IEC 63046 pour les systèmes d'instrumentation, de contrôle et d'électricité des centrales nucléaires.

[SOURCE: IEC 62138:2018, 3.8, modifié – La Note 4 à l'article a été ajoutée.]

3.5
élément électrique/électronique/électronique programmable
élément E/E/PE
élément réalisé à base de technologie électrique (E) et/ou électronique (E) et/ou électronique programmable (PE)

Note 1 à l'article: Dans ce terme et sa définition le mot “élément” peut être remplacé par les mots “système”, “équipement” ou “dispositif”.

Note 2 à l'article: Les définitions des termes suivants: élément E/E/PE, élément électrique, systèmes d'I&C, élément numérique programmable, élément informatisé, élément câblé, réseau logique programmable, circuit intégré programmé en HDL (*hardware description language* - langage de description de matériel) doivent être prises en considération conjointement et sont totalement consistantes et cohérentes. Elles sont totalement cohérentes et conformes aux exigences générales établies par l'IEC 61513 et l'IEC 63046 pour les systèmes d'instrumentation, de contrôle et d'électricité des centrales nucléaires.

[SOURCE: IEC 62138:2018, 3.15, modifié – La Note 2 à l'article a été ajoutée.]

3.6
système d'alimentation électrique
EPS
système assurant la production, le transport et la distribution et qui alimente les fonctions pour faire fonctionner les équipements de l'installation (pompes, vannes, réchauffeurs, etc.)

Note 1 à l'article: Un système d'alimentation électrique peut comprendre des éléments E/E/PE pour réaliser sa régulation et sa protection électriques internes.

Note 2 à l'article: L'abréviation "EPS" est dérivée du terme anglais développé correspondant "*electrical power system*".

[SOURCE: IEC 63046:2020, 3.12]

3.7
équipement
une ou plusieurs parties d'un système

Note 1 à l'article: Un équipement est une partie déterminée et définissable (et généralement amovible) d'un système

Note 2 à l'article: Voir également “composant”, “système d'I&C”.

Note 3 à l'article: L'équipement peut comprendre des logiciels.

Note 4 à l'article: Les termes “équipement”, “composant”, et “module” sont souvent utilisés de manière interchangeable. La relation entre ces termes n'a pas encore été normalisée.

[SOURCE: IEC 61513:2011, 3.16, modifié – La dernière phrase de la définition est devenue la Note 1 à l'article et la Note 4 à l'article de l'IEC 61513 a été supprimée.]

3.8
microprogramme
logiciel étroitement dépendant des caractéristiques du matériel sur lequel celui-ci est installé

Note 1 à l'article: La présence de microprogramme est généralement “transparente” pour l'utilisateur du composant matériel et ainsi il peut être effectivement considéré comme faisant partie intégrante de la conception du matériel (un bon exemple est le microcode d'un processeur).

Note 2 à l'article: Généralement, le microprogramme ne peut être modifié par un utilisateur qu'en remplaçant le composant matériel (par exemple puce du processeur, carte, EPROM) qui contient ce logiciel par des composants contenant le logiciel modifié, et lorsque c'est le cas, il convient que la gestion de configuration des composants matériels assure la gestion de configuration des microprogrammes. Le microprogramme, tel qu'il est envisagé dans le présent document, est effectivement un logiciel embarqué dans le matériel.

3.9
fonction
but précis ou objectif devant être accompli, qui peut être spécifié ou décrit sans référence aux moyens physiques nécessaires pour son atteinte

[SOURCE: Glossaire de sûreté de l'AIEA, 2018]

3.10
élément câblé
élément qui s'appuie sur des relais, sur des logiques électroniques analogiques ou sur des logiques numériques discrètes

Note 1 à l'article: Dans ce terme et sa définition le mot "élément" peut être remplacé par les mots "système", "équipement" ou "dispositif".

Note 2 à l'article: Ce terme utilisé par le SC 45A de l'IEC est à peu près équivalent à celui d'"élément électronique" utilisé par l'IEC 61508. Les relais sont des éléments électromécaniques et non électroniques, mais ils sont inclus dans le terme "élément câblé".

Note 3 à l'article: Les éléments câblés sont aussi généralement appelés "éléments conventionnels".

Note 4 à l'article: Les définitions des termes suivants: élément E/E/PE, élément électrique, systèmes d'I&C, élément numérique programmable, élément informatisé, élément câblé, réseau logique programmable, circuit intégré programmé en HDL (langage de description de matériel) doivent être prises en considération conjointement et sont totalement consistantes et cohérentes. Elles sont totalement cohérentes et conformes aux exigences générales établies par l'IEC 61513 et l'IEC 63046 pour les systèmes d'instrumentation, de contrôle et d'électricité des centrales nucléaires.

3.11
langage de description de matériel
HDL
langage permettant de décrire formellement les fonctions et/ou la structure d'un composant électronique, à des fins documentaires, de simulation ou de synthèse

Note 1 à l'article: Les HDL les plus utilisés sont VHDL (IEEE 1076) et Verilog (IEEE 1364).

Note 2 à l'article: L'abréviation "HDL" est dérivée du terme anglais développé correspondant "*hardware description language*".

[SOURCE: IEC 62566:2012, 3.6]

3.12
circuit intégré programmé en HDL
HPD
circuit intégré configuré avec des HDL et outils associés

Note 1 à l'article: Les HDL et outils associés (par exemple simulateur, synthétiseur) sont utilisés pour réaliser les exigences par un assemblage adéquat de ressources microélectroniques prédéveloppées.

Note 2 à l'article: Le développement de HPD peut utiliser des Blocs Prédéveloppés.

Note 3 à l'article: Les HPD sont typiquement fondés sur des FPGA ou des technologies microélectroniques similaires.

Note 4 à l'article: Un HPD est un type d'élément numérique programmable.

Note 5 à l'article: Les définitions des termes suivants: élément E/E/PE, élément électrique, systèmes d'I&C, élément numérique programmable, élément informatisé, élément câblé, réseau logique programmable, circuit intégré programmé en HDL (langage de description de matériel) doivent être prises en considération conjointement et sont totalement consistantes et cohérentes. Elles sont totalement cohérentes et conformes aux exigences générales établies par l'IEC 61513 et l'IEC 63046 pour les systèmes d'instrumentation, de contrôle et d'électricité des centrales nucléaires.

Note 6 à l'article: L'abréviation "HPD" est dérivée du terme anglais développé correspondant "*HDL-programmed device*".

[SOURCE: IEC 62566:2012, 3.7, modifié – Ajout de la Note 4 à l'article et de la Note 5 à l'article.]

3.13
système d'I&C
système exécutant des fonctions d'I&C ainsi que des fonctions de service et d'affichage liées au fonctionnement du système lui-même. Sa technologie est électrique et/ou électronique et/ou électronique programmable

Note 1 à l'article: Le terme est utilisé comme terme général comprenant tous les éléments du système, tels que les alimentations électriques, les capteurs et autres dispositifs d'entrée, les bus de données et autres chemins de communication, les actionneurs et autres dispositifs de sortie. Les différentes fonctions d'un système peuvent utiliser des ressources dédiées ou partagées.

Note 2 à l'article: Voir également "système" et "fonction d'I&C".

Note 3 à l'article: Les éléments contenus dans un système d'I&C donné sont définis dans la spécification des limites de ce système.

Note 4 à l'article: Selon leur fonctionnalité propre, l'AIEA fait la distinction entre les systèmes de contrôle et de commande, les systèmes d'IHM, les systèmes de verrouillage et les systèmes de protection.

[SOURCE: IEC 61513:2011, 3.29, modifié – La dernière phrase de la définition est devenue la Note 1 à l'article.]

3.14
intégration
agrégation et vérification progressives des composants pour former un système complet

[SOURCE: IEC 62138:2018, 3.27]

3.15
essais périodiques
réalisation d'essais à des instants prédéfinis permettant de démontrer que les capacités fonctionnelles des systèmes et des matériels d'I&C importants pour la sûreté sont assurées et de confirmer que les caractéristiques importantes pour satisfaire aux exigences de l'analyse de sûreté sont satisfaites

[SOURCE: IEC 60671:2007, 3.7]

3.16
constituant prédéveloppé
constituant matériel, câblé ou programmé qui existe déjà, qui est disponible comme produit commercial ou propriétaire, et dont l'utilisation est envisagée

Note 1 à l'article: Cette définition inclut celle des logiciels prédéveloppés ou HDL, voir l'IEC 60880, l'IEC 62138, l'IEC 62566 et l'IEC 62566-2.

Note 2 à l'article: Les constituants prédéveloppés peuvent être commercialement disponibles sur étagère (également appelés "COTS") ou des produits propriétaires utilisés en interne par un fabricant (voir l'IEC 61513:2011, 6.2.3.2).

[SOURCE: IEC 61513:2011, 3.36, modifié – La définition et les Notes à l'article ont été modifiées pour traiter les éléments électriques, électroniques, électroniques programmables et COTS.]

3.17
élément numérique programmable
élément qui s'appuie sur des instructions logicielles ou une logique programmable pour accomplir une fonction

Note 1 à l'article: Dans ce terme et sa définition le mot “élément” peut être remplacé par les mots “système”, “équipement” ou “dispositif”.

Note 2 à l'article: Les principaux éléments numériques programmables sont les éléments informatisés et les éléments à logique programmables.

Note 3 à l'article: Ce terme utilisé par l'IEC SC 45A équivaut au terme “élément électronique programmable” (élément PE) défini selon l’IEC 61508.

Note 4 à l'article: Les définitions des termes suivants: élément E/E/PE, élément électrique, systèmes d'I&C, élément numérique programmable, élément informatisé, élément câblé, réseau logique programmable, circuit intégré programmé en HDL (langage de description de matériel) doivent être prises en considération conjointement et sont totalement consistantes et cohérentes. Elles sont totalement cohérentes et conformes aux exigences générales établies par l’IEC 61513, l’IEC 60880, l’IEC 62138, l’IEC 62566 et l’IEC 62566-2* pour les systèmes d'instrumentation, de contrôle et d'électricité des centrales nucléaires.

[SOURCE: IEC 62138:2018, 3.34, modifié – La Note 4 à l’article a été ajoutée.]

3.18
élément à logique programmable
élément qui s'appuie sur circuit intégré composé d’éléments logiques avec un motif d’interconnexions, dont des parties sont programmables par l’utilisateur

Note 1 à l'article: Dans ce terme et sa définition le mot "élément" peut être remplacé par les mots “système”, "équipement" ou "dispositif".

Note 2 à l'article: Un élément à logique programmable est une sorte d'élément numérique programmable.

Note 3 à l'article: Voir aussi la définition d'élément E/E/PE et les notes associées.

[SOURCE: IEC 62138:2018, 3.35]

3.19
qualification
processus déterminant si un système ou composant est apte à l’utilisation opérationnelle. La qualification est effectuée dans le contexte de la classe de sûreté particulière du système d’I&C et d’un ensemble particulier d’exigences de qualification

Note 1 à l'article: Les exigences de qualification dérivent de la classe particulière du système d’I&C et du contexte particulier de l’application.

Note 2 à l'article: Les systèmes d’I&C sont généralement mis en œuvre à partir d’un ensemble d’équipement interagissant. De tels équipements peuvent être développés comme une partie de projet, ou ils peuvent être des équipements préexistants. Généralement, la qualification d’un système d’I&C est réalisée par étapes: d’abord la qualification de l’équipement individuel préexistant (habituellement tôt dans le processus de réalisation du système); et plus tard la qualification du système d’I&C intégré (par exemple sur la conception finale).

Note 3 à l'article: La qualification des systèmes d’I&C est toujours une activité particulière à la centrale et à l’application. Cependant, ceci peut reposer dans une grande mesure sur des activités de qualification réalisées hors du contexte particulier à la conception d’une centrale (celles-ci sont appelées “qualification générique” ou “préqualification”). Une préqualification peut réduire l’effort de qualification propre à la centrale, néanmoins, il est nécessaire de démontrer la satisfaction aux exigences de qualification particulière à l’application.

[SOURCE: IEC 61513:2011, 3.38, modifié – La définition intégrée de l’équipement préexistant a été supprimée de la Note 2 à l’article et la dernière phrase de la Note 3 a été corrigée.]

3.20
défaut aléatoire
défaut non systématique d'un composant matériel

Note 1 à l'article: Les défauts matériels sont les conséquences d'effets chimiques ou physiques, qui peuvent survenir à tout instant. Une bonne description de la probabilité d'apparition des défauts aléatoires peut être assurée en utilisant les statistiques (taux de défauts). Un taux de défauts en augmentation peut être la conséquence de défauts systématiques dans la conception ou la fabrication du matériel, si cela survient sans corrélation temporelle, par exemple comme conséquence d'un vieillissement prématuré.

[SOURCE: IEC 62340:2007, 3.15]

3.21
fonction de sûreté
objectif spécifique devant être réalisé pour la sûreté d'une installation nucléaire ou d'une activité afin de prévenir ou atténuer les conséquences radiologiques du fonctionnement normal, des incidents de fonctionnement prévus et des conditions accidentelles

Note 1 à l'article: Une fonction de sûreté est exigée pour remplir les fonctions de sûreté fondamentales qui sont (i) la maîtrise de la réactivité, (ii) l'évacuation de la chaleur provenant du réacteur et de l'installation d'entreposage du combustible, (iii) le confinement des matières radioactives, la protection contre les rayonnements et la maîtrise des rejets radioactifs programmés, ainsi que la limitation des rejets radioactifs accidentels [AIEA SSR-2/1, Exigence 4]

Note 2 à l'article: Les fonctions de sûreté sont principalement celles mentionnées dans l'analyse de sûreté et comprennent les fonctions réalisées à tous les niveaux de défense en profondeur.

[SOURCE: Glossaire de sûreté de l'AIEA, 2018]

3.22
système
ensemble de composants qui interagissent conformément à une conception donnée, un élément d'un système pouvant être un autre système, appelé sous-système

Note 1 à l'article: Voir également "système d'I&C".

Note 2 à l'article: Les systèmes d'I&C se distinguent des systèmes mécaniques et électriques d'une centrale nucléaire.

Note 3 à l'article: Cette définition du SC 45A de l'IEC est totalement compatible avec la sous-définition de "système" donnée dans la définition de "SCC Systèmes, Structures et Composants" de l'édition 2018 du Glossaire de sûreté de l'AIEA.

[SOURCE: IEC 61513:2011, 3.56, modifié – Dans la Note 3 à l'article, la définition de l'édition 2007 du Glossaire de sûreté de l'AIEA a été mise à jour en regard de l'édition 2018.]

3.23
validation du système
confirmation par examen et apport d'autres éléments justificatifs qu'un système satisfait à la totalité des exigences spécifiées (fonctionnalités, temps de réponse, tolérance aux fautes, robustesse)

[SOURCE: IEC 61513:2011, 3.59]

3.24
défaut systématique
défaut du matériel ou du logiciel qui concerne systématiquement certains ou tous les composants d'un type particulier

Note 1 à l'article: Les défauts systématiques peuvent être le résultat d'erreurs de spécification ou de conception, de défauts de fabrication ou d'erreurs introduites durant les activités de maintenance.

Note 2 à l'article: Les composants contenant des défauts systématiques cachés peuvent avoir des défaillances aléatoires ou de façon coïncidente, suivant le type de défaut et les mécanismes associés qui sollicitent le défaut.

[SOURCE: IEC 62340:2007, 3.24]

3.25
défaillance matériel non détectée
défaillance matériel qui n'est pas automatiquement détectée par un système et qui n'est mise en évidence que par une tentative d'utilisation d'une fonction dépendant du matériel défaillant

Note 1 à l'article: De telles défaillances peuvent être découvertes par des essais fonctionnels, ou lorsqu'une demande relative à l'exploitation sollicite le système

3.26
vérification
confirmation par examen et apport d'éléments objectifs que les résultats d'une activité sont conformes aux objectifs et exigences établis pour cette activité

Note 1 à l'article: L'édition 2018 du Glossaire de sûreté de l'AIEA donne les deux définitions suivantes:

> Validation: Processus visant à déterminer si un produit ou un service est capable de remplir sa fonction prévue de façon satisfaisante. La validation (généralement d'un système) concerne la vérification par rapport à la spécification des exigences, tandis que la vérification (généralement d'une spécification de conception, d'une spécification d'essai ou d'un rapport d'essai) concerne le résultat d'un processus. La validation peut comporter un élément de jugement plus important que la vérification.
>
> Vérification: Processus visant à déterminer si la qualité ou les performances d'un produit ou d'un service sont conformes à celles indiquées, voulues ou exigées. La vérification est étroitement liée à la gestion et au contrôle de la qualité.

La définition de l'AIEA pour la "vérification" est très proche de celle de la "validation", et les deux s'intéressent au produit final ou au service.

Dans les normes du SC 45A de l'IEC, les termes "vérification" et "validation" font référence à des résultats provenant du cycle de vie de produits particuliers, à savoir les équipements et les systèmes d'I&C, mais en général pas à des services.

D'autre part, les termes "vérification" et "validation" sont utilisés pour identifier deux types d'évaluations différentes et complémentaires:

"Vérification" fait référence à une évaluation d'une activité individuelle par rapport à ses entrées.

"Validation" fait référence à une évaluation du produit final par rapport à ses objectifs et ses exigences documentés.

[SOURCE: IEC 61513:2011, 3.62, modifié – Dans la Note 1 à l'article, la définition de l'édition 2007 du Glossaire de sûreté de l'AIEA a été mise à jour en regard de l'édition 2018 et le contenu de la note a été adapté de manière cohérente.]

4 Symboles et termes abrégés

ATE	Automated Test Equipment (banc d'essai automatique)
BOM	Bill Of Materials (nomenclature des matériaux)
COTS	Commercial Off The Shelf (commercialement disponible sur étagère)
AMDE	Analyse des modes de défaillances et de leurs effets
AMDEC	Analyse des modes de défaillances, de leurs effets et de leur criticité
FPGA	Field Programmable Gate Array (réseau de portes programmable sur site)
AAP	Analyse par arbre de panne
HDL	Hardware Description Languages (langages de description de matériel)
HPD	HDL-Programmed Device (circuit intégré programmé en HDL)
ISA	International Society of Automation (société internationale d'automatisation)
NEMA	National Electrical Manufacturers Association (association nationale des fabricants de matériel électrique)
CNP	Centrale nucléaire de puissance
OMM	Operation and Maintenance Manual (guide d'exploitation et de maintenance)

5 Cycle de vie et de sûreté du matériel

5.1 Généralités

Le processus de production des systèmes d'I&C destinés aux centrales nucléaires est décrit dans l'IEC 61513 qui introduit le concept de cycle de vie et de sûreté des systèmes. Il s'agit d'un véhicule permettant de contrôler le processus de développement et dont l'adoption se traduit également par des preuves nécessaires pour justifier le bon fonctionnement des systèmes importants pour la sûreté. Il comprend et impose des exigences, mais ne dicte pas les modalités du projet à utiliser pour la production des systèmes (voir la Figure 1).

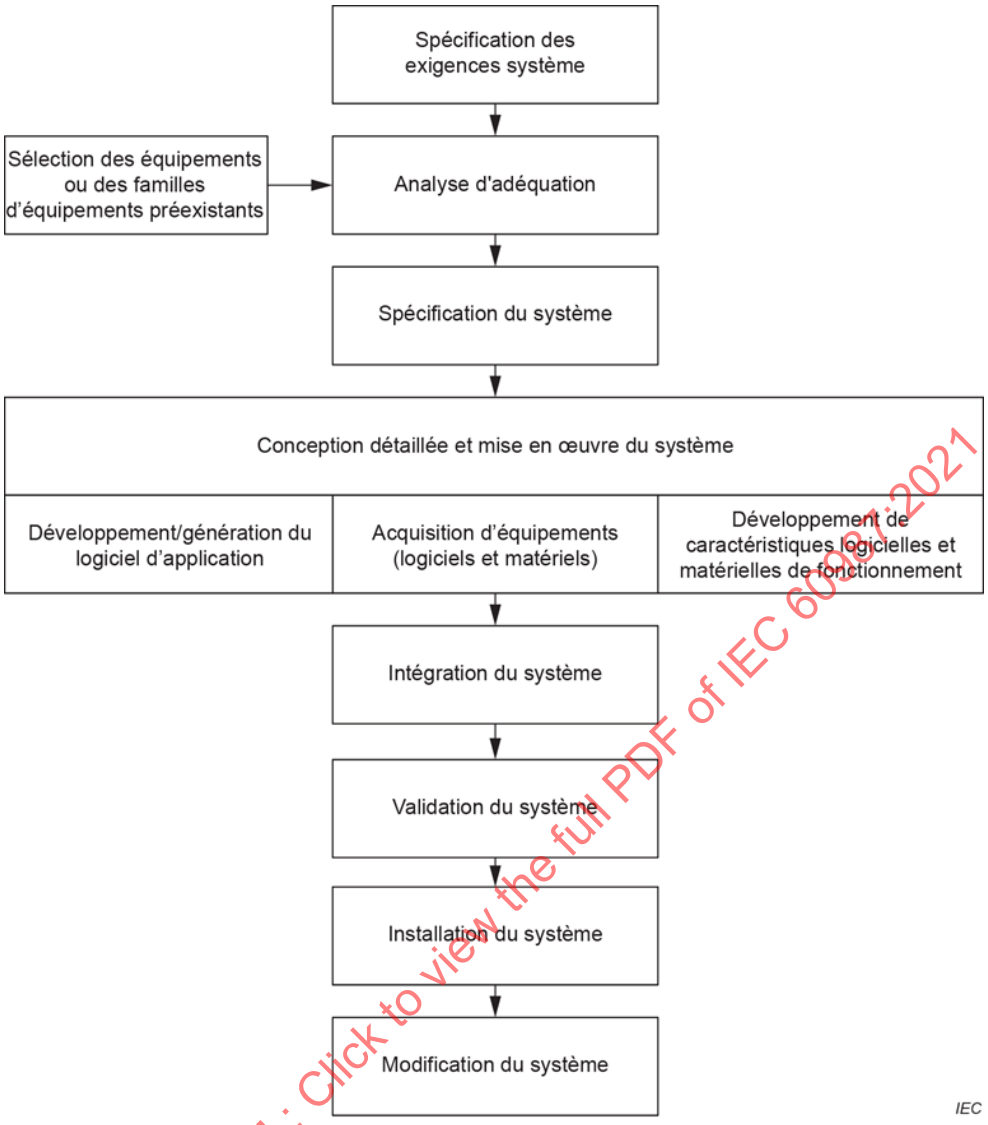


Figure 1 – Cycle de vie et de sûreté du système (informative, comme cela est défini par l'IEC 61513)

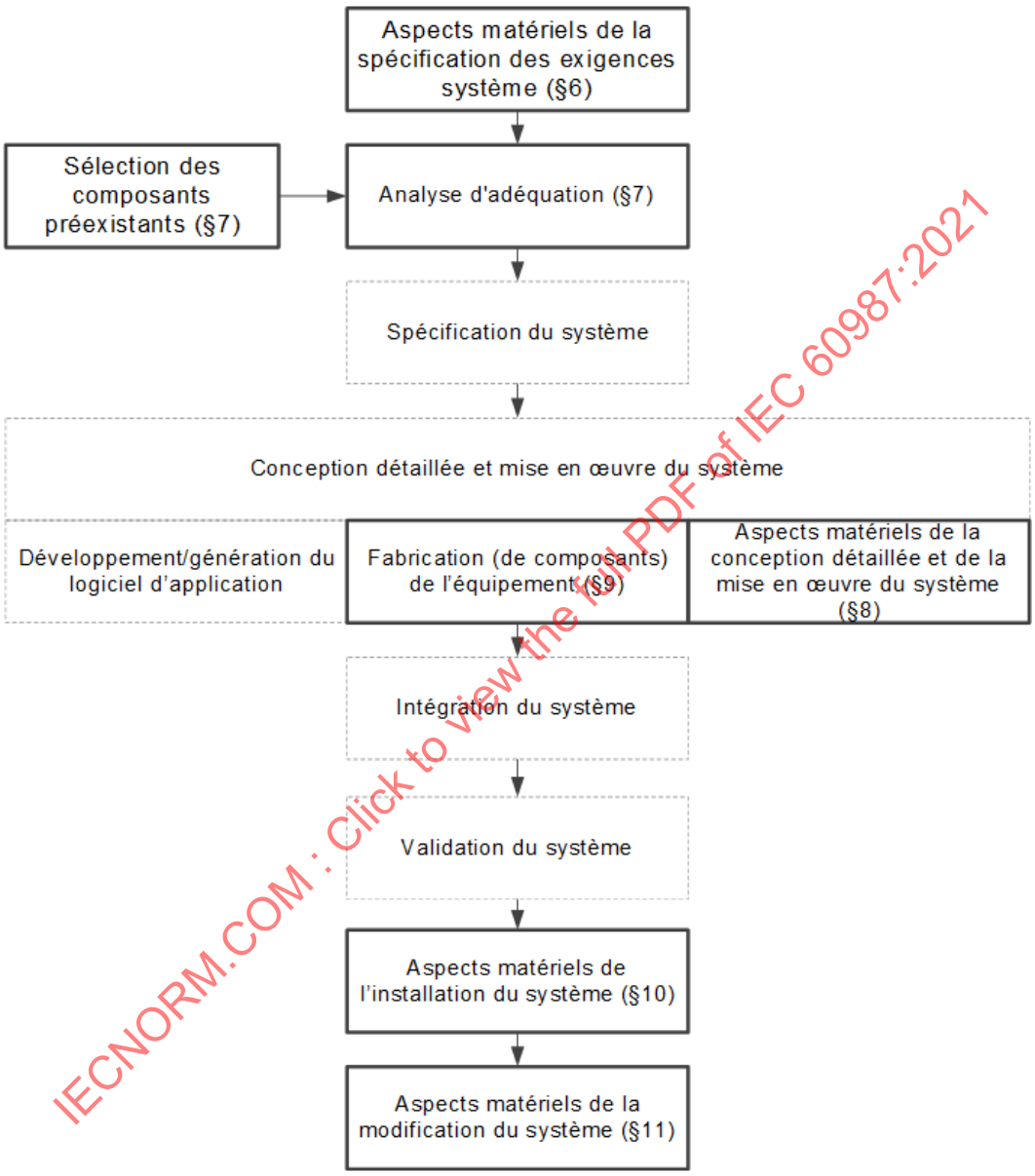
Le cycle de vie et de sûreté du système de l'IEC 61513 est complété par l'IEC 60880 (pour les fonctions de catégorie A) et IEC 62138 (pour les fonctions de catégories B et C) pour le développement de logiciels, par l'IEC 62566 (pour les fonctions de catégorie A) et IEC 62566-2 (pour les fonctions de catégories B et C) pour le développement HPD et par l'IEC 60987 pour le développement matériel des systèmes d'I&C de classe 1, 2 et 3.

Les équipements d'I&C, y compris les composants matériels, sont développés selon un cycle qui comprend des activités de développement couvrant la spécification des exigences, la conception et la mise en œuvre, la qualification, la fabrication, l'intégration et la validation, ainsi que des activités d'assurance qualité et de vérification.

Dans la plupart des cas, les fournisseurs d'I&C utilisent des composants préexistants et le cycle de vie et de sûreté du matériel est fortement intégré dans le cycle de vie et de sûreté du système. En particulier, la spécification des exigences matériel fait partie de la spécification des exigences système et de la conception du système ou en est directement dérivée.

Si nécessaire, le développement de nouveaux composants spécifiques peut être effectué en parallèle de l'application spécifique à la centrale. Dans ce cas, le développement et la qualification sont effectués à l'avance ou avec certains chevauchements avec le projet.

La Figure 2 présente la relation entre les activités du cycle de vie et de sûreté du matériel et les activités du cycle de vie et de sûreté du système.



NOTE Les cases en fines lignes pointillées représentent les activités du système qui ne sont pas traitées dans le présent document.

Figure 2 – Activités liées au matériel dans le cycle de vie et de sûreté des systèmes

Les activités de planification supplémentaires suivantes, non représentées à la Figure 2 soutiennent également le cycle de vie et de sûreté du matériel:

– assurance qualité;
– vérification;
– gestion de la configuration.

L'exploitation et la maintenance qui ne sont pas représentées à la Figure 2 sont également traitées dans le présent document.

La qualification aux conditions d'environnement n'est pas représentée à la Figure 2 et n'est pas traitée par le présent document. Les systèmes d'I&C doivent être soumis à l'essai et qualifiés aux conditions d'environnement conformément aux exigences applicables de l'IEC/IEEE 60780-323 complétée par l'IEC 60980 lorsqu'il est nécessaire que le système d'I&C soit résistant aux séismes.

Il est nécessaire, si l'environnement opérationnel et l'IEC 62003 l'exigent, de spécifier le degré d'immunité aux interférences électromagnétiques. Il est nécessaire de spécifier les exigences électromagnétiques par rapport à des estimations réalistes des conditions de fonctionnement en prenant en considération les circonstances crédibles les plus défavorables.

Il est nécessaire que les essais du degré d'immunité aux interférences électromagnétiques soient exécutés conformément aux normes applicables de la série IEC 61000.

5.2 Cycle de vie et de sûreté du matériel pour la classe 1 et la classe 2

5.2.1 Structure du projet pour la classe 1 et la classe 2

5.2.1.1 Le cycle de vie et de sûreté du matériel doit être compatible avec l'ensemble du cycle de vie et de sûreté du système.

Le projet de développement d'un nouveau module peut être un projet autonome et géré séparément du développement de l'équipement d'I&C dans lequel il est destiné à être intégré. Aujourd'hui, il s'agit d'une situation typique pour laquelle la plupart des modules intégrés dans le système d'I&C sont des modules prédéveloppés faisant partie d'une famille d'équipements génériques fournis par les fournisseurs d'I&C.

5.2.1.2 Chaque phase du cycle de vie et de sûreté du matériel doit être constituée d'activités bien définies et bien documentées.

5.2.1.3 Il convient que chaque phase constitue en quelque sorte une entité, même si celle-ci dépend d'autres phases pour les entrées et qu'elle produise des sorties utilisées par d'autres phases.

NOTE Il est considéré que les différentes phases du projet forment ensemble un cycle de vie et de sûreté global (voir l'Article 5 de l'IEC 61513 qui fournit les exigences applicables aux cycles de vie et de sûreté des systèmes). L'IEC 61513 admet le déroulement des phases en parallèle tant que l'intégrité du cycle de vie et de sûreté du système n'est pas compromise.

5.2.1.4 Chaque phase doit comprendre la production d'une documentation, y compris les hypothèses ou les limites à appliquer à l'équipement d'I&C, avant le début de la phase de développement suivante.

5.2.1.5 Chaque phase doit se terminer en réalisant la vérification (voir 5.2.3).

5.2.1.6 Chacune des activités doit être programmée pour assurer qu'un temps suffisant soit prévu pour:

– les interactions entre les phases de développement nécessaires pour les matériels, les HPD ou les logiciels, pour assurer la compatibilité entre le matériel, les logiciels et le HPD du système;

– la production de la documentation et réalisation des activités d'essai, de vérification et d'assurance qualité.

5.2.2 Gestion de la qualité pour la classe 1 et la classe 2

5.2.2.1 Un plan d'assurance qualité pour les aspects matériels doit exister ou bien comme document(s) séparé(s) ou bien en tant que partie d'un document décrivant un programme d'assurance qualité.

5.2.2.2 Il convient d'inclure dans le plan d'assurance qualité toutes les activités qualité liées au matériel et faisant partie du cycle de vie et de sûreté du matériel.

5.2.2.3 Le plan d'assurance qualité doit exiger que des ressources adéquates (par exemple, ressources humaines, budgets), des moyens adéquats (c'est-à-dire pièces de rechange, dispositifs pour les essais et la maintenance, etc.) et des environnements de travail adéquats (c'est-à-dire laboratoires, ateliers, espace de travail) soient fournis pour exécuter les tâches associées à chaque phase du cycle de vie et de sûreté du matériel.

5.2.2.4 Le plan d'assurance qualité doit exiger que la mise en œuvre de chaque activité soit confiée à des personnes compétentes.

5.2.2.5 Le plan d'assurance qualité doit couvrir les phases suivantes, lorsque celles-ci sont pertinentes pour un système ou un développement:

– les aspects matériels de la spécification des exigences système;
– la sélection des composants préexistants;
– les aspects matériels de la conception détaillée et de la mise en œuvre du système;
– la fabrication d'équipements (composants);
– les aspects matériels de l'installation du système;
– les aspects matériels de la modification du système.

5.2.2.6 Il convient que le ou les plans d'assurance qualité décrivent l'organisation, la gestion et la réalisation des activités liées à la qualité, ceci comprenant, selon le cas:

– le processus de conception;
– le contrôle de la configuration de la documentation;
– le contrôle des instructions de montage, des procédures, des schémas;
– le processus d'approvisionnement des biens et des services;
– le contrôle des matériaux et des éléments utilisés pour fabriquer le matériel du système;
– les activités de contrôle de la qualité, par exemple des inspections formelles;
– le contrôle des équipements et des outils d'essai;
– le contrôle de l'envoi, du stockage et de la manutention du matériel;
– le processus d'essai;
– le suivi des non-conformités et les actions correctives correspondantes;
– la procédure d'archivage des rapports d'assurance qualité;
– les procédures d'audit interne et externe.

5.2.3 Vérification du matériel pour la classe 1 et la classe 2

5.2.3.1 Exigences générales pour la classe 1 et la classe 2

Le processus de conception détaillée et de mise en œuvre doit comprendre des contrôles formels pour vérifier que les produits de la conception matériel associés à chaque phase satisfont aux exigences élaborées lors de la phase précédente.

NOTE Il est généralement considéré que le processus de vérification du matériel débute avec la vérification des spécifications des exigences matériel par rapport aux spécifications des exigences système. Il se termine lorsque

le logiciel et le HPD ont été intégrés avec le matériel. L'IEC 60880 et l'IEC 62138, l'IEC 62566 et l'IEC 62566-2 fournissent des exigences pertinentes relatives aux phases de l'intégration matériel/logiciel/HPD.

5.2.3.2 Plan de vérification pour la classe 1 et la classe 2

5.2.3.2.1 Un plan de vérification doit être préparé pour définir l'approche retenue pour vérifier la conception matériel et contrôler l'application correcte du processus de vérification. Le plan peut faire partie d'un plan de vérification global.

5.2.3.2.2 Ce plan doit être préparé avant le début des actions de vérification.

5.2.3.2.3 Il convient que le ou les plans documentent l'organisation retenue, le personnel impliqué, la structure organisationnelle, les méthodes de vérification employées, le niveau de vérification à atteindre, les plannings et toutes autres activités significatives pour le projet et liées à la vérification.

5.2.3.2.4 Les actions de vérification doivent avoir lieu uniquement lorsque les produits de conception (par exemple, documents, composants) sont mis à disposition, par le personnel de conception, pour vérification et lorsque la documentation correspondante est enregistrée dans un environnement dédié à un contrôle formel des configurations.

Une prévérification informelle peut être effectuée en parallèle avec le processus de conception afin que les erreurs puissent être détectées et corrigées au plus tôt (à condition que les dispositions adéquates de contrôle de la configuration soient assurées).

5.2.3.2.5 Après mise à disposition pour vérification, le processus de modification de la conception doit assurer que toutes les modifications ultérieures de la conception matériel soient vérifiées de façon appropriée (par exemple, tel qu'exigé par l'Article 11).

5.2.3.3 Indépendance de la vérification du matériel pour la classe 1 et la classe 2

5.2.3.3.1 Le plan de vérification doit être élaboré et mis en œuvre par des personnes qui n'ont pas participé à la conception.

5.2.3.3.2 Pour la vérification de classe 1, il convient que les vérificateurs soient hiérarchiquement indépendants des concepteurs matériel; par exemple ils peuvent être dans différents départements de la même organisation.

5.2.3.3.3 Le personnel de vérification doit être compétent.

5.2.3.3.4 La vérification doit se dérouler conformément à des procédures documentées.

5.2.3.3.5 Tout élément découvert à la vérification et toutes réponses de l'équipe de conception associées à cet élément doivent être formellement documentés.

5.2.3.3.6 Pour la classe 1, lorsqu'un ATE est utilisé et exécute automatiquement les essais, l'indépendance doit être assurée entre:

– les concepteurs du matériel et les développeurs des scénarios d'essai;
– les concepteurs du matériel et le personnel chargé d'effectuer les essais et d'évaluer les résultats des essais.

5.2.3.3.7 Pour la classe 2, lorsqu'un ATE est utilisé et exécute automatiquement les essais, l'indépendance doit être assurée entre:

– les concepteurs du matériel et les développeurs des scénarios d'essai;
– les concepteurs du matériel et le personnel chargé d'évaluer les résultats des essais.

5.2.3.4 Méthodes de vérification pour la classe 1 et la classe 2

5.2.3.4.1 Les bases sur lesquelles repose le choix de la ou des méthodes de vérification doivent être documentées avec suffisamment de détails pour pouvoir être auditées par des personnes qui n'ont pas pris part directement aux activités de conception et de vérification.

NOTE Les examens essentiels, les audits, les analyses, les essais manuels ou les essais effectués à l'aide de l'ATE sont des exemples typiques de méthodes de vérification.

5.2.3.4.2 Lorsqu'est choisie une méthode de vérification adaptée, les questions suivantes doivent être prises en considération:

– le classement de sûreté du système (par exemple la classe 1 exigeant l'emploi des techniques les plus rigoureuses);
– les revues documentées et les essais qui seront réalisés sur le logiciel/matériel/HPD intégrés, comme partie intégrante des processus de vérification et de validation du système (par exemple pour éliminer de telles activités des processus de validation et de vérification, pour ne pas utiliser inefficacement des ressources par duplication du travail);
– des activités de vérification réalisées sur le matériel ou sur les systèmes intégrant le matériel (par exemple lorsqu'un matériel a été préqualifié avec rigueur);
– les caractéristiques de conception du système, par exemple la taille, la maturité/nouveauté des principes de conception utilisés, les modes de défaillance et la complexité;
– les données support qui peuvent être disponibles à partir d'autres sources, telles que celles obtenues des processus d'assurance qualité et de qualification environnementale.

5.2.3.4.3 Des outils et des méthodes doivent être disponibles en support aux essais des sous-systèmes et des composants et pour assurer que ces derniers puissent être rigoureusement soumis à l'essai.

5.2.3.4.4 Il convient d'utiliser des bancs d'essai automatiques pour améliorer la répétition et la précision des essais lorsque ceci est pertinent.

5.2.3.4.5 Les moyens d'essai utilisés durant la vérification ou le processus d'essai doivent être étalonnés pour garantir la précision de mesure lorsque le critère d'acceptation de l'essai dépend de la valeur mesurée. Dans ce cas, des procédures doivent assurer que seuls des appareils de mesure étalonnés soient utilisés.

5.2.3.4.6 Les outils d'essai fonctionnant avec un logiciel doivent être validés avant utilisation et doivent être soumis à un contrôle de configuration.

NOTE La validation des outils d'essai fonctionnant avec un logiciel repose sur la documentation de l'utilisateur et l'adéquation par rapport aux exigences d'essai.

5.2.3.4.7 Les résultats de tous les essais formels doivent être enregistrés (les essais informels peuvent être réalisés durant le processus de conception en tant que précurseurs des essais formels). Des enregistrements des essais formels susceptibles d'être audités, suffisants pour démontrer que tous les essais ont été réalisés et que chaque non-conformité d'essai a été gérée de façon satisfaisante, doivent être disponibles.

5.2.3.5 Documentation de vérification pour la classe 1 et la classe 2

5.2.3.5.1 Les enregistrements relatifs aux activités de vérification, susceptibles d'être audités, doivent contenir le plan de vérification, les procédures d'essai, les résultats d'essai, les enregistrements correspondant aux modifications de conception et la documentation associée aux non-conformités découvertes durant le processus de vérification matériel (ceci avec les enregistrements prouvant que chaque non-conformité a été gérée).

5.2.3.5.2 Les procédures d'essai doivent être écrites clairement, elles doivent fournir des instructions étape par étape pour la vérification matériel et qu'elles contiennent des informations détaillées sur la préparation des essais.

5.2.3.5.3 Les procédures d'essai doivent contenir des critères de réussite/échec de l'essai non ambigus.

5.2.3.5.4 Lorsque les procédures d'essai sont mises en œuvre par un logiciel, la version du logiciel doit être incluse dans la documentation.

5.2.3.6 Gestion des non-conformités pour la classe 1 et la classe 2

5.2.3.6.1 Les non-conformités découvertes durant le processus de vérification doivent être formellement documentées et transmises aux bonnes personnes pour traitement.

5.2.3.6.2 Les réponses doivent être formellement documentées de façon à laisser une trace prouvant que toutes les non-conformités ont été traitées et que tous les défauts de conception identifiés ont été corrigés ou acceptés.

5.2.3.6.3 Lorsque des défauts de conception sont acceptés, toutes les modifications induites sur le système de documentation doivent être complètement intégrées.

5.3 Cycle de vie et de sûreté du matériel pour la classe 3

5.3.1 Structure du projet et gestion de la qualité pour la classe 3

5.3.1.1 Le cycle de vie et de sûreté du matériel doit être compatible avec l'ensemble du cycle de vie et de sûreté du système.

Le projet de développement d'un nouveau module peut être un projet autonome et géré séparément du développement de l'équipement d'I&C dans lequel il est destiné à être intégré. Aujourd'hui, il s'agit d'une situation typique pour laquelle la plupart des modules intégrés dans le système d'I&C sont des modules prédéveloppés faisant partie d'une famille d'équipements génériques fournis par les fournisseurs d'I&C.

5.3.1.2 Il convient que chaque phase constitue en quelque sorte une entité, même si celle-ci dépend d'autres phases pour les entrées et qu'elle produise des sorties utilisées par d'autres phases.

NOTE Il est considéré que les différentes phases du projet forment ensemble un cycle de vie et de sûreté global (voir l'Article 6 de l'IEC 61513 qui fournit les exigences applicables aux cycles de vie et de sûreté des systèmes). L'IEC 61513 admet le déroulement des phases en parallèle tant que l'intégrité du cycle de vie et de sûreté du système n'est pas compromise.

5.3.1.3 Il convient que chaque phase comprenne la production d'une documentation, y compris les hypothèses ou les limites à appliquer à l'équipement d'I&C, avant le début de la phase de développement suivante.

5.3.1.4 Un plan d'assurance qualité pour les aspects matériels doit exister ou bien comme document(s) séparé(s) ou bien en tant que partie d'un document décrivant un programme d'assurance qualité.

5.3.1.5 Le plan d'assurance qualité doit couvrir les phases suivantes, lorsque celles-ci sont pertinentes pour un système ou un développement:

– les aspects matériels de la spécification des exigences système;
– la sélection des composants préexistants;
– les aspects matériels de la conception détaillée et de la mise en œuvre du système;
– la fabrication d'équipements (composants);
– les aspects matériels de l'installation du système;

– les aspects matériels de la modification du système.

5.3.2 Vérification du matériel pour la classe 3

5.3.2.1 Le processus de conception et de mise en œuvre doit comprendre des contrôles pour vérifier que les produits de la conception matériel associés à chaque phase de la conception et de la mise en œuvre satisfont aux exigences élaborées lors de la phase précédente.

NOTE Il est généralement considéré que le processus de vérification du matériel débute avec la vérification des spécifications des exigences matériel par rapport aux spécifications des exigences système. Il se termine lorsque le logiciel et le HPD ont été intégrés avec le matériel. L'IEC 60880 et l'IEC 62138, l'IEC 62566 et l'IEC 62566-2 fournissent des exigences pertinentes relatives aux phases de l'intégration matériel/logiciel/HPD.

5.3.2.2 Il convient que les non-conformités découvertes durant le processus de vérification soient formellement documentées et transmises au personnel compétent pour traitement.

5.3.2.3 Il convient que les enregistrements susceptibles d'être audités relatifs aux activités de vérification comprennent le plan de vérification, les procédures d'essai, les résultats d'essai, les enregistrements des modifications de conception et le traitement des non-conformités.

6 Aspects matériels de la spécification des exigences système

6.1 Aspects matériels de la spécification des exigences système pour la classe 1 et la classe 2

6.1.1 Exigences générales pour la classe 1 et la classe 2

6.1.1.1 Les exigences matériel doivent être spécifiées dans la spécification des exigences matériel ou dans le cadre d'une spécification plus large.

6.1.1.2 Les exigences matériel doivent être conformes à la spécification des exigences système (voir l'IEC 61513:2011, Article 6).

La spécification des exigences système est une description des aspects relatifs à la combinaison du matériel et aux aspects matériel/logiciel/HPD et énonce les objectifs de conception du système et les fonctions assurées par le système. Le système peut être entièrement développé pour une application particulière ou peut être fondé sur une famille d'équipement générique assemblée pour une application de projet spécifique.

La spécification des exigences matériel identifie les fonctions et les performances exigées du matériel, identifie les exigences de conception matériel, énonce les exigences de fiabilité du matériel, et énonce les exigences des conditions d'environnement matériel.

6.1.1.3 Les exigences matériel doivent être présentées selon des techniques ou des méthodes dont le format ne doit pas empêcher la lisibilité.

6.1.1.4 Les exigences matériel fonctionnelles doivent être non ambiguës, doivent pouvoir être soumises à l'essai et/ou vérifiables et doivent être atteignables.

6.1.1.5 En général, il convient que les exigences matériel spécifient ce qui doit être fait et non comment cela doit être fait.

Cependant, l'utilisation de composants préexistants peut avoir pour résultat, jusqu'à un certain niveau, une conception matériel ascendante.

6.1.2 Exigences fonctionnelles et de performances pour la classe 1 et la classe 2

6.1.2.1 Les exigences matériel fonctionnelles et de performance doivent être cohérentes avec les exigences fonctionnelles et de performances du système.

6.1.2.2 La conformité aux exigences système des exigences matériel fonctionnelles et de performances, combinées aux exigences des éléments câblés ou aux exigences des éléments numériques programmables (autant que nécessaire pour couvrir toutes les exigences matériel) doit être vérifiée.

6.1.2.3 Les exigences matériel fonctionnelles doivent au minimum comprendre, les définitions pour:

– les objectifs assignés au matériel pour le système dans son ensemble et au matériel de chaque sous-ensemble;
– les nombres et les types de capteurs et d'actionneurs à connecter au système;
– les nombres et les types d'appareils relatifs à l'interface homme/machine tels que les afficheurs, les imprimantes et les claviers.

6.1.2.4 Chaque composant ou sous-système livré par un fournisseur et qui doit être intégré dans le système doit:

– être accompagné d'une spécification qui couvre tous les aspects de sûreté de la performance de cet élément; ou
– être accompagné d'une analyse qui détermine les caractéristiques de conception matériel du composant de façon à pouvoir confirmer son adéquation.

6.1.2.5 Les exigences de performances matériel doivent contenir (cela est applicable à toute application particulière):

– le taux d'acquisition de données exigé;
– la capacité de traitement de données exigée;
– la puissance de calcul exigée;
– les interfaces de communication exigées (protocoles, vitesse de transmission);
– la précision exigée sur les conversions et les calculs;
– la capacité exigée en matière d'élimination du bruit des signaux;
– les temps de réponse exigés;
– les limitations concernant les dimensions physiques;
– les exigences spatiales (par exemple les longueurs des lignes de transmission de données);
– les quantités de pièces de rechange exigées (si exigé);
– les conditions d'environnement opérationnel;
– les exigences concernant l'alimentation électrique.

6.1.2.6 Les contraintes relatives aux interfaces matérielles avec d'autres systèmes doivent être spécifiées dans la spécification des exigences matériel ou dans un document de portée plus large.

Les 6.2.2.3.2, 6.2.2.4, 6.2.2.5, 6.2.3.3.3.3 et 6.2.3.3.4 de l'IEC 61513:2011 fournissent des exigences relatives aux interfaces système qui visent à assurer une intégration correcte et à empêcher la propagation des défaillances entre les interfaces des systèmes.

6.1.2.7 Toutes les contraintes imposées sur la conception matériel par les conceptions logiciel/HPD ou système doivent être établies.

6.1.3 Exigences de fiabilité pour la classe 1 et la classe 2

6.1.3.1 Les exigences de fiabilité du matériel doivent être définies et doivent être cohérentes avec les exigences de fiabilité globales du système.

NOTE Dans ce contexte, la fiabilité du matériel concerne les défauts aléatoires et exclut toute considération de défauts systématiques.

6.1.3.2 Il convient que les exigences de fiabilité/disponibilité du matériel incluent une description des types de défaillance qui doivent être tolérés sans perte ou avec une perte limitée définie des fonctions.

6.1.3.3 Il convient que les exigences matériel donnent des objectifs chiffrés pour les paramètres de fiabilité matériel (tels que le temps moyen entre défaillances (détectées), le temps moyen entre défaillances (non détectées), le temps moyen de réparation pour les défaillances détectées).

6.1.3.4 Il convient d'établir toutes les exigences de fiabilité devant être étayées par des analyses détaillées de la conception matériel (par exemple des analyses au niveau des composants, du module ou du sous-ensemble).

6.1.3.5 Les exigences de maintenance doivent être définies de manière à assurer la fiabilité exigée pendant la durée de vie du système d'I&C.

6.1.3.6 Les exigences de maintenance doivent couvrir (cela est applicable à chaque système particulier):

– les exigences pour l'exploitation du système durant les activités de maintenance;
– le remplacement des éléments consommables, par exemple les filtres à air, les batteries;
– toutes les exigences relatives au remplacement préventif des sous-systèmes, des modules et/ou des composants;
– toute exigence concernant les essais périodiques, y compris la périodicité;
– des mesures visant à prévenir les erreurs de maintenance susceptibles de conduire à des DCC;
– le domaine de la revalidation système (par exemple les essais) exigée après une activité de maintenance matériel.

6.1.3.7 Il convient de définir les exigences de maintenance lors de la spécification des exigences matériel et, si elles ne peuvent pas être définies en détail au cours de cette phase, il convient de les finaliser à un stade ultérieur, avant l'installation du système.

6.1.4 Exigences relatives aux conditions d'environnement pour la classe 1 et la classe 2

6.1.4.1 Les exigences matériel relatives aux conditions d'environnement doivent identifier les contraintes auxquelles le système d'I&C peut être soumis et prendre en compte les niveaux physiques correspondants, le cas échéant.

NOTE Les contraintes typiques sont les conditions climatiques, de vieillissement, sismiques, chimiques, électriques, de CEM et de rayonnement.

6.1.4.2 Les plages normales et extrêmes de conditions d'environnement auxquelles le système doit résister doivent être spécifiées conformément aux contraintes imposées dans le cadre de conception de la centrale (voir 5.2.4 de l'IEC 61513:2011).

6.1.4.3 Il convient d'y inclure toutes exigences particulières liées au stockage, à l'installation et à la mise en service.

6.1.5 Exigences de fabrication pour la classe 1 et la classe 2

Les exigences matériel doivent identifier en particulier:

– Tous les matériaux de construction interdits et toutes les exigences relatives à l'utilisation de matériaux particuliers;
– Les types particuliers de procédés de fabrication;
– Les critères minimaux d'acceptabilité IPC-A-610 (voir 9.1.6.4).

6.1.6 Exigences documentaires pour la classe 1 et la classe 2

Les exigences documentaires pour le matériel doivent faire partie des exigences documentaires du système d'I&C (voir l'IEC 61513).

L'Annexe A identifie la documentation type pour chacun des principaux articles du présent document.

6.2 Aspects matériels de la spécification des exigences système pour la classe 3

6.2.1 Exigences générales pour la classe 3

6.2.1.1 Les exigences matériel doivent être spécifiées dans la spécification des exigences matériel ou dans le cadre d'une spécification plus large.

6.2.1.2 Il doit être assuré que la spécification des exigences matériel satisfasse aux exigences exprimées dans la spécification des exigences système en matière de:

– fonctionnalité;
– fiabilité;
– conditions d'environnement opérationnel;
– fabrication (par exemple, matériaux de construction interdits, critères d'acceptabilité minimum IPC-A-610 (voir 9.2.5), interchangeabilité).

6.2.1.3 Il convient que chaque composant ou sous-système livré par un fournisseur et qui doit être intégré dans le système soit accompagné d'une analyse suffisamment détaillée des caractéristiques de conception matériel du composant pour confirmer son adéquation comme cela est indiqué en 7.2.

6.2.2 Fiabilité pour la classe 3

Si elle est exigée pour appuyer l'analyse de fiabilité de niveau système, une analyse des défaillances matériel potentielles doit être exigée dans la spécification des exigences matériel.

6.2.3 Exigences relatives aux conditions d'environnement pour la classe 3

Les exigences matériel relatives aux conditions d'environnement doivent identifier les contraintes auxquelles le système d'I&C peut être soumis et prendre en compte les niveaux physiques correspondants, le cas échéant.

NOTE Les contraintes typiques sont les conditions climatiques et électriques.

6.2.4 Exigences documentaires pour la classe 3

Les exigences documentaires pour le matériel doivent faire partie des exigences documentaires du système d'I&C (voir l'IEC 61513).

L'Annexe A identifie la documentation type pour chacun des principaux articles du présent document.

7 Sélection des composants préexistants

7.1 Sélection de composants préexistants pour la classe 1 et la classe 2

7.1.1 Une analyse d'adéquation doit être effectuée et documentée pour démontrer que les composants préexistants utilisés dans l'équipement sont conformes aux exigences spécifiées définies en 6.1. L'analyse peut faire partie d'une analyse d'adéquation globale.

7.1.2 Outre cette analyse d'adéquation, des preuves de qualité doivent être fournies et être fondées sur:

– l'identification, les versions;
– les changements historiques et les enregistrements y afférents;
– les enregistrements de gestion de la qualité;
– les essais de type effectués par le fabricant;
– les normes ou les guides appliqués;
– l'expérience opérationnelle du fabricant.

7.1.3 Si l'analyse d'adéquation ou les preuves de qualité ont révélé un manque d'informations, des mesures compensatoires doivent être mises en place, par exemple des essais, des analyses, des justifications.

7.1.4 Si l'analyse d'adéquation a révélé des non-conformités, celles-ci doivent être traitées en modifiant la conception du matériel ou du système (tout en veillant à ce que les exigences relatives à la sûreté nucléaire ne soient pas compromises) ou en rejetant le composant de toute autre manière.

7.1.5 La conception des composants préexistants doit répondre à toutes les exigences spécifiques de maintenance résultant de la spécification des exigences matériel.

NOTE Ceci peut comprendre des procédures d'essai opérationnel, d'étalonnage, de réparation, de remplacement périodique et de maintenance.

7.1.6 Si la fiabilité du matériel n'est pas suffisante pour atteindre les objectifs exigés, des mesures compensatoires doivent être prises.

NOTE Ces mesures peuvent inclure des améliorations de la conception ou des changements liés à l'exploitation en service (comme l'augmentation de la fréquence des essais périodiques).

7.1.7 Il convient d'être prudent lorsqu'il est décidé d'augmenter les essais périodiques, car toutes les opérations intrusives sur les équipements installés comportent un risque intrinsèque d'introduire directement ou indirectement des erreurs (par exemple, l'effet global des essais périodiques peut avoir une influence négative sur la sûreté). Idéalement, il convient d'effectuer les essais lorsque les défauts potentiels de la procédure d'essai ne peuvent pas avoir d'impact sur la sûreté, par exemple lors des arrêts de l'installation ou lorsque l'équipement soumis à l'essai est isolé du reste de l'installation.

7.1.8 Il convient d'évaluer la conception par rapport au risque d'erreurs humaines lors des activités d'exploitation et de maintenance (voir 8.1.4.3).

7.2 Sélection de composants préexistants pour la classe 3

7.2.1 Une analyse d'adéquation doit être effectuée et documentée pour démontrer que les composants préexistants utilisés dans l'équipement sont conformes aux exigences spécifiées définies en 6.2. L'analyse peut faire partie d'une analyse d'adéquation globale.

7.2.2 Outre cette analyse d'adéquation, des preuves de qualité doivent être fournies et être fondées sur:

– l'expérience opérationnelle du fabricant;
– et/ou les données fournies par les fabricants de modules électroniques (nature et résultats des essais en fin de fabrication, expérience opérationnelle, essais par échantillonnage, audits, compétences, certificats);
– et/ou les essais de type effectués par le fabricant.

7.2.3 Lorsque la preuve repose sur l'expérience opérationnelle du fabricant, elle doit être formalisée et fondée sur:

– les résultats d'inspection d'approvisionnement effectuée sur des lots successifs et permettant de vérifier la conformité et la variation des lots;
– et/ou les résultats d'essais sur des échantillons;
– et/ou des résultats opérationnels qui indiquent des défauts dans les composants d'équipement des modules, détectés soit par l'inspection effectuée pendant ou à la fin de la fabrication, soit par des retours de clients pour réparation.

8 Aspects matériels de la conception détaillée et de la mise en œuvre du système

8.1 Aspects matériels de la conception détaillée et de la mise en œuvre du système pour les classes 1 et 2

8.1.1 Exigences générales pour la classe 1 et la classe 2

8.1.1.1 Les aspects matériels de la conception détaillée du système et de sa mise en œuvre doivent découler de la spécification des exigences matériel.

8.1.1.2 Il convient que le processus de conception suive les phases de conception définies dans le plan de l'assurance qualité (voir 5.2.2), de manière à aboutir à la production d'un matériel conforme à la spécification des exigences matériel.

Le niveau d'activité de conception le plus général peut être appelé conception générale matériel, cela comprend l'analyse des différentes solutions de conception de façon à définir l'architecture système en matière de sous-systèmes et de modules.

La conception générale matériel est généralement suivie d'une ou de plusieurs étapes de conception détaillée.

8.1.1.3 Les activités de conception détaillée doivent développer la conception générale pour couvrir la conception détaillée des sous-systèmes, des modules et des composants de sorte que la description de la conception matériel soit suffisamment aboutie pour pouvoir être mise en œuvre.

Des prototypes du matériel peuvent être réalisés, non seulement pour démontrer le bon fonctionnement des modules matériel entre eux, mais aussi pour vérifier la compatibilité du matériel, du logiciel et du HPD.

8.1.1.4 Si la conception a lieu en une seule phase, cette phase doit comprendre la conception matériel détaillée.

8.1.2 Activités de conception pour la classe 1 et la classe 2

8.1.2.1 Les caractéristiques de performances du système dépendantes des performances du matériel doivent être prises en considération lors de la conception matériel, et il faut prouver, soit par analyse, soit par essai que la conception matériel satisfait à ses exigences (voir 6.1.2.5).

8.1.2.2 Toute non-conformité par rapport aux exigences matériel doit être gérée, soit en modifiant la conception, soit en analysant à nouveau les exigences (voir 5.2.3.6).

8.1.2.3 Les essais nécessaires pour démontrer que la performance exigée a été atteinte doivent être identifiés.

8.1.2.4 De tels essais peuvent être réalisés sur le matériel seul, ou bien réalisés lorsque le matériel est intégré avec le logiciel et/ou le HPD, par exemple comme une partie de la phase d'intégration système.

8.1.2.5 Les activités de maintenance exigées pour assurer que les exigences de fiabilité et de performance aient été atteintes tout au long de la durée de vie opérationnelle du matériel doivent être spécifiées. Il peut s'agir d'essais périodiques, d'étalonnage, de réparations, de maintenance préventive et corrective. Toutes ces activités doivent être documentées dans des procédures de maintenance.

8.1.2.6 Il convient de réaliser les activités de maintenance pour obtenir une confiance suffisante dans le bon fonctionnement du matériel et ainsi réduire au minimum les interventions humaines ou les activités intrusives sur le système, diminuant ainsi la probabilité de défauts introduits par des activités de maintenance.

8.1.2.7 Pour les équipements d'un système redondant ou plusieurs systèmes utilisés pour assurer une fonction de sûreté, il convient qu'une analyse prenne en considération les possibilités de défaillances de cause commune dues au matériel.

Les possibles causes entraînant l'introduction de défaillances de cause commune liées au matériel sont les suivantes:

– Activités de maintenance effectuées simultanément ou à la suite sur plusieurs équipements (en particulier lorsque ces activités peuvent introduire des pannes matérielles);
– Essais périodiques;
– Défauts cachés de conception matériel qui ne sont pas détectés pendant le cycle de vie du développement.

8.1.3 Fiabilité pour la classe 1 et la classe 2

8.1.3.1 Comme cela est exigé pour appuyer l'analyse de sûreté de niveau système, une analyse des défaillances matériel potentielles doit être réalisée lors de la conception.

8.1.3.2 La méthode utilisée pour réaliser les analyses de fiabilité du matériel doit être choisie en fonction des objectifs à atteindre.

Les exigences de fiabilité sont spécifiées dans la spécification des exigences matériel, conformément à 6.1.3.

Les méthodes qui peuvent être utilisées pour analyser la fiabilité du matériel du système comprennent:

– les AAP (analyses par arbre de panne), qui servent à identifier et à analyser les facteurs qui ont eu pour conséquence ou qui ont contribué à l'apparition d'un événement indésirable défini (voir l'IEC 61025 pour les recommandations concernant cette technique);
– les AMDE (analyses des modes de défaillance et de leurs effets), qui identifie les défaillances ayant des conséquences importantes sur les performances du système, par exemple, la fiabilité, la sûreté; voir l'IEC 60812 qui décrit un certain nombre de techniques pour réaliser des AMDE et des AMDEC (analyse des modes de défaillance, de leurs effets

et de leur criticité), et donne des conseils concernant l'application de ces méthodes selon les objectifs à atteindre;

– Pour les estimations des taux de défaillance utilisées comme données d'entrée pour l'AMDE/AMDEC, lorsqu'il existe des différences entre les conditions d'environnement finales et les conditions de référence, il est possible de trouver des recommandations pour corriger ces données, par exemple dans l'IEC 61709.

8.1.3.3 Pour les équipements de classe 1, une AAP ou une AMDE combinée avec les données de défaillance des composants doit être utilisée pour fournir des valeurs calculées de la fiabilité du matériel du système (voir IEC 61513), à moins que l'expérience d'exploitation soit suffisante pour donner une grande confiance dans l'atteinte des objectifs de fiabilité du matériel.

8.1.3.4 Pour les équipements de classe 2, la fiabilité du matériel du système doit être établie soit:

– par l'AAP ou l'AMDE combinée avec les données sur les défaillances des composants;

– par la justification d'une fiabilité adéquate fondée sur un raisonnement qualitatif, en particulier si la fiabilité du matériel du système n'est pas trop exigeante (par exemple, qualité des composants, redondance du matériel, expérience d'exploitation, proportion de défaillances matérielles révélées par rapport aux défaillances matérielles non révélées).

8.1.3.5 Il convient que la conception matériel réduise le plus possible l'impact potentiel des facteurs suivants sur la sûreté nucléaire:

– activités de maintenance;

– défaillance de système due à une défaillance aléatoire;

– défaillance matériel due à des conditions d'environnement.

8.1.3.6 Si la fiabilité matériel estimée est insuffisante pour les objectifs attendus, des mesures compensatoires doivent être prises, soit sous la forme d'améliorations de la conception, soit de modifications opérationnelles (telles qu'une augmentation de la fréquence des essais périodiques).

Lorsque l'option d'un essai périodique renforcé est choisie, il est nécessaire d'être prudent, car toute activité intrusive sur l'installation en exploitation comporte un risque intrinsèque d'introduction directe ou indirecte d'erreur (par exemple l'effet d'ensemble des essais périodiques peut avoir un impact négatif sur la sûreté). Idéalement, les essais doivent être réalisés lorsque les défauts potentiels du processus d'essai lui-même ne peuvent avoir d'impact sur la sûreté nucléaire, par exemple durant les arrêts de l'installation ou lorsque les matériels à soumettre à l'essai sont isolés de l'installation en fonctionnement.

Lorsque sont réalisées des évaluations probabilistes de sûreté en appui du rapport de sûreté de la CNP, les valeurs estimées de la fiabilité matériel (par exemple celles résultant d'une AAP) peuvent être utilisées dans l'analyse de la centrale et ainsi contribuer à la précision des calculs de fiabilité de l'installation dans son ensemble.

8.1.4 Maintenance pour la classe 1 et la classe 2

8.1.4.1 La conception matériel doit prendre en compte toutes les exigences spécifiques de maintenance provenant des spécifications d'exigences matériel.

8.1.4.2 Parmi tous les modules électroniques constituant un équipement, ceux qui sont réparables et ceux qui ne sont pas réparables doivent être identifiés comme tels.

8.1.4.3 De plus, dans la mesure du possible, il convient que la conception intègre des dispositions pour réduire le risque d'introduction de panne durant les activités de maintenance comme suit:

– un accès facile aux composants dont le remplacement est prévu en tant que consommables ou par suite de pannes;
– une identification claire des composants remplaçables afin que le personnel de maintenance puisse facilement vérifier que les bons composants de remplacement sont utilisés;
– l'utilisation de composants qui peuvent être remplacés sans intrusion sur le raccordement des câbles aux procédés de la centrale;
– prévoir un espacement suffisant entre les bornes;
– la mise à disposition de bornes dédiées pour réaliser les activités d'étalonnage ou d'essai (de sorte que le câblage d'exploitation ne doive pas être débranché pour faciliter la réalisation de ces activités);
– une conception matériel soutenue par un modèle structuré avec un étiquetage clair pour réduire le risque d'erreurs de maintenance.

8.1.5 Perte d'alimentation électrique pour la classe 1 et la classe 2

8.1.5.1 Conformément aux spécifications d'exigences matériel, le système d'I&C doit être conçu pour être insensible aux conséquences des pertes d'alimentation électriques de courte durée et aux variations de tension de l'alimentation électrique (tension/fréquence).

8.1.5.2 Des dispositions système doivent être prises pour avertir les opérateurs et le personnel de maintenance de telles fluctuations d'alimentation (ce rôle peut ne pas avoir été assigné au matériel et ainsi être hors du domaine d'application du présent document).

8.1.6 Documentation de conception pour la classe 1 et la classe 2

8.1.6.1 La documentation de conception matériel doit décrire la conception matériel et les moyens par lesquels les exigences matériel ont été satisfaites.

8.1.6.2 Il convient d'utiliser des formats normalisés pour la documentation de la conception matériel et des outils automatisés de conception matériel.

8.1.6.3 Il convient de mettre en place une hiérarchie de documents de conception matériel du système d'I&C constituée d'un certain nombre de "niveaux" documentaires.

8.1.6.4 Il convient de spécifier pour chaque niveau de la documentation de conception matériel les aspects de conception pertinents pour ce niveau et de définir les exigences matériel pour les niveaux inférieurs ou de prendre en compte les caractéristiques matériel du niveau inférieur.

8.1.6.5 La documentation de conception matériel doit définir l'architecture matériel, c'est-à-dire la structure et les relations entre les différentes parties du système.

8.1.6.6 Il convient que la documentation de conception matériel intègre une représentation globale du matériel à l'aide de schémas de principe représentant les sous-systèmes et les modules de niveaux inférieurs.

8.1.6.7 Il convient aussi d'y intégrer les exigences matériel pour la conception matériel détaillée, telles que:

– le nombre et le type de processeurs principaux ou autres;
– les exigences matériel relatives à la mémoire informatique;
– le nombre et le type des HPD;
– le nombre et le type des interfaces;
– le nombre et le type de bus et de liaisons de données.