# IEC 62671

Edition 1.0 2013-02

# INTERNATIONAL STANDARD

# NORME INTERNATIONALE

## Nuclear power plants – Instrumentation and control important to safety – Selection and use of industrial digital devices of limited functionality

## Centrales nucléaires de puissance – Instrumentation et contrôle-commande importants pour la sûreté – Sélection et utilisation des appareils numériques à fonctionnalités limitées

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

Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00
info@iec.ch
www.iec.ch

## About the IEC

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

## About IEC publications

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

**Useful links:**

IEC publications search - www.iec.ch/searchpub

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It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished

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

Electropedia - www.electropedia.org

The world's leading online dictionary of electronic and electrical terms containing more than 30 000 terms and definitions in English and French, with equivalent terms in additional languages. Also known as the International Electrotechnical Vocabulary (IEV) on-line.

Customer Service Centre - webstore.iec.ch/csc

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

---

## A propos de la CEI

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

## A propos des publications CEI

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

**Liens utiles:**

Recherche de publications CEI - www.iec.ch/searchpub

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

Just Published CEI - webstore.iec.ch/justpublished

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

Electropedia - www.electropedia.org

Le premier dictionnaire en ligne au monde de termes électroniques et électriques. Il contient plus de 30 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans les langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (VEI) en ligne.

Service Clients - webstore.iec.ch/csc

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

# IEC 62671

Edition 1.0 2013-02

# INTERNATIONAL STANDARD

# NORME INTERNATIONALE

## Nuclear power plants – Instrumentation and control important to safety – Selection and use of industrial digital devices of limited functionality

## Centrales nucléaires de puissance – Instrumentation et contrôle-commande importants pour la sûreté – Sélection et utilisation des appareils numériques à fonctionnalités limitées

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

PRICE CODE
CODE PRIX XA

ICS 27.120.20

ISBN 978-2-83220-630-0

# CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

# NUCLEAR POWER PLANTS – INSTRUMENTATION AND CONTROL IMPORTANT TO SAFETY – SELECTION AND USE OF INDUSTRIAL DIGITAL DEVICES OF LIMITED FUNCTIONALITY

## 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 62671 has been prepared by subcommittee 45A: Instrumentation and control of nuclear facilities, of IEC technical committee 45: Nuclear instrumentation.

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

| FDIS | Report on voting |
|---|---|
| 45A/898/FDIS | 45A/907/RVD |

Full information on the voting for the approval of this standard can be found in the report on voting indicated in the above table.

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.

The committee has decided that the contents of this publication will remain unchanged until the stability date indicated on the IEC web site under "http://webstore.iec.ch" in the data related to the specific publication. At this date, the publication will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

# INTRODUCTION

## a) Technical background, main issues and organisation of the Standard

This IEC standard specifically focuses on the selection and evaluation of pre-developed dedicated devices of limited, specific functionality and limited configurability for use in a nuclear power plant, where these devices incorporate either software or digital circuit designs specified using hardware description languages and where these devices have been produced to a recognized non-nuclear standard, but not to the SC 45A series of standards.

It is intended that the Standard be used by designers of NPPs, operators of NPPs (utilities), systems evaluators and by licensors.

The focus of this standard is on two aspects that are not addressed by other standards in the IEC SC 45A series:

- Other standards address the hardware aspects of devices containing software, or address complex devices such as PLCs containing software where that software has the potential to be much more complex[1] than in the devices covered by this standard, and
- Other standards focus on devices to be designed specifically for nuclear applications, whereas this standard focuses on the considerations necessary to apply devices in NPPs that have not been designed for nuclear use.

Designers of I&C systems for NPPs are increasingly forced to turn to such devices because of reasons such as equipment obsolescence, the small size of the nuclear market as compared to the industrial market, and the growing number of suppliers who choose to design to general safety standards such as IEC 61508.

Hence it has become vital for designers of these systems to have the guidance provided by this standard to be able to select and evaluate candidate devices for their suitability to applications in NPPs. This standard provides such guidance without which I&C designers would be required to consider how to interpret IEC 60880, IEC 62138 or IEC 62566 for this purpose.

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

IEC 61513 is a first level IEC SC 45A document and gives guidance applicable to I&C at the system level. It is supplemented by guidance at the device level by IEC 60987 for design of hardware, by IEC 60880 and IEC 62138 for software and by IEC 62566 for potentially complex devices. All of these standards focus on nuclear-specific designs and apply the concept of a life cycle.

IEC 62671 is a second level IEC SC 45A document tackling the specific issue of selecting and evaluating devices for use in NPPs where the candidate devices have been designed for non-nuclear use (and possibly certified as compliant with a widely-accepted general safety standard such as IEC 61508). Additionally, IEC 62671 addresses only devices that have dedicated limited and specific functionality, and limited configurability.

IEC 62671 is to be read in association with IEC 60880 (informative), IEC 62138 (informative), IEC 60987 (informative) and IEC 62566 (informative) which are the other appropriate IEC SC 45A documents which provide guidance on computer-based systems performing functions important to safety in NPPs.

---

1 There is no agreed upon definition of “complexity”, but where devices support more functionality, there are associated increases in volume of code, contention for system resources, and timing-related phenomena that can lead to unexpected failures of the device. This standard addresses these problems by covering only devices with very restricted functionality.

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 systems of class 1, 2 or 3.

Aspects for which specific requirements have been provided in this Standard are:

- The use of a planned process to select, and then evaluate candidate devices for use, as well as to include considerations of the integration of the device into plant systems.
- Criteria for evaluating the functional suitability of a device that contains embedded software or uses digital circuits designed with software-based tools such as HDL (Hardware Description Language).
- Criteria to consider and balance in an overall evaluation to obtain an appropriate level of assurance that the device will perform as specified when called upon.
- Considerations for the safe application of the selected device in plant systems.

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 technologies.

Throughout this standard, the emphasis is on the review of evidence of the processes in place at the designer and the manufacturer (who may be different organisations) since they are the organisations that impact the acceptability of the candidate device for its intended application. This evidence may have to be obtained through the supplier with whom the end user has direct contact.

**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 document of the IEC SC 45A standard series is IEC 61513. It provides general requirements for I&C systems and equipment that are used to perform functions important to safety in NPPs. IEC 61513 structures the IEC SC 45A standard series.

IEC 61513 refers directly to other IEC SC 45A standards for general topics related to categorization of functions and classification of systems, qualification, separation of systems, defence against common cause failure, software aspects of computer-based systems, hardware aspects of computer-based systems, and control room design. The standards referenced directly at this second level should be considered together with IEC 61513 as a consistent document set.

At a third level, IEC SC 45A standards not directly referenced by IEC 61513 are standards related to specific equipment, technical methods, or specific activities. Usually these documents, which make reference to second-level documents for general topics, can be used on their own.

A fourth level extending the IEC SC 45 standard series, corresponds to the Technical Reports which are not normative.

IEC 61513 has adopted a presentation format similar to the basic safety publication IEC 61508 with an overall safety life-cycle framework and a system life-cycle framework. Regarding nuclear safety, it provides the interpretation of the general requirements of IEC 61508-1, IEC 61508-2 and IEC 61508-4, for the nuclear application sector, regarding nuclear safety. In this framework IEC 60880 and IEC 62138 correspond to IEC 61508-3 for the nuclear application sector. IEC 61513 refers to ISO as well as to IAEA GS-R-3 and IAEA GS-G-3.1 and IAEA GS-G-3.5 for topics related to quality assurance (QA).

The IEC SC 45A standards series consistently implement and detail the principles and basic safety aspects provided in the IAEA code on the safety of NPPs and in the IAEA safety series, in particular the Requirements NS-R-1, establishing safety requirements related to the design of Nuclear Power Plants, and the Safety Guide NS-G-1.3 dealing with instrumentation and control systems important to safety in Nuclear Power Plants. The terminology and definitions used by SC 45A standards are consistent with those used by the IAEA.

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, that are based on the requirements of standards such as IEC 61508.

# NUCLEAR POWER PLANTS – INSTRUMENTATION AND CONTROL IMPORTANT TO SAFETY – SELECTION AND USE OF INDUSTRIAL DIGITAL DEVICES OF LIMITED FUNCTIONALITY

## 1 Scope

### 1.1 General

This International Standard addresses certain devices that contain embedded software or electronically-configured digital circuits that have not been produced to other IEC Standards which apply to systems and equipment important to safety in Nuclear Power Plants, but which are candidates for use in nuclear power plants. It provides requirements for the selection and evaluation of such devices where they have dedicated[2], limited, and specific functionality and limited configurability.

In accordance with IEC 61513, I&C systems important to safety of classes 1, 2 and 3 may be implemented using conventional hard-wired equipment, digital technology equipment (computer based or programmed hardware) or by using a combination of both types of equipment. This International Standard provides the acceptance criteria for the selection, evaluation and use of certain digital devices that have not been developed specifically for use in these nuclear I&C systems. Such devices are very often developed to meet IEC 61508, and this standard acknowledges that compliance with IEC 61508 can be a key positive factor when qualifying non-nuclear components for nuclear sector use.

Devices addressed by this Standard are dedicated devices of limited, specific functionality, that contain or may contain components driven by software or digital circuits designed using software-based tools. Examples are smart sensors, valve positioners, electrical protective devices or inverters that contain or may contain components driven by software or digital circuits designed using software-based tools. This standard does not address the software aspects of complex general-purpose devices that are addressed by other standards, such as IEC 60880 and IEC 62138 for software. This standard addresses the issues that should be considered when evaluating the suitability of these dedicated devices of limited, specific functionality for use in a nuclear power plant. The intent is to apply a graded approach to these issues, with more demanding requirements applied for higher classes.

These issues include:

- functional suitability (does the device perform the functions required, and are these functions suitably secure from interference from any other functions),
- the evidence required to demonstrate this suitability (such as the development process followed, and the operational experience and maturity of the device),
- aspects affecting integration of the device in existing systems (e.g. functional compatibility and impact on maintenance and operation), and
- requirements related to ensuring the device will retain its suitability for its required lifetime (such as the lifetime of the plant).

This Standard relies on other standards, especially IEC 60780, to address hardware qualification issues not related to the complexities of software, namely reliability aspects related to environmental qualification and failures due to aging or physical degradation. Other

---

2 "Dedicated" in the sense in which it is used in this standard refers to design for one specific function that cannot be changed in the field. Refer to 3.7.

standards such as IEC 61508 can be used as complementary guidance for the evaluation and assessment of components, but it is recognized that certification to non-nuclear standards alone is insufficient.

### 1.2 Background

The need for this standard arises from current trends in the I&C industry including the advancing obsolescence of existing devices presently in use in nuclear power plants. It is becoming increasingly difficult, if not impossible, to identify analog devices or replace many existing devices with identical ones because suppliers increasingly employ micro-controllers, ASICs etc. embedded within the candidate replacement devices, and analog devices are becoming increasingly unavailable.

There are various technical risks regarding the acceptance of these devices for use in nuclear plants, because:

- many of these devices do not duplicate the precise functionality of the obsolete device to be replaced, having in some cases less and in other cases more functionality, or even subtly different functionality that may be inconsistent with the original design intent,
- these differences in functionality are not always readily apparent. Examples exist of problems that have occurred because of the lack of guidance in this area, and are generally caused by the difference in design goals between nuclear plants and industrial applications for which equipment is designed, and
- they may have specific vulnerabilities or failure modes that did not exist with the original equipment and that need to be considered.

### 1.3 Use of this standard

This standard provides requirements for determining whether digital devices of industrial quality, that are of dedicated, limited and specific functionality and limited configurability, are suitable for use in a nuclear application. This will require the application of criteria similar to those applied to non-digital devices, but this standard provides additional criteria that apply to digital devices. It will also take into account the limits of feasibility given that limited or no change will be made to the evaluated industrial device.

This standard is intended for use in the context of a defined application for which the application designers seek suitable devices for its implementation. Very often, however, the application designer is forced to consider using devices not designed specifically for nuclear application. The objective of this standard is to help the application designer to select and use such devices in a way that is consistent with the safety class and requirements of the intended application.

Thus, this standard may be applied at different stages of the life cycle of system design as defined in IEC 61513. It may be applied early in the plant design life cycle, where the architecture of the specific I&C system is being drafted, and the availability of suitable devices may influence the system design. If applied somewhat later when the system design has been finalized, this standard can be used to assess candidate devices. Finally, this standard may also be applied to retrofit situations where a system is already in operation and some devices have to be replaced.

Classes 1, 2 and 3 are characterised by graded sets of requirements. This standard is intended to be interpreted in the context of the category of safety function being performed and the class of the system. This means that a graded interpretation of the requirements is appropriate and expected. It is also recognized that the tolerable modes of failure may be quite different in each plant application context, and this may determine the acceptability of a given device or its form of use. The interpretation and rigor in application of the requirements of this standard is assumed to be appropriately considered in each case.

Another issue frequently encountered is supplier resistance to providing evidence of correctness, such as details about the internal functions of the device, or how it was developed. This issue should be addressed as early as possible, possibly through pre-qualification of suppliers, and may require the selection of other vendors in order to comply with this standard.

The Evaluation and Application Plan (EAP)[3] sets the objectives of the evaluation and provides a guide to interpreting this standard for the specific device and application. This Plan identifies and justifies the approaches that will be used in problematic cases, including the kind of compensatory measures which will be taken to address issues such as discrepancies between required and available functionality or the lack of traditional evidence of correctness.

The final step in the evaluation process is the preparation of the Evaluation and Application Report (EAR). This Report identifies the device being qualified, the application(s) for which it is qualified and all the constraints that apply to its use.

### 1.4 Framework

This standard is organized as follows:

- Clause 5 addresses the applicability of this standard, and the evaluation process, defining:
  - the variation of device functionality which is covered by this standard, and
  - the degree of flexibility and configurability of the device which is covered by this standard, as well as
  - the inputs and outputs of the evaluation process and the EAP which will document how the evaluator(s) will apply the clauses of this standard,
  - the contents of the EAR document, the evidence reviewed and the results of the analysis of this evidence, and the conclusions reached as to the suitability of the device.
- Clause 6 addresses the elements of functionality and other requirements that shall be evaluated, such as
  - the minimal level of development documentation of the candidate device,
  - the ability of the candidate device to perform the required function(s),
  - the immunity of the candidate device's primary function to unwanted influences from superfluous functions,
  - the ability of the candidate device to function under all expected environmental conditions, following IEC 60780 and other identified standards,
  - the reliability and maintainability of the candidate device,
  - the adequacy of cyber security measures, and
  - the user documentation provided.
- Clause 7 addresses the criteria for providing confidence in the correctness of the design and manufacture of the device, identifying:
  - the usefulness of previous non-nuclear certifications,
  - methods to avoid systematic faults,
  - the application of a safety life cycle during the design of the device,
  - manufacturing quality assurance, and
  - permitted means to compensate for some weaknesses in the evidence of some of these concerns, by completing the case in favour of accepting a candidate device on

[3] The requirement for a Qualification Plan defined in IEC 61513 is met by the Evaluation and Application Plan.

the basis of product stability, focussed operating experience, improvements in the documentation or complementary testing and/or analysis.

- Clause 8 addresses criteria for the integration of the device into a plant I&C system, including:
  - restrictions on how the device may be used (such as the highest class of application for which it is qualified),
  - modifications that may be necessary to either the device or the target system in order to integrate the device into the target system, and
  - the integration and commissioning of the device in the plant safety systems.
- Clause 9 addresses considerations for preserving the acceptability of the device, such as:
  - notifications by the device designer or manufacturer to users of the device,
  - the support lifetime of the device,
  - preservation of maintenance tools and documentation, and
  - recommendations for the end-user.

## 2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

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

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

IEC 60880:2006, *Nuclear power plants – Instrumentation and control systems important to safety – Software aspects for computer based systems performing category A functions*

IEC 60980, *Recommended practices for seismic qualification of electrical equipment of the safety system for nuclear generating stations*

IEC 60987:2007, *Nuclear power plants – Instrumentation and control important to safety – Hardware design requirements for computer based systems*

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

IEC 61226, *Nuclear power plants – Instrumentation and control important to safety – Classification of instrumentation and control functions*

IEC 61508-7:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 7: Overview of techniques and measures*

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

IEC 62138:2004, *Nuclear power plants – Instrumentation and control important for safety – Software aspects for computer-based systems performing category B or C functions*

ISO 9001:2008, *Quality management systems – Requirements*

## 3 Terms and definitions

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

**3.1**
**ancillary function**
any function provided by the candidate device that supports its primary function

Note 1 to entry: Examples are functions of the candidate device used to support the function important to safety, such as providing an appropriate means to monitor its operating parameters or its continued correct operation as required for the safety application.

Note 2 to entry: See also “Primary function” and “Superfluous function”.

**3.2**
**auditable**
property of documented evidence that is readily available for review by independent personnel

**3.3**
**category of an I&C function**
one of three possible safety assignments (A, B, C) of I&C functions resulting from considerations of the safety relevance of the function to be performed. An unclassified assignment may be made if the function has no importance to safety

Note 1 to entry: See also “class of an I&C system”, “I&C function”.

Note 2 to entry: IEC 61226 defines categories of I&C functions. To each category corresponds a set of requirements applicable on both the I&C function (concerning its specification, design, implementation, verification and validation) and the whole chain of items which are necessary to implement the function (concerning the properties and the related qualification) regardless how these items are distributed in a number of interconnected I&C systems. For more clarity, this standard defines categories of I&C functions and classes of I&C systems and establishes a relation between the category of the function and the minimal required class for the associated systems and equipment.

[SOURCE: IEC 61513:2011, 3.4]

**3.4**
**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 relevance. An unclassified assignment is made if the I&C system does not implement functions important to safety

Note 1 to entry: See also “category of an I&C function”, “items important to safety”.

[SOURCE: IEC 61513:2011, 3.6]

**3.5**
**Common Cause Failure**
**CCF**
failure of two or more structures, systems or components due to a single event or cause

[SOURCE: IEC 61513:2011, 3.8]

**3.6**
**computer-based system**
I&C system whose functions are mostly dependent on, or completely performed by microprocessors, programmed electronic equipment or computers

Note 1 to entry: Equivalent to: software-based system, programmed system.

[SOURCE: IEC 61513:2011, 3.11]

**3.7**
**dedicated functionality**
property of devices that have been designed to accomplish only one clearly defined function or only a very narrow range of functions, such as, for example, capture and signal the value of a process parameter, or invert an alternating current power source to direct current. This function (or narrow range of functions) is inherent in the device, and not the product of programmability by the user

Note 1 to entry: Ancillary functions (e.g., self-monitoring, self-calibration, data communication) may also be implemented within the device, but they do not change the fundamental narrow scope of applicability of the device.

Note 2 to entry: This standard applies to devices of dedicated functionality that comply with all of the required criteria in 5.2.2.

Note 3 to entry: “Dedicated” in the sense in which it is used in this standard refers to design for one specific function that cannot be changed in the field.

**3.8**
**digital device**
device whose implementation is based on operations performed using signals with defined, discrete levels or contains defined, discrete internal states and makes transitions between those states

Note 1 to entry: The functions of such devices are usually defined by processes that include development and testing involving software or hardware description languages; such devices may be internally controlled by software or may consist of ASICs or FPGAs etc. that have been configured through the use of software.

Note 2 to entry: Devices, equipment or systems that are controlled by software are described as “computer-based”, whereas “digital” is a broader term that encompasses any device using digital circuits to implement logic.

Note 3 to entry: Digital devices developed for non-nuclear industries are called industrial digital devices.

**3.9**
**equipment**
one or more parts of a system. An item of equipment is a single definable (and usually removable) element or part of a system

Note 1 to entry: See also “component”, “I&C system”.

Note 2 to entry: Equipment may include software.

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 definition deviates from that provided in IEC 60780. The deviation is justified by the fact that IEC 61513 considers "equipment" as part of a system whereas IEC 60780 considers equipment as the object of qualification.

[SOURCE: IEC 61513:2011, 3.16]

**3.10**
**Hardware Description Language**
**HDL**
language used to formally describe the functions and/or the structure of an electronic component for documentation, simulation or synthesis

The most widely used HDLs are VHDL (IEEE 1076) and Verilog (IEEE 1364).

[SOURCE: IEC 62566:2012, 3.6]

**3.11**
**HDL-Programmed Device**
**HPD**
integrated circuit configured (for NPP I&C systems), 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.

[SOURCE: IEC 62566:2012, 3.7]

**3.12**
**I&C function**
function to control, operate and/or monitor a defined part of the process

Note 1 to entry: The term “I&C function” is used by process engineers to structure the functional requirements for the I&C. An I&C function is defined in such a way that it

- gives a complete representation of a functional objective,
- can be categorised according to its degree of importance to safety,
- comprises the smallest entity, from sensor to actuator, to achieve its functional objective.

Note 2 to entry: An I&C function may be subdivided into a number of subfunctions (for example, measuring function, control function, actuation function) for the purpose of allocation to I&C systems.

[SOURCE: IEC 61513:2011, 3.28]

**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.

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 (see Note 2). The different functions within a system may use dedicated or shared resources

Note 1 to entry: See also “I&C function”.

Note 2 to entry: The elements included in a specific I&C system are defined in the specification of the boundaries of the system.

Note 3 to entry: According to their typical functionality, IAEA distinguishes between automation and control systems, HMI systems, interlock systems and protection systems.

[SOURCE: IEC 61513:2011, 3.29]

**3.14**
**interrupt**
suspension of a process such as the execution of a computer program, caused by an event external to that process

[SOURCE: IEC 61513:2011, 3.32]

**3.15**
**item important to safety**
an item that is part of a safety group and/or whose malfunction or failure could lead to radiation exposure of the site personnel or members of the public

Items important to safety include:

a) Those structures, systems and components whose malfunction or failure could lead to undue radiation exposure of the site personnel or members of the public.

b) Those structures, systems and components that prevent anticipated operational occurrences from leading to accident conditions.

c) Those features which are provided to mitigate the consequences of malfunction or failure of structures, systems or components.

Note 1 to entry: This definition is intended to encompass all aspects of nuclear safety.

Note 2 to entry: In this standard the items considered will be mainly I&C systems or I&C functions.

Note 3 to entry: See also “I&C function”.

[SOURCE: IAEA Safety Glossary, 2007 Edition]

**3.16**
**limited functionality**
synonym for dedicated functionality (refer to 3.7)

**3.17**
**overall I&C safety life cycle**
necessary activities involved in the implementation of the systems and equipment important to safety of the I&C architecture, occurring during a period of time that starts with deriving I&C requirements from the plant safety design base and finishes when none of the I&C systems are available for use

[SOURCE: IEC 61513:2011, 3.34]

**3.18**
**primary function**
the singular function (or minimal set of related functions) of the candidate device which is required for the system important to safety to perform its function claimed in the safety analysis, and which is relied on to operate autonomously to achieve this function.

Note 1 to entry: As defined in 5.2.2, a multi-function device may offer the possibility of using several of its main functions as a “primary function”, but such a device may not fall within the scope of this standard, or in any case would be less favoured than a single-function device.

Note 2 to entry: See also “ancillary function” and “superfluous function”

Note 3 to entry: For example, a smart amplifier could be used to generate and output both a log power and a linear power signal, each of which is used for a reactor trip signal. These two functions would form the set of primary functions (and for purposes of this standard the term “primary function” would apply to this set); while the functionality to support changing the output scale or filtering of the outputs would be an ancillary function. Other functions which are not necessary to the selection of the device, such as local display, or remote signalling via a network connection would be superfluous functions.

Note 4 to entry: For example, a smart sensor may be capable of outputting a signal representing the flow or level via an analog output ranging from 4 mA to 20 mA or via a HART protocol. If the designer of the nuclear application opts to use the 4 mA to 20 mA signal for safety purposes, then this would be the primary function and the other output would be superfluous.

**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 (i.e. developed in the framework of a previous project, or being a COTS product). 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).

[SOURCE: IEC 61513:2011, 3.38]

**3.20**
**quality**
degree to which a set of inherent characteristics fulfils requirements

[SOURCE: ISO 9000:2005]

**3.21**
**quality assurance**
the function of a management system that provides confidence that specified requirements will be fulfilled

[SOURCE: IAEA Safety glossary, 2007 Edition]

**3.22**
**requirement**
expression in the content of a document conveying criteria to be fulfilled if compliance with the document is to be claimed and from which no deviation is permitted

[ISO/IEC Directives, Part 2, 2011, 3.3.1]

Note 1 to entry: In IEC SC 45A documents the following types of requirements are distinguished:

*Safety requirements* - Requirements imposed by authorities (legal, regulatory or standards bodies) and design organizations on the safety of the NPP in terms of impact on individuals, society and environment during the NPP lifecycle.

*Functional and performance requirements* - Functional requirements state what actions the system must take in response to specific signals or conditions, and performance requirements define features such as response times and accuracy.

*Operational requirements* - Requirements on the operational capacity and ability of the plant imposed by the owner.

*Plant design requirements* - Technical requirements on plant general design for the fulfilment of the safety requirements and operational requirements on the plant.

*System design requirements* - Design requirements on individual systems to give a design of the complete plant fulfilling the plant design requirements.

*Equipment requirements* - Requirements on individual equipment for its fulfilment of the demands of the system design.

Note 2 to entry: The IAEA safety glossary Edition 2007 contains the following definitions:

*Required, requirement* - Required by (national or international) law or regulations, or by IAEA Safety Fundamentals or Safety requirements.

This IAEA definition is useful in the framework of IAEA publications, but too narrow for use in a technical standard. It corresponds to the IEC/SC 45A definition “Safety requirement” as provided in Note 1.

Note 3 to entry: It is understood that any deviations from the requirements will be justified.

Note 4 to entry: If there are any deviations from the requirements, the deviations and their justifications will also be clearly documented in the EAR to permit a potential user of the device to justify his application of the device or select an alternative device.

[SOURCE: IEC 61513:2011, 3.44]

**3.23**
**restricted configurability**
applies to devices that can be configured in only very limited ways to select from among relatively few options the manner in which a device will function in its intended application

**3.24**
**security**
capability of the CB system to protect information and data so that unauthorized persons or systems cannot read or modify relevant data or perform or inhibit control actions, and authorized persons or systems are not denied access

Note 1 to entry: Within this standard, “security” should be interpreted by substituting the expression “CB system” with the expression “digital device containing software or digital circuit designs specified using hardware description languages”.

[SOURCE: IEC 61513:2011, 3.48]

**3.25**
**self-supervision**
automatic testing of system hardware performance and software consistency of a computer based I&C system

Note 1 to entry: As used in this standard, the definition is extended to go beyond merely testing, and includes the automatic functions performed by a programmable device designed to detect (primarily) hardware failures that may be inherently safe or dangerous (i.e., failures which prevent the device from performing its safety function) in order to convert them to safe events, either by alarming the failure or by causing the device to go to its safe state.

Note 2 to entry: See also “surveillance test”, which is not automatically initiated.

Note 3 to entry: The expression “self-surveillance testing” is equivalent.

[SOURCE: IEC 60671:2007, 3.8]

**3.26**
**software**
programs (i.e. sets of ordered instructions), data, rules and any associated documentation pertaining to the operation of a computer-based I&C system

[SOURCE: IEC 61513:2011, 3.51]

**3.27**
**software criticality analysis**
analysis of software to classify each function within the software as to its potential to cause unsafe failures

**3.28**
**software fault**
design fault located in a software component

[SOURCE: IEC 61513:2011, 3.53]

**3.29**
**superfluous function**
all functions performed by a candidate device that are not required functions.

Note 1 to entry: For example, while a primary function may be the sensing of pressure transmission of a 4 mA to 20 mA signal to another device, an ancillary function may be one which supports adjusting the filtering parameters of this output to achieve the desired safety function, while a superfluous function may be a second output such as a voltage signal that is not needed for the safety function.

Note 2 to entry: See also “Primary function” and “ancillary function”.

**3.30**
**surveillance test**
a manually initiated end to end test of a safety function. It may be conducted as a once-through end to end test or a series of overlapping tests. The test is manually initiated but may include automated or semi-automated test equipment to implement the test and/or record the test results. Surveillance tests are performed on the primary safety function(s) of a device

Note 1 to entry: IEC 60671 defines “surveillance testing” as the “complete scope of activities to demonstrate that the functional capabilities of I&C systems and equipment important to safety are retained and confirmation that the design basis requirements are met”. This standard recognizes that the automatic self-surveillance tests are a requirement of IEC 61508 at the higher Safety Integrity Levels and which are distinct from the manually initiated tests because of the large difference in initiation frequency and test coverage.

Note 2 to entry: A synonym is “proof test”.

Note 3 to entry: See also “self-supervision” (“self-surveillance testing”), which is automatically initiated.

**3.31**
**systematic fault**
fault related in a deterministic way to a certain cause, which can only be eliminated by a modification of the design or of the manufacturing process, operational procedures, documentation or other relevant factors

[SOURCE: IEC 61513:2011, 3.60]

## 4 Symbols and abbreviations

| | |
|---|---|
| ASIC | Application specific integrated circuit |
| CB | Computer-based |
| CM | Compensatory Measure |
| COTS | Commercial off the shelf |
| CPU | Central processing unit |
| EAP | Evaluation and Application Plan |
| EAR | Evaluation and Application Report |
| EMI | Electromagnetic interference |
| FMEA | Failure modes effects analysis |
| FMECA | Failure modes effects and criticality analysis |
| FMEDA | Failure modes effects and diagnostic analysis |
| FPGA | Field programmable gate array |
| FTA | Fault tree analysis |
| HART | Highway addressable remote transducer (protocol) |
| HAZOP | HAZard and OPerability |
| HDL | Hardware description language |
| HMI | Human machine interface |
| HPD | HDL programmed device |
| I&C | Instrumentation and control |
| I/O | Input/output |
| NPP | Nuclear power plant |
| PLC | Programmable logic controller |
| PROM | Programmable read only memory |
| QA | Quality assurance |
| VHDL | Very high speed integrated circuit hardware description language |

## 5 General requirements

### 5.1 General

The major concern with digital devices is that they are very often complex, and this complexity creates the potential for systematic faults in their design, particularly in their software or HDL-

Programmed Device (HPD) design; and the faults may not be detected until the occurrence of an event which has an operational profile that has not been a test case. Hence, a major objective of this standard is to provide criteria for assessing the design of a digital device to provide a degree of assurance commensurate with the class of the intended application so that the device will not fail to perform its function when called upon under its conditions of use due to systematic faults.

To achieve this, this standard identifies specific requirements in 5.2.2 that shall be met by a device so that this standard may be applied. This standard then defines the process and requirements for assessing the candidate device on the basis of the suitability of its functions and the level of confidence one may have in its design and operation, and secondarily the confidence that the device design definition is stable. It is also recommended that the likelihood of long-term support be considered.

## 5.2 Application of this standard

### 5.2.1 General

The object of this subclause is to provide assistance in the application of this standard to those charged with evaluating the suitability of an industrial device for use in an application important to safety in a nuclear power plant.

This subclause describes

– the criteria to be used to decide whether this standard applies, and

– the principles involved in defining the applicability of this standard.

### 5.2.2 Applicability criteria for this standard

A digital device to which this standard may be applied shall comply with the following criteria:

a) The device is a pre-existing digital device that contains pre-developed software or programmed logic (e.g. an HPD) and is a candidate for use in an application important to safety.

b) The primary function performed is well-defined and applicable to only one type of application within an I&C system, such as measuring a temperature or pressure, positioning a valve, or controlling speed of a mechanical device, or performing an alarm function.

c) The primary function performed is conceptually simple and limited in scope (although the manner of accomplishing this internally may be complex).

d) The device is not designed so that it is re-programmable after manufacturing nor can the device functions be altered in a general way so that it performs a conceptually different function: only pre-defined parameters can be configured by users.

e) If the primary device function can be tuned or configured, then this capability is restricted to parameters related to the process (such as process range), performance (speed or timing), signal interface adjustment (such as selection of voltage or current range), or gains (such as adjustment of proportional band).

NOTE 1 The intent is to prefer devices without ancillary functions and particularly without superfluous functions. If such functions exist in the device, they will be identified and assessed in terms of their potential to interfere with the primary function of the device according to 6.3 and 6.5 respectively.

NOTE 2 The intent is to exclude devices which provide a capability of defining functionality with either a general purpose language, such as “C” or using application specific language such as ladder logic or function blocks.

NOTE 3 It is not possible to define all devices that fall under the aegis of this standard, but the functions listed below serve as examples, assuming they provide a degree of configurability commensurate with the intended scope of this standard:

- pressure and temperature sensors,
- smart sensor (e.g. pressure transmitter),

- valve positioner,
- electrical protective devices, such as over-voltage/over-current relays,
- motor starter,
- dedicated display unit (e.g. multi-segment LED bar display), or
- dedicated simple communications interfaces.

NOTE 4 It is not possible to define all devices that do not fall under the aegis of this standard, but the equipment and devices listed below serve as examples:

- PLCs,
- Devices provided with a programmable language, regardless of its restricted nature (in terms of number of function blocks (or equivalent) or inputs and outputs), where such devices have been designed to allow them to be configured for more than one application (example: single loop digital controller with a function block language).

## 5.3 General requirements on the evaluation process

### 5.3.1 Evaluation process

The object of this subclause is to identify the major steps required to select and evaluate a candidate device for use in a target application. These steps are illustrated in Figure 1 and specified in the paragraphs below.

The evaluation and application process shall include the following steps:

a) The pre-requisite to the evaluation and application process shall be the documentation of all the functional and performance requirements that apply to the device in the target application. This may entail reconstructing the design basis of the application[4]. Defining the requirements for the candidate device shall include addressing all the relevant aspects given below:
   - definition of the safety purpose of the target system or application in sufficient detail to support the categorisation of the function of the target application according to IEC 61226 or a process equivalent to IEC 61226 and accepted by national authorities;
   - safety category of the function of the target application and the class of the system involved in this target application;
   - primary functionality required of the device, including functional requirements and performance requirements such as response time, consistent with the criteria defined in 5.2.2;
   - all the other specific safety properties and characteristics required of the product, as addressed in Clause 6.

b) An Evaluation and Application Plan (EAP) shall be prepared that takes the documented functional and performance requirements into account according to 5.3.2 and 5.3.4, and where relevant defines the strategy to account for multiple uses of a candidate device (whether to perform a single evaluation to cover all the intended uses or to perform individual evaluations).

As the EAP is followed, it may become necessary to revise the Plan in view of the results obtained or the availability of evidence of correctness.

c) A candidate device shall be selected and evaluated under this standard only if it meets the requirements of 5.2.2.

---

4 While this standard applies to replacement of any device by a digital one, there are some particular concerns to consider when replacing analog devices with digital devices, such as the sampling rate and the sampling theorem, analog to digital quantization and least significant bit noise which can raise questions about a digital device not sensing an event, and on the other hand the possible advanced filtering possible with digital techniques that could allow a digital device to detect an event to which the analog device would be blind. Such issues need to be considered when reconstituting the design basis and the requirements for a digital device.

In the case of a system already developed for which a device shall be replaced, the functional and performance requirements are relatively fixed; whereas for a new system the requirements might be more fluid as there is more freedom in defining the interfaces between devices. For new systems, designers will likely consider in advance the likelihood of success in the evaluation of each candidate device and the implications of its application in the target system, and thereby narrow the selection of candidate devices. This tends to blur the distinction between selecting and evaluating candidate devices, but it is not a valid reason to avoid following the prescribed process.

d) Each candidate device shall be evaluated according to the EAP (described in 5.3.2) and 5.3.4 to demonstrate that it complies with the requirements of this standard.

e) The results of the evaluation shall be documented in an Evaluation and Application Report (EAR). This Report shall document:

   1) the evaluation of the candidate device against each of its requirements for the target application according to the EAP, and

   2) provide a clear conclusion as to its acceptability; namely the device is acceptable as-is, it is acceptable under some specific conditions and/or constraints, or it is not acceptable.

   To do this, the EAR shall either reference concise and complete requirements in pre-existing and available documents, or it shall include documentation of the reconstituted requirements.

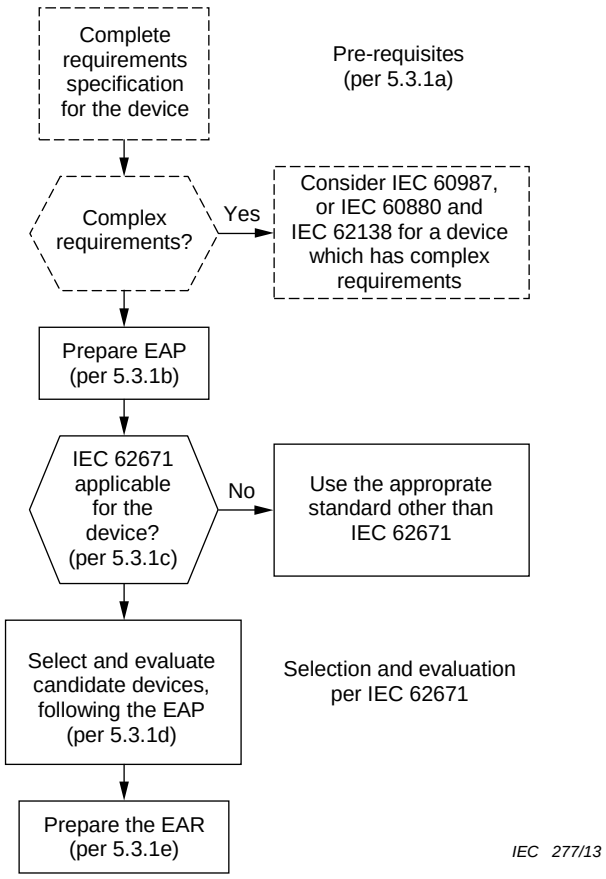


**Figure 1 – Selection and evaluation process**

### 5.3.2 Evaluation and Application Plan (EAP)

The object of this subclause is to identify the purpose and scope of the EAP.

The EAP:

a) Shall justify the applicability of this standard, in terms of the criteria given in 5.2.

b) Shall identify the scope and applicability of the evaluation work in terms of:

- the application (safety function) or applications and the corresponding system class or classes;
- if more than one application is under consideration, whether to qualify only the application of the highest class or every one;
- the candidate device(s) to be covered by the EAR.

c) Should identify the technical resources, and their qualification needed to execute the evaluation work, such as:

- safety application experts to ensure a complete requirements specification, particularly in retrofit situations;
- software experts to examine the susceptibility of the software to systematic faults;
- specific hardware experts to evaluate EMI/EMC qualification, etc.

d) Shall identify the criteria defined in the subclauses of Clause 6 that are relevant to the target application.

e) Shall identify the recommended (where “should” applies) criteria defined in the subclauses of Clause 7 that shall be applied, and justify the omission of these criteria and the reliance on the compensatory measures permitted in Clause 7.

f) Should identify the selection criteria and their relative importance which may influence the selection of candidate devices, such as:

- the required lifetime of the device in the target application;
- the amount of supplier support that may be needed, and over what time period; and
- the degree to which the target system into which the candidate device may be integrated may need to be modified to allow the use of the device considering its functions and failure modes, etc.

g) Shall identify the review requirements for the EAR.

### 5.3.3 Evaluation and Application Report (EAR)

The object of this subclause is to identify the scope and content of the EAR.

The EAR:

a) Shall document the results of the evaluation.

b) Shall document the reasons why applying this standard is justified in terms of the applicability criteria in 5.2.2.

c) Shall define the scope and applicability of the evaluation work and of the evaluation reported in the EAR, in terms of:

- the specific target application (safety function) and its system class;
- if relevant, a higher class to which the device has been evaluated;
- the candidate device(s) covered by the EAR, including the precise identification of the candidate device, including product name, version number of the software and hardware components, configuration, and any other component or option which may pertain to the evaluation.

d) Shall summarize or reference the key functional and performance requirements (including those that may have had to be reconstituted) that impact the acceptability of the device, the target class, safe failure mode(s), and environmental service conditions criteria.

NOTE 1 If there are any deviations from the requirements, the deviations and their justifications will also be clearly documented in the EAR to permit a potential user of the device to justify his application of the device or select an alternative device.

e) Shall document the reliability limits that are achievable by the device either alone or in a redundant configuration.

f) Shall document the selection criteria identified in the EAP.

g) Shall include (or reference if they are available for inspection) all documents used to verify each development phase of the device, including verification strategy and tests performed; or alternatively include references to these documents under the condition that the referenced documents are available to a third party assessor.

h) Shall document how the criteria defined in the subclauses of Clauses 6 through 9 have been applied according to 5.3.4, and provide the justification of the relative ranking of importance or omission of these criteria.

i) Shall document the required compensatory measures for the target application(s) under consideration to cover the case where either the candidate device does not meet all compliance requirements or the original evidence of compliance is considered insufficient.

Potential compensatory measures may include complementary testing, improvements in the documentation, extra surveillance testing during operation, strict limitations on the use of the device (such as use only in systems with certain functional properties), disabling of certain options, or modifications to the target system or very restricted modifications to the device itself, as described in Clause 8.

j) Shall identify all modifications subject to 8.3 and 8.4 that may be necessary to the device or to the target system in order for the candidate device to be integrated into the target system(s) and retain the acceptability under the preceding items. Any such modifications to the device shall be limited in scope and not involve software or HPD design, so that the device retains its original function; otherwise the device would no longer be a standard industrial device that would come under this standard.

NOTE 2 Examples of such a modification would be substitution of an impedance matching resistor, change to a mounting bracket, or substituting a keyed component for a switch or potentiometer.

k) Shall identify all restrictions on the use of the device in each application and class for which it is acceptable.

l) Shall identify the measures (and their adequacy) recommended to ensure that application of the candidate device observes all restrictions and recommendations provided in the EAR.

m) Shall state the final conclusion as to the acceptability of the candidate device(s) for use in each of its target applications, expressed in terms of:

- the candidate device is acceptable as-is, or
- the candidate device is acceptable under listed conditions, or
- the candidate device is not acceptable.

### 5.3.4 Application of clauses of this standard

The object of this subclause is to indicate how to apply the requirements presented in Clauses 6 through 9 in evaluating digital devices of dedicated functionality as defined in 3.7 for use in a given application.

a) The applicability of this standard shall be justified in terms of the applicability criteria in 5.2.2.

b) The evaluation of the candidate device shall be performed based on the intended function and its category or the intended application and its class.

c) Evidence shall be documented to demonstrate functional and performance suitability of the candidate device as defined in Clause 6 based on all of the applicable criteria in that clause.

d) Evidence shall be documented to demonstrate correctness, based on a combined qualitative assessment of all the applicable criteria in Clause 7, according to the EAP.

e) The evaluation shall identify all of the restrictions that shall be applied so that its use is constrained within the bounds of the evidence documented under Clause 7.

f) The evaluation shall identify all of the restrictions that shall be applied for the safe use of the candidate device in the target application (see Clause 8).

g) The evidence shall demonstrate that the results of the evaluation can be preserved for an adequate length of time, considering the life of plant and corresponding plans for equipment replacement, based on all of the applicable criteria in Clause 9.

## 6 Criteria for functional and performance suitability

### 6.1 General

The criteria for functional and performance suitability address the questions:

- does the candidate[5] device perform the functions required,
- does it perform only those functions (or alternatively, is any non-required functionality shown to be non-interfering to the required functions),
- does it perform its functions with suitable reliability and defined acceptable failure modes, and
- is this functionality appropriately documented?

Each criterion that is applicable shall be demonstrated by analysis and/or testing, and review of specifications of interfacing devices as appropriate. This demonstration shall be documented.

### 6.2 Functional competence of the primary function

The primary function or functions of the candidate device shall meet the functional requirement(s) derived from the plant and system requirements. If the candidate device is to be installed in the intended application:

a) The candidate device shall be capable of operating over the complete range of plant process signals and the complete operational domain specified for the intended application.

b) The candidate device shall exhibit the required accuracy and repeatability over this entire range.

c) The candidate device shall exhibit the required speed of response and suitable digital signal processing (defined in terms of the appropriate criteria, such as sampling rate, time delay, rise time, bandwidth, filter characteristics such as corner frequency, noise rejection, etc.).

d) Where the frequency domain transfer function is of concern (such as in a closed loop application), the candidate device shall exhibit adequate gain and phase change over the frequency range of concern.

e) The failure modes shall be well defined, and in these failure modes the values of the outputs shall be set to pre-determined output states (e.g. an open circuit, or an increase or decrease in output or as-is stasis in output), which are either inherently safe in the target application, or are both detectable and convertible to a state which is safe in the application, or where they are both undetectable and not convertible to a state which is safe in the application they shall be of acceptably low likelihood.

f) For the purposes of e) above, the failure modes shall be analysed in terms of the impact of the candidate device on the system in which it will be installed, taking into account all the factors that can influence failure modes (see also 6.7). Particular attention should be paid to common cause failures, especially those relating to other devices (possibly in other

---

5 Normally, candidate devices are evaluated for an application based on presumed compliance with the functional requirements for the application. This clause provides guidance on the criteria to review to ensure that all the appropriate criteria are considered in the evaluation of the candidate device.

classes) that have a role credited in the safety analysis as protecting against the same initiating events.

### 6.3 Ancillary functions

Ancillary functions of the candidate device are those functions that are not part of the primary function of the device, but that are required to be able to adjust the parameters of the primary function so that it can perform its required safety function, or that enhance the device dependability, such as self-monitoring.

a) For applications of class 1 and 2, it shall be shown by analysis (and/or test if this can be done conclusively) that no operation or failure mode of the ancillary functions can interfere with the primary functions except as specified (for example, by making a manually-initiated change in a set-point) or to cause the device to fail to a state that is safe in the context of the application.

NOTE 1 The failure mode which is “safe” depends upon the application, and is not always fail-stop or fail-open contact. Some examples are given in 7.2.

b) The ancillary functions related to adjusting parameters of primary functions shall meet the requirements of 6.4.

c) For applications of class 3 where two or more devices are determined to be equivalent in all other ways, the device least likely to be adversely affected by ancillary function failures shall be selected. The number, probability and severity of postulated ancillary function failures shall be factors in the comparison.

d) Where an external device of lower class is used to communicate with the candidate device, no operation or failure of the external device shall be capable of interfering in an unintended way with the primary function of the candidate device.

NOTE 2 This requirement is based upon the requirement for communications in IEC 61513 whereby a system of higher class may not be unintentionally affected by a system of lower class. Inter-class communications are therefore usually one-way (such as to a monitoring system which cannot affect the higher class system) or the communications are only temporarily enabled. Furthermore, the higher level system is usually tested after the short period of two-way communications, and two-way communications are controlled so that only one channel of the higher level system is connected at a time.

### 6.4 Configurability

The functions of the candidate device that are configurable and the ancillary functions providing that configurability shall together meet the following requirements:

a) The configuration parameters of the primary functions shall be limited in capability to on/off (activate/de-activate) settings or scale-like adjustments such as calibration of process range and output, gain or damping setting, etc.

b) For systems applications of class 1 and 2, configuration protection shall include deliberate design features so that more than one mistake is necessary before an error in setting a configuration parameter is committed.

NOTE 1 It is common practice to verify the impact on the primary function of the device following any change to its configuration parameters.

c) The configuration parameters of the primary functions shall be protected from inadvertent, malicious or unauthorised adjustment in a manner consistent with the overall security plan for the nuclear facility (see 5.4.2 of IEC 61513). This protection shall include password protection if it is supported by the candidate device.

It is permissible for there to be unprotected read-only access to configuration parameters, provided this read-only access meets the requirements for non-interference of an ancillary function as in item d) below.

For class 1 systems, physical access limitations includes accessibility constraints such as locked cabinets or instrument rooms. (This requirement applies to the installation, not to the candidate device, and is therefore the responsibility of the end-user.)

d) Where it is necessary to configure ancillary or superfluous functions so that they cannot interfere with primary functions these configuration parameters shall be protected as in items b) and c).

e) It shall be possible to check a device after its configuration parameters have been changed to verify that the change has been done correctly.

f) If the device provides operators with display or modify-enabled access to configuration parameters, then the device shall provide enabled access for only those configuration parameters that they require to execute their duties.

g) Where the device provides operators with modify-enabled access to configuration parameters, all operator inputs shall be subject to applicable range and validity checks and or limits appropriate to the application.

h) Where it is required that configuration parameters and any necessary associated logic states be automatically restored following a power failure, whether partial or total, and this property is configurable, these configuration parameters shall be protected as in b) and c).

Integral parts of filters or PID controllers are typical sources of bump in output on resumption of the operation after a power transient.

i) If the device is to operate in a channelized system, provisions shall be in place to ensure that only one channel of the redundant system can be subject to configuration changes at a time.

NOTE 2 This is typical of class 1 and class 2 systems.

### 6.5 Superfluous functions

Superfluous functions of the candidate device are those functions that are not part of the required safety function of the device nor its required ancillary functions. While superfluous functions are often integral parts of a device, their presence implies possible unnecessary complexity and additional potential failure modes which are undesirable in applications of higher classes.

a) For applications of class 1 and 2, it shall be shown by analysis (and/or test if this can be done conclusively) that no failure mode of the superfluous functions can interfere with the primary function.

b) For applications of class 1 and 2, it shall be shown by analysis (and/or test if this can be done conclusively) that under all operating circumstances the superfluous functions can be configured (or inherently function) so that they cannot interfere with the primary function.

c) For applications of class 3 where two or more devices are determined to be equivalent in all other ways, the device least likely to be affected by any superfluous functions or their failures shall be selected. The number, probability and severity of postulated superfluous function failures shall be factors in the comparison.

d) For applications of class 1 and 2, if a superfluous function cannot be shown to be non-interfering to the primary function as per items b) and c), then it shall meet all the requirements for safety design as required for the primary function(s).

e) For applications of class 1 and 2, it shall be shown by analysis (and/or test if this can be done conclusively) that under all operating circumstances that no operation or failure of an external device in communication with the candidate device shall be capable of interfering in an unintended way with the primary function of the candidate device. If this cannot be demonstrated then it shall be possible to test the primary function of the candidate device following this use of the communications to an external device.

NOTE 1 See the NOTE following 6.3 d).

f) Superfluous functions shall be eliminated in preference to minimising the number of ancillary functions.

NOTE 2 Subclause 8.3 applies for modifications to the device.

### 6.6 Hardware robustness

Hardware robustness is evaluated by functional and environmental qualification (also called hardware qualification), and is necessary to ensure that the candidate device will perform its functions in all environments (both that of normal plant operation and that during and following an accident) in which it is required to function.

IEC 61513 addresses hardware robustness in 6.4.2.1, and references IEC 60780, and IEC 60980, which in turn refer to other standards as appropriate. IEC 61513 permits qualification to industrial conditions for devices to be used in application of class 3, but requires documentary evidence for claims for operation in abnormal environmental conditions. One way to achieve this would be to apply IEC 60780.

NOTE 1 IEC 61513 also references IEC 60987 for bespoke computer-based systems in applications of class 1 and class 2.

a) The robustness of a candidate device shall be evaluated in terms of all environmental conditions (temperature, pressure, humidity, radiation, EMI) and durations of these conditions to which it may be subjected for which it is intended to perform its function. (This may include accident conditions inside containment.)

b) In order to qualify a candidate device, the robustness of the device shall be evaluated in terms of the referenced standards identified below; and where compliance to the standard is not documented, the shortfall shall be analysed and justified or compensatory measures shall be provided to address the following:

   - temperature and humidity in accordance with IEC 60780 for class 1 and class 2, and in accordance with IEC 61513 for class 3;
   - radiation;
   - vibration and seismic conditions in accordance with IEC 60980;
   - immunity to electro-magnetic interference in accordance with IEC 61000 series.

NOTE 2 IEC 62003 covers electro-magnetic interference and applies to systems important to safety in nuclear power plants, and references a large number of parts of IEC 61000-4. IEC 61000-6-2 is the normal industrial standard.

   - Dust and airborne particulates.

c) In order to qualify a candidate device, the effects of the candidate device on the other devices in the system where it will be installed shall also be considered. This may require modifying the device or evaluating the other devices as per item a) above considering the presence of the candidate device in their operating environment. The following shall be considered:

   - vibration produced by the candidate device;
   - heat produced by the candidate device;
   - electro-magnetic interference produced by the candidate device; and
   - the impact on the seismic qualification of the structure upon which the devices is to be installed.

### 6.7 Reliability, maintainability and testability

Reliability, maintainability and testability are linked properties of a device, since the testing frequency is determined largely by the inherent random failure rates of the device or system in question and the required probability of failure on demand. Maintainability plays a role in reducing repair time and avoiding maintenance faults that could lead to failures.

Requirements for the design of periodic tests and self-tests (self-surveillance) are addressed by IEC 60671. This subclause highlights issues related to testing and maintainability for selection, evaluation and application of a candidate device.

Failure Modes and Effects Analysis (FMEA), and extensions such as FMEDA (Failure Modes, Effects and Diagnostic Analysis) and FMECA (Failure Modes, Effects and Criticality Analysis) are widely accepted methods for systematically analysing a device to determine its hardware failure modes, their frequency, and their impact. Other techniques in use include Fault Tree Analysis (FTA).

The candidate device shall be evaluated and the outcome of the evaluation shall be documented with respect to the criteria listed below.

a) An analysis shall be performed to determine (or confirm) the failure modes of the device, and determine whether they are safe or dangerous in the context of the intended application(s).

Failure modes are interpreted in terms of the purpose of the device and the impact on plant safety. This may require distinguishing between the need to fail energized and fail de-energized, to fail up-scale, down-scale or as-is, or to immediately annunciate a failure so that the impact on plant safety can be assessed by operational personnel.

b) For intended applications of class 1 and class 2, it should be shown by analysis that an acceptably large fraction of the hardware failure modes are well defined, detected and annunciated.

c) For intended applications of class 1 and class 2, it should be shown by analysis that the subset of faults that could be dangerous in the application is of acceptably low probability for the application.

d) In the case of applications where requirements include quantitative failure rates, a quantitative analysis shall be used to determine the failure rates, and it shall be shown by this analysis that an acceptable fraction of the hardware failure modes which could be dangerous in the application are detected and annunciated or converted to safe failures in a timely manner, and of acceptably low probability so that the application requirements are met.

NOTE 1 Examples of quantitative methods include FTA and FMEDA. See also 5.3 in IEC 60987.

NOTE 2 Standards such as IEC 61508 provide guidance on these techniques.

NOTE 3 The importance of detecting a fault under specified time constraints is to allow corrective manual action and the replacement of the device by a non-faulty one within a sufficiently short delay, consistent with the availability target for safety functions.

e) The provisions in the design for self-supervision and periodic surveillance testing of the device shall not pose a risk of inadvertently interfering with the defences of the device's primary function against interference from ancillary or superfluous functions or pose a risk of inappropriately modifying the configuration parameters.

f) Where a device includes self-supervision capability, the detection of a failure shall be alarmed, annunciated, or acted upon by setting the outputs to a state that is safe in the context of the application.

g) The periodic testing defined to demonstrate the device's continued availability shall be designed to maximize the detection capability of faults that are not revealed by self-supervision.

h) Provisions for testing the candidate device, particularly if the tests are required to be complex, should be considered in the evaluation, including the following criteria:

- maintenance and surveillance test procedures and intervals;
- complexity and frequency of required tests;
- practicality of effecting the tests on-power;
- evaluation of software-based tools required for the tests.

i) The specific lifetime-limiting components (e.g. aluminium or electrolytic capacitors) shall be identified so as to provide a basis for component or device replacement before the expected failure rate of the device will likely show evidence of the end of useful life.

NOTE 4 Components are affected to a greater or lesser extent by different conditions (e.g. temperature, radiation, vibration, etc.) and this may result in a different set of components being life-limiting, depending on the application.

### 6.8 Cyber security

The candidate device and its associated configuration, maintenance, or test tools shall be included in the evaluation of its host system with respect to cyber security.

NOTE 1 IEC 62645 provides requirements on cyber security programmes.

NOTE 2 IEC 61513 provides requirements for security at the level of the I&C architecture and of an individual I&C system.

NOTE 3 IEC 60880 provides requirements for software security for applications of class 1, and IEC 62138 provides requirements for software security for applications of class 2 and class 3.

### 6.9 User documentation for safety

The candidate device shall be supported by both design and verification documentation (see 7.4.6) and by instructions for its safe use. Safe use of a device means that the safety objectives intended in the application will be met, given the way the device is installed, configured, and maintained in appropriate compliance with the documentation provided by the supplier of the device.

a) User documentation for safety may be divided into the following documents:

- Safety Manual – a document or index to documents wherein all the requirements for the safe use and application of the device are documented, including the precise identification, including version identifier, of the device.
- Installation manual – a document that defines how the device shall be installed and connected to other devices so as to ensure its performance in accordance with the functional specification.
- User or operating manual – a document that defines how the in-service user will interact with the device (This covers for example how a plant operator would read any display of data and change any settings which he is permitted to change).
- Maintenance manual – a document that covers all aspects of maintaining the device in the field: personnel safety precautions, system safety precautions, testing the device in situ, removing the device from service and restoring it to service.

NOTE The exact requirements for documentation, such as the specific title or scope of each document will depend on the specific operating organisation.

This standard does not require a specific title or scope of each document; rather it requires that all the subject matter be documented in the set of documents:

b) In order for the candidate device to be used correctly and safely, the documents described in item a) above shall collectively provide the following information:

- Complete version information.
- Complete documentation of the primary function in terms of overall black-box functionality, including specific effects of configuration parameters, device interfaces, behaviour during power-up, behaviour during power-interruption, failure effects, time and frequency domain response (if applicable), slew rates, input and output impedances and ranges, etc.
- Full documentation of the primary function in terms of failure modes and indications of failures.
- Full documentation of the ancillary and superfluous functions in terms of functionality, including where relevant the means of configuration to prevent interference with the primary function.
- Functional integrity requirements, such as self-surveillance to detect hardware failures, and the actions that are taken upon detection of a failure (as distinct from the functional requirements).

- The environmental and robustness limitations of the device and life-time limiting components.
- All maintenance procedures and appropriate cautions.
- All operating procedures and appropriate cautions.
- All periodic surveillance test requirements and procedures and appropriate cautions.
- Any other information important to the safe use of the device and appropriate cautions.

# 7 Criteria for dependability – Evidence of correctness

## 7.1 General

The object of this subclause is to provide guidance on:

- collecting and evaluating the evidence that the candidate device is suitable for use in an application important to safety in a nuclear power plant by virtue of the processes followed in its design and manufacture, and
- the means which may be used to compensate for any weaknesses in such evidence of correctness.

NOTE 1 The assessment of the evidence of correctness of the device is usually qualitative because there are no generally recognised means to quantify it, and because it may not be possible to obtain all of the kinds of evidence defined in this clause. It is based on a balanced assessment of product and process elements of both design and manufacture that have been documented; taking into account the possibility that certain elements of evidence of correctness may individually or in combination compensate for limited weakness in others as detailed in the corresponding subclauses.

The evidence of correctness shall be established by:

- assessing the processes by which the product was developed and its design is now maintained (including its verification and validation for both the current design and modifications),
- assessing the development documentation of the device,
- assessing the processes by which the product is manufactured, and
- assessing the attributes of the product itself.

The evidence of correctness addresses design and manufacturing separately because different means to compensate for weaknesses in the evidence of correctness are appropriate for design and manufacturing.

Furthermore, specific compensatory measures cannot be applied in a general way: specific compensatory measure apply only to specific deficiencies in principal elements of evidence of correctness.

The principal elements of evidence of correctness of design include:

- evidence of a disciplined development and maintenance life cycle for design,
- evidence of the tools used to support a disciplined life cycle (e.g., change control, configuration management),
- evidence of appropriate independence from likely systematic faults,
- review of the development documentation, including that of verification and validation,
- review of documentation of the design and use of the device.

NOTE 2 If a generic pre-assessment or certification of the candidate device has been done, it may be a convenient source of references to some evidence or may contain useful analysis.

Means which may be used to compensate for some weaknesses in the principal elements of evidence of correctness of design include:

- applicable and credible operational experience, which may be used where justified to compensate for weaknesses in other elements,
- evidence of stability (i.e. low rate of changes) of the product during a meaningful amount of manufacture and use of the product,
- device specific complementary tests performed to fill gaps in pre-existing documentation of tests, or to extend test coverage as appropriate to the intended application and the other elements of evidence of correctness,
- compensation at the system level to mitigate device failures or convert them to safe failures,
- improvements in the documentation initially provided by the designer.

The principal elements of evidence of correctness of manufacturing include:

- evidence of a disciplined development and maintenance life cycle for manufacturing, including change control and configuration management,
- review of documentation of the manufacturing and use of the device.

Means which may be used to compensate for some weaknesses in the elements of evidence of correctness of manufacturing include:

- evidence of stability (i.e. low rate of changes) of the product, during a meaningful amount of manufacture and use of the product;
- device specific inspections, functional and ageing tests appropriate to the weaknesses in the elements of evidence of correctness of manufacturing;
- procurement of sufficient numbers of devices from the same manufacturing batch to ensure sufficient spares for the lifetime of the NPP.

The EAP (see 5.3) identifies and justifies how the requirements of the subclauses below should be ranked in terms of importance, and which of the permissible compensatory measures will be considered.

Some of the subclauses below use tables to most clearly define the requirements for the three classes and the permissible compensatory measures. In these tables, the following interpretations shall apply:

a) “M” shall indicate the mandatory nature of the described criterion, corresponding to the use of “shall” in the statement of requirement.

b) “R” shall indicate the recommended nature of the requirement statement, corresponding to the use of “should” in the statement of requirement.

c) The columns indicated by “CM” shall indicate the compensatory measures which may be available, and:

   - “PS” indicates that the application of product stability in accordance with 7.6 may be used to compensate for some degree of weakness in the principal evidence,
   - “OE” indicates that the application of operating experience in accordance with 7.7 may be used to compensate for some degree of weakness in the principal evidence,
   - “CT” indicates that the application of complementary testing and/or analysis in accordance with 7.8 may be used to compensate for some degree of weakness in the principal evidence,
   - “DI” indicates that the application of documentation improvement in accordance with 7.9 may be used to compensate for some degree of weakness in the principal evidence.

The indicated potential for compensatory measures shall not be construed to permit a wide-ranging avoidance of the need for the principal forms of evidence; rather the indications in the tables of the possibility of applying compensatory measures shall be used sparingly.

NOTE 3 Widespread need of compensatory measures is an indication of a lack of a well-defined development process or of adherence to the declared process, and this could rule out the acceptance of a candidate device.

NOTE 4 As an example, the presence of “M” in the column “class 3” and the presence of “CT” in the CM column for class 3 would be interpreted to mean that the criterion is mandatory for class 3 but that some weakness in the designer’s or manufacturer’s fulfilment of this subclause could be compensated by documentation generated by complementary testing and/or analysis in accordance with 7.8.

### 7.2 Previous certification

In general, there are significant advantages to selecting a device that has been previously certified to a suitable safety standard. Such devices tend to have well-defined failure modes, and have been developed under a disciplined software and/or HPD development process, and therefore supporting documentation is likely to exist, although it might be proprietary.

NOTE 1 IEC 61508 is a suitable safety standard.

This is often very different for non-certified products because they tend to be developed with objectives of bringing them to market quickly and to be frequently changed to add expanded new features. Thus, non-certified products may include functionalities which are not required for the intended nuclear application. In addition, it is possible that the products may include functionalities which are not only not required but are not defined overtly (i.e. the functionality is hidden) in the product’s specification. In contrast, devices that have been developed to safety standards are likely to have a specific, well-defined functionality.

The second benefit of certification to a safety standard as compared to non-certified products is that the selection process may proceed with greater certainty that the necessary evidence of correctness will be available, because the development processes followed under such standards may require documentation similar to that required under nuclear standards.

NOTE 2 IEC 62138 and IEC 60880 are nuclear standards that have this kind of documentation requirement.

Care shall nevertheless be exercised in evaluating both previously certified and non-certified devices with respect to failure modes. Even though the failure modes of devices certified to a non-nuclear safety standard may be well defined, they are usually conceived within the process shutdown philosophy such as reactor trip, whereas other nuclear applications may require a fail-operate state as opposed to fail-shutdown. Examples of this include diesel generator and compressor controllers required to operate after an accident has occurred: in such cases the device controller should merely alarm conditions such as high vibration that would require a shutdown in a non-nuclear application.

Thus in general, the evaluation of an industrial device is facilitated and perhaps simplified if it is certified to a non-nuclear safety standard, but this is not in itself sufficient, and there are conditions which shall be considered when relying on a certification.

Certification to a non-nuclear safety standard may be used as evidence for criteria in Clause 7; in which case, the certification shall meet the following criteria:

a) Where the certification used to support compliance with a subclause of this standard is to a standard which is not widely recognized, this use shall be justified.

b) Where the certification is used to support compliance with a subclause of this standard, the certification shall provide evidence of correctness that directly addresses the subclause.

c) The supporting evidence material for the certification shall be available for review. This evidence shall include all elements needed to independently assess the scope and boundaries of the certification, in particular:

   - the documentation assessed,
   - the hypotheses made on the intended use of the device and its expected behaviour for all use cases,

- the certification methods and tools,
- the device properties assessed (whether the outcome of the assessment has been successful or not) and the results.

d) The certification shall be current and shall apply to the candidate device as follows:

- For intended applications of class 1 and 2 where the failure of the candidate device would cause failure of the target system (such as for instance if it were installed in all channels of a redundant system), the certification shall pertain to the specific version that has been certified.
- For intended applications of class 1 and 2, where the failure of the candidate device would not cause failure of the target system the certification shall pertain to a version that differs from the version intended for use in no more than minor ways that are well-documented and validated and that do not affect the primary function;
- For intended applications of class 3, the certification shall pertain to a version that differs from the version intended for use only in ways that are well-documented and validated.
- Where the version intended for use is not identical to the certified version(s), the conclusion that the differences are minor shall be supported by suitable and auditable analysis. Differences that affect the fundamental design concepts employed by the device, such as the physical principle that is exploited, the technology used, and the means of preventing systematic faults, are not minor. Differences in parameter settings that pertain to signal ranges would likely be minor.

e) The conditions of use assumed in the certification shall be relevant to the conditions of use in the intended nuclear application (see also 7.7).

f) The certifying authority shall be identified and be independent of the device designer and manufacturer.

g) The certifying authority shall be competent for the properties and / or measurements certified, and its competence shall be judged based on all available information regarding its experience and qualifications.

### 7.3 Avoidance of systematic faults

The criteria presented in this subclause apply particularly to intended applications of class 1 and class 2, but are also recommended for class 3. It should be noted that in the case of software and HPD, the assurance regarding avoidance of systematic faults is obtained primarily via analysis. By contrast, however, environmental conditions can also lead to systematic faults, but qualification can use analysis or testing following IEC 60780 as described in 6.6.

Evidence shall be documented that the device is free from potential causes of systematic faults. To define this for each class, this subclause uses tables wherein “M” indicates “mandatory”, corresponding to the use of “shall” in a requirement statement, and “R” indicates “recommended” corresponding to the use of “should”.

This shall be demonstrated by assessment of the overall architecture of the device, to provide assurance that:

a) The design of the device digital controller (i.e., the digital part of the device) shall be assessed. The following information shall be made available for the assessment as defined for each class in the table below:

| | Information to be available | Class 1 | | Class 2 | | Class 3 | |
|---|---|---|---|---|---|---|---|
| | | | CM | | CM | | CM |
| 1 | The overall functioning of the device digital controller, in normal and abnormal conditions (including faulted conditions) | M | DI | M | DI | M | DI |
| 2 | The overall architecture of the device digital controller, identifying and stating the roles of the main digital hardware (including programmable integrated circuits) and software components. | M | DI | M | DI | R | DI |

| | Information to be available | Class 1 | | Class 2 | | Class 3 | |
|---|---|---|---|---|---|---|---|
| | | | CM | | CM | | CM |
| 3 | All documents needed to verify compliance with the requirements of Clause 6, including verification strategy and tests or analysis performed. | M | CT | M | CT | M | CT |
| 4 | All documents needed to show that a verification of each development phase of the device was performed, including verification strategy and tests or analysis performed. | M | CT | M | CT | R | CT |

NOTE 1 The specification of the interpretation of the indicators “M”, “R”, “DI” and “CT” is given in 7.1.

NOTE 2 Where “DI” is shown, it indicates that documentation improvements made in accordance with 7.9 is a potential compensatory measure to clarify the system design.

NOTE 3 Where “CT” is shown, it indicates that documented complementary testing or analysis in accordance with 7.8 is a potential compensatory measure where there are gaps in the verification documentation.

b) The information regarding the overall functioning of the digital device shall in particular cover the particulars described in the table below as defined for each class:

| | Information to be available | Class 1 | | Class 2 | | Class 3 | |
|---|---|---|---|---|---|---|---|
| | | | CM | | CM | | CM |
| 1 | The general design approach (e.g., time-based design vs. event-based design, static vs. dynamic resource management, synchronous vs. asynchronous electronic design) | M | DI | M | DI | R | DI |
| 2 | The inputs (including interrupts) to, and the outputs of, the device controller | M | | M | | M | |
| 3 | How the inputs are processed to provide the outputs | M | CT | M | CT | M | CT |
| 4 | Clear identification and characterisation of all the factors that could affect the device behaviour during operation | M | CT | M | CT | R | CT |
| 5 | The various tasks (including interrupt handling) performed within the device | M | | M | | | |
| 6 | The sequencing and synchronisation of the tasks | M | | M | | | |
| 7 | The protection / separation of the tasks performing the primary function of the device from those performing the ancillary functions | M | | M | | R | |
| 8 | The factors influencing the response time and response time variability of the primary function | M | | M | | R | |
| 9 | The on-line and off-line test and diagnostic capabilities provided by the device | M | | M | | R | |
| 10 | Start-up, shutdown and reset conditions, including power transients including loss of power and restart, and device response | M | | M | CT | M | CT |

NOTE 4 The specification of the interpretation of the indicators “M”, “R” and “CT” is given in 7.1.

c) In accordance with the table below the indicated evidence shall be provided for each class to demonstrate that:

| | Information to be available or criterion to be met | Class 1 | | Class 2 | | Class 3 | |
|---|---|---|---|---|---|---|---|
| | | | CM | | CM | | CM |
| 1 | The primary function will not be adversely affected by any interrupt conditions | M | | M | | R | CT |
| 2 | Supported by documentation, the design of any self-monitoring measures is such that upon fault detection by the self-monitoring measures, the device will alarm or fail safe. | M | | M | CT | M | CT |

| | Information to be available or criterion to be met | Class 1 | | Class 2 | | Class 3 | |
|---|---|---|---|---|---|---|---|
| | | | CM | | CM | | CM |
| 3 | Faults that affect the primary function are detected by self-monitoring measures or by other means, such as periodic surveillance testing | M | CT | M | CT | R | CT |
| 4 | Analysis has been documented that determines possible residual failure mechanisms and failure modes (e.g., using a FTA, FMEA or criticality analysis), and demonstrates that measures have been taken to reduce the likelihood of the failure mechanisms and failure modes thereby revealed | M | | M | | | |

NOTE 5 For item 2, the reference to “fail safe” is based on the requirements of 6.2 item e).

NOTE 6 For item 4, possible measures could include focused additional testing, restriction in the use of the device, or external monitoring.

NOTE 7 For item 4, Annex A provides guidance on some software design features that could prove problematic in meeting the requirements of this subclause.

## 7.4 Evidence of quality in the design process

### 7.4.1 General

The criteria presented in this subclause provide assurance that the design process was systematic and follows the general principles exemplified by the life cycles defined in the related nuclear standards.

For all topics, the general approach shall be as follows:

- obtain evidence of the use of a quality-based development cycle from the device designer;
- compare the evidence available with the corresponding requirements of IEC 61513, this standard and other appropriate IEC standards specific to nuclear power plants; and
- determine whether any lack, omissions or discrepancies are acceptable or not, and whether the compensatory measures (if any) indicated for each requirement can complete the evidence required to conclude the candidate device is acceptable.

The subclauses below present the criteria which shall be examined according to the preceding paragraph.

### 7.4.2 Product designer’s QA program

The table below defines the requirements for a design QA program in terms of the information to be available or the criterion to be met. The requirements shall be applied by replacing “___” with “shall” where “M” is indicated and “should” where “R” is indicated in accordance with the table below:

| | Information to be available or criterion to be met | Class 1 | | Class 2 | | Class 3 | |
|---|---|---|---|---|---|---|---|
| | | | CM | | CM | | CM |
| a | The designer ___ have maintained and followed, and continue to follow, a documented QA program that ___ be evaluated in terms of the QA requirements of IEC 61513. This evaluation ___ identify any gaps and address them or provide justification for their acceptability. | M | | M | | R | |
| b | If parts of the processes of developing the software or hardware (including HPDs) are specified in quality documents other than the QA program, then these development quality documents (e.g. Software QA Plan) ___ be consistent with the overall QA program. | M | | M | | R | |
| c | If parts of the processes of developing the software or hardware (including HPDs) are specified in quality documents other than the QA program, then the requirements of this subclause ___ apply equally to these subsidiary quality documents. | M | | M | | R | |

| | Information to be available or criterion to be met | Class 1 | | Class 2 | | Class 3 | |
|---|---|---|---|---|---|---|---|
| | | | CM | | CM | | CM |
| d | The QA program **shall** require the following throughout the design and development process to the level indicated by “M” or “R”: | -- | | -- | | -- | |
| | 1) Persons performing design and development activities ___ be competent for the work assigned to them. | M | | M | OE CT | R | OE CT |
| | 2) The final design ___ be independently validated with a level of independence appropriate to the class of the intended application. | M | | M | | M | |
| | 3) Each phase of design and development ___ involve verification that the requirements of that phase have been met. | M | | M | | R | |
| | 4) Configuration management ___ be in place in accordance with 7.4.4. | M | | M | | M | |
| | 5) Change control ___ be in place in accordance with 7.4.5. | M | | M | | M | |
| | 6) Documentation practices ___ be in place in accordance with 7.4.6. | M | | M | | M | |
| e | Where tools were used in the design and development, the designer’s QA program shall have required them to be justified for the purpose to the level indicated by “M” or “R”. Where the justification of the tools is judged insufficient by the qualifier or application designer, then he shall consider what compensatory measures can and will be applied. | -- | | -- | | -- | |
| | 1) The tools’ history of use, their stability, their user documentation, notification of faults, etc. | M | CT OE | R | CT OE | | |
| | 2) Their potential to introduce faults or failure to detect faults in the device design as well as the likelihood of such tool failures being revealed through other means. | M | CT | M | CT | | |
| f | Where the designer and/or manufacturer permits the use of sub-contractors, all requirements of this standard that apply to the device manufacturer or designer ___ apply equally to the sub-contractors. | M | | M | | M | |

NOTE Relative to item e), a tool which can introduce a fault that cannot be detected by other means (e.g. human review) would require justification comparable to the class of the intended application of the device whose design depends on the tool. A tool that may fail to detect a fault, but which cannot introduce a fault would be considered at a lower class.

### 7.4.3 Design and development process

The table below defines the requirements regarding the design and development process in terms of the information to be available or the criterion to be met. The requirements shall be applied by replacing “___” with “shall” where “M” is indicated and “should” where “R” is indicated in accordance with the table below:

| | Information to be available or criterion to be met | Class 1 | | Class 2 | | Class 3 | |
|---|---|---|---|---|---|---|---|
| | | | CM | | CM | | CM |
| a | Development plans for software and hardware (including HPDs) ___ require that the design and development process follow a life cycle which divides the design and development into phases; | M | | M | | R | |
| b | For each phase in the design and development life cycle, the QA Plan ___ document the following:<br>– objectives,<br>– inputs and outputs,<br>– tools used. | M | | M | | R | |
| c | Evidence ___ be available that all the above requirements were complied with during the development of the specific device. This evidence ___ be documented in retrievable and reviewable form. | M | CT | M | CT | R | CT OE |

NOTE Standards that require suitable life cycles include: IEC 61513 (for system level design), IEC 62138 and IEC 60880 (for software), IEC 60987 (for bespoke computer-based hardware), IEC 61508 (for software and hardware), or IEC 62566 for HPDs.

### 7.4.4 Design configuration management

The table below defines the requirements regarding design configuration management to be available or the criterion to be met. The requirements shall be applied by replacing "___" with "shall" where "M" is indicated and "should" where "R" is indicated in accordance with the table below:

| | Information to be available or criterion to be met | Class 1 | | Class 2 | | Class 3 | |
|---|---|---|---|---|---|---|---|
| | | | CM | | CM | | CM |
| a | Evidence ___ be documented of the use of a configuration management system concerning the development of the candidate device, its software and hardware (including HPDs). This configuration management system ___ include all design documentation and validation test procedures and test reports and these ___ be linked with the versions of the hardware, software and HPD; | M | CT | M | CT | M | CT |
| b | The configuration management system ___ have been in place for all artefacts (documents, design reviews, software and HPD designs, hardware drawings, test results, etc.) from the beginning of development of the device; | R | | R | | | |
| c | The configuration management system ___have been in place for all artefacts (documents, design reviews, software and HPD designs, hardware drawings, test results, etc.) from the beginning of validation testing of the device. | M | | M | | M | |

### 7.4.5 Design change control

Evidence shall be documented that the device designer currently maintains a change control system, including procedures and software-based tools, that to the degree indicated by "M" or "R" in accordance with the table below:

| | Information to be available or criterion to be met | Class 1 | | Class 2 | | Class 3 | |
|---|---|---|---|---|---|---|---|
| | | | CM | | CM | | CM |
| a | Supports and requires the convening of a review committee operating under a managed process for reviewing and approving changes that shall authorize all changes and record its decisions. | M | | M | | M | |
| b | Supports and requires that all changes to hardware, software and HPD design and documentation include reference to the change authorisation. | M | | M | | R | |
| c | Systematically collects and tracks field problem reports, manufacturing problems that impact design, and test anomalies as inputs to the change control process.<br>NOTE This standard cannot prescribe the feedback chain for field problem reports where the end-user should report a problem to a distributor, manufacturer or designer. The essential element is that the end-user be provided a point of contact that provides appropriate communication to the party best able to address the reported problem. | M | | M | | R | |
| d | Tracks all versions and releases of the software and HPD design or hardware configuration and can report the changes that have been identified and that have been rectified at each version or release. | M | | M | | R | |
| e | Supports and requires an impact analysis of each proposed change, and use of this impact analysis in the change approval process. This impact analysis shall include consideration of the extent of the change, its impact on the primary functions of the candidate device, its potential for adversely affecting the reliability of the primary functions, the part of the realisation life cycle where work shall begin, and the extent and rigour of validation testing required. | M | | R | | | |

| | Information to be available or criterion to be met | Class 1 | | Class 2 | | Class 3 | |
|---|---|---|---|---|---|---|---|
| | | | CM | | CM | | CM |
| f | Supports and requires a second review of the authorised change by the change review committee to authorise its release to manufacturing, during which the change review committee shall base its approval upon a review of the completeness and accuracy of:<br>– the change documentation;<br>– the re-validation documentation; and<br>– the user documentation. | M | | R | | | |
| g | Has been in place from the beginning of development of the specific model of the device. | R | | R | | | |
| h | Has been in place from the beginning of validation testing of the specific model of the device. | M | | M | | M | |

It is entirely possible to design a change control process that involves two levels of change review committee, provided that there are clear procedures and rules so that the lower level committee can recognize that a change comes under the authority of the higher level committee for consideration. These rules may consider the class of system affected by the change, the magnitude of the change or other suitable criteria.

### 7.4.6 Design documentation

The design documentation is part of the 'documentation for safety' that is examined as part of evaluation. The other part of 'documentation for safety', that is supplied to the users who will design systems using the device or who will operate and maintain these systems, is addressed in 6.9.

The table below defines the requirements for design documentation in terms of the information to be available or the criterion to be met. The requirements shall be applied by replacing "___" with "shall" where "M" is indicated and "should" where "R" is indicated in accordance with the table below:

| | Information to be available or criterion to be met | Class 1 | | Class 2 | | Class 3 | |
|---|---|---|---|---|---|---|---|
| | | | CM | | CM | | CM |
| a | All documents ___ be verified and approved by authorized persons. | M | | M | | R | |
| b | All documents ___ be complete, correct, and unambiguous. | M | DI | M | DI | R | DI |
| c | Functional Requirements Documentation:<br>A functional requirements document defines the functions of the device, whether implemented in hardware, software or HPD. This document specifies in explicit language the primary functions, the ancillary and superfluous functions (if any) and any restrictions on the use of the device.<br>The device designer shall have produced documentation covering the functional requirements that provides the following information to the degree indicated by "M" or "R": | -- | | -- | | -- | |
| | 1) The primary, ancillary and superfluous functions provided by the device | M | | M | | M | |
| | 2) If relevant, the means to ensure the primary functions are protected from all intended and unintended actions of the ancillary and superfluous functions | M | | M | | R | |
| | 3) The self-surveillance functions provided and their actions upon detection of failures | M | | M | | R | |
| | 4) The internal interfaces between modules of the device | M | | R | | - | |
| | 5) The external interfaces of the device | M | | M | | M | |
| | 6) The roles, types, formats, ranges and constraints of inputs, outputs, exception signals, parameters and configuration data, where appropriate | M | | M | | M | |

| | Information to be available or criterion to be met | Class 1 | | Class 2 | | Class 3 | |
|---|---|---|---|---|---|---|---|
| | | | CM | | CM | | CM |
| | 7) The different modes of behaviour and the corresponding conditions of transition | M | | M | | M | |
| | 8) Any constraint to be respected when using the device | M | | M | | M | |
| | 9) Response times, bandwidth and other dynamic parameters needed to fully understand the device's functions and limitations | M | CT | M | CT | M | CT |
| | 10) Environmental limitations (see 6.6) | M | CT | M | CT | M | CT |
| | 11) If relevant, security provisions to protect settings from accidental or malicious change | M | DI | M | DI | M | DI |
| d | Principle of operation documentation:<br>The documentation describes the theory underlying the principles of operation of the device and device design and overall functioning of the hardware, and the software and HPD with sufficient detail that the efficacy of the verification and validation of the device can be assessed; | M | DI | M | DI | M | DI |
| e | Hardware documentation<br>Hardware documentation describes the overall structure of the hardware, the hardware component functions and properties (including robustness properties – see 6.6) that are used in the design and in interaction with the software or HPD, to a degree of detail that would be required to competently modify the hardware to accommodate a replacement component that is not identical to the original | M | DI | M | DI | M | DI |
| f | Description of the software and HPD<br>This documentation describes the overall structure of the functional logic implemented in software or HPD, its decomposition to a modular level at which any maintenance or modifications would require knowledge, and details of the interaction between the conventional hardware and the software or HPD | M | DI | M | DI | R | DI |
| g | Verification and test records at each phase of design. For software and HPD, this will include unit tests (for class 1), integration tests and validation tests | M | CT | M | CT | R | CT |
| h | Version identification information that can be authenticated during installation at site | M | | M | | M | |
| i | User documentation for safety as described in 6.9 | M | DI | M | DI | M | DI |
| j | Modification history – a report or extractable report from the configuration management system that identifies the revision history of the product as required by 7.4.4 | M | | M | | R | |

## 7.5 Evidence of quality in manufacturing

Quality assurance in manufacturing is important in that it can provide the basis for accepting devices of the same or similar models which may be manufactured at a later time, even though factors such as availability of identical components may affect the device.

The table below defines the requirements for evidence of quality in manufacturing in terms of the information to be available or the criterion to be met. The requirements shall be applied by the replacing "___" with "shall" where "M" is indicated and "should" where "R" is indicated in accordance with the table below:

| | Information to be available or criterion to be met | Class 1 | | Class 2 | | Class 3 | |
|---|---|---|---|---|---|---|---|
| | | | CM | | CM | | CM |
| a | Evidence ___ be documented that the supplier maintains a manufacturing QA program comparable to ISO 9001 | M | | M | | M | OE PS |
| b | Evidence of compliance with the manufacturing QA program ___ be documented | M | | M | | R | |

| | Information to be available or criterion to be met | Class 1 | | Class 2 | | Class 3 | |
|---|---|---|---|---|---|---|---|
| | | | CM | | CM | | CM |
| c | Evidence ___ be documented that shows that the manufacturer maintains a supplier qualification program that:<br>– performs incoming inspection,<br>– performs first issue inspection and/or testing,<br>– controls changes and substitutions of components, and<br>– reports changes and substitutions to the design organisation | M | | M | | R | OE |
| d | Evidence ___ be documented that the manufacturer performs appropriate operational tests and burn-in of the device<br>NOTE "CT" in this case refers to the end-user performing burn-in. | R | CT | R | CT | R | CT |
| e | Evidence ___ be documented of the versions and serial numbers of test equipment used for functional testing, and that this test equipment calibration meets appropriate standards for calibration. | M | CT | M | CT | R | CT |
| f | Evidence ___ be documented that there are mechanisms in place to ensure that only known and verified software and HPD configurations are installed in the device during manufacturing. | M | | M | | M | |
| g | Evidence ___ be documented that the manufacturer maintains records of the date of manufacture, complete version information and serial number of devices as they are manufactured. | M | | M | | R | |
| h | Evidence ___ be documented that the manufacturer affixes to each unit shipped the complete identity of the version or release information pertaining to that unit (this may be a human-readable label or an electronically readable internal parameter). | M | | M | | M | |
| i | Evidence ___ be documented that the manufacturer facilitates the reporting of field problems related to the device, and systematically collects and tracks field problem reports related to the device design, and reports these to the device designer.<br>NOTE This standard cannot prescribe the feedback chain for field problem reports where the end-user should report a problem to a distributor, manufacturer or designer. The essential element is that the end-user be provided a point of contact that provides appropriate communication to the party best able to address the reported problem. | M | | M | | R | |
| j | The impact of the stability of the manufacturing process ___ be considered | M | OE<br>PS<br>CT | M | OE<br>PS<br>CT | R | OE<br>PS<br>CT |

### 7.6 Product stability

The criteria presented in this subclause examine the evidence of the maturity of the product and the likelihood that the product will remain unchanged and that the supplier will be capable of supporting it throughout the life of its installation in the nuclear power plant. It is also a measure of the thoroughness with which impact analysis is used in change control and the application of the full rigour of the design process to changes, including appropriate regression testing. The stability of the product is closely related to its operational experience, and where operational experience is relied on as a factor in the evaluation, product stability is essential.

a) Product stability shall be assessed in terms of the volume of changes to the primary function, the volume of changes having the potential to affect the primary function, the volume of changes affecting other functions, the impact of any of the changes on the primary function, and the reasons for these changes (such as bug correction, substitution of obsolete parts, regulatory changes, etc.).

NOTE A low frequency of corrective changes over a significant period of use of the product may indicate to a degree the stability and correctness and/or soundness of the product design.

b) The assessment as per item a) shall be based upon maintenance records supported by change control and configuration management tools and procedures that shall meet the requirements of 7.4.4, 7.4.5, and 7.5.

c) The stability of the product shall be assessed taking the volume of installations and applications into account and shall be credited only if the product has exhibited a meaningful amount of manufacture and use of the product,

d) Where product stability is applied, it shall be applied to support weak or missing evidence for specific criteria in clauses 7.3, 7.4 or 7.5 where the pertinent subclause allows product stability to be applied, or where it supports the application of operational experience.

### 7.7 Operating experience

The criteria presented in this subclause examine the evidence of the robustness of the product in the face of operating environments and operating profiles similar to and at least as challenging as the intended application. Such evidence is important because it represents exercising the device with operational profiles that may supplement the testing of the candidate device beyond the limited number of test cases that can be exercised during development.

a) All of the credited evidence of operating experience shall be auditable.

b) The identity of the reporting organisation or organisations shall be documented.

c) Operating experience evidence shall be correlated to precisely known versions of the software and HPD.

d) Operating experience evidence shall be correlated to known configuration settings of the hardware and software and HPD.

e) Where operating experience is to be credited for versions of the software, HPD or hardware other than the version to be used, justification shall be provided that analyses the differences between these versions, and these analyses shall be used to determine the degree to which the operating experience of each version of the device may be credited.

Complementary testing may serve to permit crediting some earlier software and HPD versions in the operating experience.

f) The analysis of the operating experience evidence shall take into account whether the specific functions of the candidate device operate on a continuous basis or intermittently on-demand. In the first case, the basis of the evidence shall be the hours of actual operation; in the latter, the basis of evidence shall be the number of executions (including surveillance tests) without failure of the on-demand functions.

g) All aspects of the functions of the candidate device in the intended application shall be covered by the operating experience.

h) The coverage and volume of operating experience shall be sufficient to provide confidence in the candidate device commensurate with the class of the intended application.

i) The coverage and volume of operating experience shall be sufficient to provide confidence in the candidate device commensurate with the complexity of the device, considering both software and HPD and other hardware.

j) Where the operating experience is a major or heavily-weighted criterion for evidence of correctness, the volume and breadth of the operating experience is crucial, so the volume and source of the required operating experience data shall be justified.

   The sufficient operating time should be determined on a case-by-case basis using engineering judgement. This judgement should take into account notably the anticipated reliability level required at system level for the functions in which the device is used.

   For intended applications of class 1, the operating experience should be based on several applications from a number of reporting organisations.

There is no requirement for the operating experience to have been realized at a nuclear facility. The intent of the requirement is that the coverage and volume of operational experience be carefully documented (which may not be the case in industrial environments) and pertinent to the operational profile to be experienced by the candidate device in the intended application (see item k) below).

NOTE IEC 61508-7, Annex D provides information relating the volume of operating experience to reliability criteria.

k) The credited operating experience shall include conditions of operation that are as challenging as in the intended application. These conditions shall include the following as applicable:

- process conditions (e.g., temperature, pressure, viscosity, particle content, etc.) for wetted devices such as valves or sensors (refer to 6.6);
- hardware operating environment (e.g., temperature, humidity, vibration, EMI, radiation) (refer to 6.6);
- operating profile or method of use (such as speed of transients like a start-up of a compressor or harmonics seen by an inverter being fed from a generator instead of the grid) if this can in any way affect the operation of the candidate device in terms of software loading;
- interfaces with other devices.

l) Evidence shall be documented that a reliable system of failure reporting has been set up and is in use so that operational experience can be estimated with a high degree of confidence. Where all failures or abnormal operation may not have been reported, the estimated operational experience shall be discounted so as to reflect the uncertainty in the accuracy of the failure reporting system.

For example, where no firm evidence exists that all failures are reported, the estimated operational hours may be discounted by 30 % within the warranty period and 50 % or more beyond it.

m) Where the operational experience indicates an incidence of apparent random hardware failures exceeding the predicted rate, then consideration shall be given to the possibility that systematic faults may exist in the device, such as a fault in the software or HPD design, environmental weakness of a sub-component, etc.

n) Where operational experience is applied, it shall be applied to support weak or missing evidence for specific criteria in 7.3, 7.4 or 7.5 where the pertinent subclause allows operational experience to be applied.

### 7.8 Complementary testing and/or analysis (verification)

Complementary testing may be used for a variety of reasons. These may include confirmation of the applicability of earlier versions of a device in the operational experience, confirmation of device modifications, closure of gaps in validation tests, compensation for some shortfall in operating experience, or confirmation of correctness or robustness under the applicable operating conditions.

Complementary testing may also be used to compensate for gaps in the design process (or knowledge of it), design documentation (especially omissions in the functional requirements and validation testing), documentation covering responses to specific input conditions (such as abnormal inputs), and for the lack of specific operational experience by identifying in detail the response to specific inputs, or to test device robustness toward specific stresses.

Examples of the kinds of the tests that may be applied include:

- fault insertion tests to confirm that the self-supervision functions detect each fault and result in fail-safe device outputs;
- specific tests to confirm the performance of low demand or poised functions (i.e. those which wait for a detection of a specific event, as opposed to functions that operate continuously) for which operational experience is by definition difficult to accumulate;
- specific tests to confirm the parts of the device's functional behaviour that are incompletely or ambiguously documented;
- specific tests related to a modification to confirm that it is acceptable to include prior versions in the credited volume of operational experience;

- specific tests to determine the response of the device to out-of-range or failing inputs, (such as a 4 mA to 20 mA input of less than 4 mA input, or downward drift in a power supply to an analog input and instrument loop) and determine the acceptability of this response in the target application;
- statistically valid random testing, such as described in IEC 61508-7, Annex D. Note that it may be quite difficult to meet the pre-requisites for such testing;
- complementary tests to confirm that in the configuration(s) and intended conditions of use, the device meets its functional and performance requirements;
- specific tests to confirm the non-perturbation of primary function by superfluous or ancillary functions;
- specific tests to confirm the efficacy of security and safety-oriented mechanisms.

NOTE The reference to “fail safe” is based on the requirements of 6.2 item e).

Where complementary testing is used in the evaluation of a candidate device, the following shall apply, and be documented and available for review:

a) The documentation of the tests shall include identification of the precise version of the product being tested.

b) The functions tested shall be documented (this shall include the test procedure, the test data, and the expected test results and the observed results).

c) The tests shall be designed with respect to the intended application to demonstrate that the device’s behaviour is consistent with the requirements of the application, including marginal and exceptional conditions.

d) The test results shall be reviewed with respect to the intended application to demonstrate that the device’s behaviour is consistent with the requirements of the application.

e) The test environment shall be representative of the intended application, or reasons why deviations are acceptable shall be documented.

f) Where the intended application is of class 1 or class 2, the basis of the tests shall be documented so as to explain why the test results will demonstrate what is required (this may for example include an analysis or model of the software, the HPD or other hardware design features which are being tested).

g) The identity of the organisation conducting the test shall be recorded.

h) Where complementary testing or analysis is applied, it shall be applied to support missing evidence for specific criteria in clauses 7.3, 7.4 or 7.5 where the pertinent subclause allows compensatory testing or analysis.

### 7.9 Documentation improvement

In many cases, it is possible to compensate for weaknesses in the documentation available from the designer or manufacturer by generating improvements in the body of documentation during the evaluation process or in accordance with the EAR.

One kind of documentation improvement is often called “document reconstitution”. This is usually based on using complementary testing to implement a form of reverse-engineering aimed at clarifying the design specification and the validation test procedure. In document reconstitution, the final product is not modified in any way, and a draft black box specification of the product is prepared from all available information, including support from the designers. From this draft specification, a test procedure is developed and executed. The differences between test expectations and test results are used to modify the draft product specification and the test specification and the whole process is repeated iteratively until the accuracy of the specification is confirmed by successful tests.

If documentation improvement is used as a compensatory measure then the following shall apply:

a) There shall be a solid pre-existing foundation for the improvements in the documentation consisting of either a complete functional description, or a combination of software and hardware description as well as a description of the principle of operation.

NOTE 1 The intent is to build upon documentation prepared by the designer, not to create the documentation from scratch. This is because a major lack of consistent documentation that truly explains the product's workings is an indication of weakness in the approach of the designer that calls into question the design itself.

b) All improvements in the documentation describing the functionality of the design shall be reviewed by the designer of the candidate device.

NOTE 2 The intent is to ensure technical correctness in the critical areas of product design that are key to the defences of the principal function against ancillary or superfluous functions under all demand profiles.

c) Where complementary testing is used as part of the methodology of reconstituting the documentation, this testing shall comply with 7.8.

d) Where document improvement is applied, it shall be applied to support weak descriptions for specific criteria in clauses 7.3, 7.4 or 7.5 where the pertinent subclause allows for document improvement.

# 8 Criteria for integration into the application – limits and conditions of use

## 8.1 General

This Clause addresses possible limits and conditions that may restrict the use of the candidate device. These conditions and limitations may arise either from the results of the suitability evaluation, or may be imposed so as to partially qualify a device for use under the imposed limitations and conditions. The EAR (see 5.3.3) and the user documentation for safety (see 6.9) covering the candidate device shall document all restrictions.

## 8.2 Restrictions on use

A candidate device may be evaluated as qualified for use in certain applications provided that its use is subject to certain limitations and conditions.

The EAR shall identify the following:

- the highest class for which the candidate device is qualified for use;
- where applicable, the specific applications for which the candidate device is qualified for use;
- the reliability limits which the device can achieve, alone or in redundant configuration;
- specific options or secondary functions that shall be enabled or disabled, including specific parameter settings required for each class;
- the limits of the operating environment (as per 6.6) for which the candidate device is qualified to be operated;
- limiting factors affecting operational lifetime (such as the use of aluminium capacitors);
- any special measures that shall be observed during operation or testing in order to ensure safe use of the device.

## 8.3 Modifications of the device required for the application

A candidate device may be evaluated to be qualified for use in certain applications if certain modifications to the hardware or possibly extremely minor modifications to the software of the device are made prior to use. This can sometimes be necessary, for example in retrofit applications where form-fit is a concern or where impedance matching may be required, but it is essential that such modifications do not have the effect of creating a new device in which case this standard would no longer apply.

For example, some potential candidate devices may have secondary functions such as HART, which is implemented by superimposing high frequency signals on the 4 mA to 20 mA process

signal. It may be required to disable this option or to use a low-pass filter so that the high frequencies do not affect other devices in the target system.

Where it is necessary to modify the device in any way, the following shall apply:

a) The EAR shall:
   - identify the changes required, and
   - verify the extent of support for these changes from the device designer.

b) All the modifications to the device design shall be such that they do not invalidate the operating experience credited in the evaluation. The modifications shall not conceptually change the primary function of the candidate device.

c) All modifications shall be small in scale, confined in extent, and simple to verify and validate.

d) All modifications shall be performed under all of the requirements given in 7.4 and in a manner consistent with the class of the intended application.

e) The EAR shall be revised following the modifications and this revision shall take all factors into account that could affect the conclusions of the report.

### 8.4 Modifications to the system to accommodate the device

A candidate device may be evaluated to be qualified for use in certain applications if certain modifications to the system are made prior to use. This subclause is particularly applicable to retrofits where for example an interposing relay may be needed to provide the necessary interfaces between the candidate device and other system components.

In such cases, the following issues shall be considered and documented in the evaluation of the candidate device:

a) The EAR shall address the possible changes to the system design that may be required, including the following:
   - additional equipment to monitor for a failure;
   - additional redundancy or diversity required;
   - the need for inter-channel comparisons;
   - re-allocation of a function to a different sub-system;
   - changes resulting from protection against environmental conditions such as additional shielding, ventilation, cooling, etc;
   - changes in maintenance and/or operating practices.

b) The EAR shall address the training requirements at the system level that will arise from use of the candidate device.

c) The EAR shall be revised following the modifications and this revision shall take all factors into account that could affect the conclusions of the report.

### 8.5 Integration and commissioning of the device in the plant safety systems

A candidate device qualified for use in a given application will eventually be commissioned and integrated into a new build or retrofitted into a safety system of the plant.

Two situations should be distinguished here:

- Applications where the newly qualified device is used singly, in a way that does not carry the risk of causing the complete failure of a plant safety function, and
- Applications where the newly qualified device is used in all channels of a system or in a single potential point of failure so that there is a risk of this device causing the complete failure of a plant safety function, such as a protection device of a safety system power supply.

Based on the EAR, the Commissioning/Integration Plan shall be prepared and it shall:

a) Incorporate the relevant requirements of Clause 6 of IEC 61513.

b) Incorporate recommendations and restrictions documented in the EAR and the supplier's commissioning instructions.

c) In the second case above, or if there are any remaining aspects of device functionality to be validated, the Commissioning/Integration Plan shall also

   1) consider a stepwise introduction of the candidate device into a system, addressing the possibility of an initial validation period where the candidate device is commissioned in only one channel or train of a redundant system, to permit evaluation of the device in operation in the actual target system;

   2) define suitable means to ensure and verify correct parameter settings in all devices implemented in the system, including those specified in the EAR;

   3) specify commissioning test cases based on the dynamic aspects of the safety systems (transients), where:

      - selection of particular test scenarios should be based on system modelling and simulations;
      - these tests shall consider device response times and the correct sequence and priority of protective actions; and
      - for devices protecting power supply systems, the test cases should include whole sequences of the system start-up, and stress testing of selected safety systems.

   4) require recording of the following during commissioning:

      - all deviations of the device function from data of the EAR. Small deviations shall not be neglected as they can indicate serious deficiencies in the software or HPD designs of the device;
      - values of all parameter settings of the device;
      - all test results, up to the final device integration into the system.

# 9 Considerations for preserving acceptability

## 9.1 General

In the evaluation of a candidate device, the device may appear to be ideal in terms of functional suitability and evidence of correctness, but the product lifetime of the device and long-term support from the supplier should be weighed as a factor because of the long service lifetimes of nuclear plants.

This clause identifies criteria for evaluating the candidate device from this perspective, particularly from the perspective of maintainability of software and HPD.

## 9.2 Notifications by the device designer and manufacturer

Appropriate measures shall be taken to guarantee that the user be formally warned of any modification of a qualified device. In the event that a modification to the hardware software or HPD is made, an impact analysis shall be performed and the device shall be re-qualified in accordance with this standard.

The candidate device should be evaluated in terms of notifications of failures from the manufacturer or designer that occur after the period of evaluation of the operational experience when the device may be in service. Learning of a failure at another installation could be used to initiate preventative maintenance or device replacement.

The evaluation should consider the following factors and report the results of attempting to obtain the manufacturer's (and designer's) agreement to:

- provide notification in a timely way of every failure at other installations;
- include in the notification analysis that could help determine if a defect could possibly affect the primary function or reduce its immunity to ancillary and superfluous function failures;
- make available a current defect list that identifies the possible effects of reported failures, their current resolution status, and the precise versions that are affected;
- provide notification of every change, whether a hardware component substitution, change to a manufacturing process, or change to the software or HPD.

### 9.3 Manufacturing and support lifetime of the current version

The candidate device should be evaluated in terms of the expected lifetime of the product support for the candidate device, as well as the lifetime of the device itself. In the first case, longer support periods are desirable and possibly negotiable. In the second case, this knowledge serves to plan the replacement of the device before the end of the service lifetime of the device.

The evaluation should consider the following factors and document them in the EAR:

- product lifetime of the current version and of the device in general;
- service lifetime of the current version and of the device in general;
- the willingness of the manufacturer or designer to warn of retirement of the version and the device in general;
- the supplier's willingness to commit to plug compatibility of future replacements;
- the supplier's willingness to commit to functional compatibility of future replacements;
- the impact of customized modifications required for the application.

### 9.4 Preservation of maintenance tools and documentation

The life cycle of nuclear power plants is much longer than that of digital devices, so obsolescence should be considered in the evaluation of a device. The evaluation should consider whether the device designer is willing to provide a contractual commitment (e.g. in an escrow arrangement) or to give assurances that the following would be available if the designer or manufacturer decides to discontinue support of the candidate device:

- installation copies of configuration tools such as editors, compilers;
- a copy of the operating environment of these tools (e.g. specific version of Unix or Windows);
- copies of all source files, build files, libraries, etc., from the configuration management system;
- special hardware tools (e.g. PROM burners, logic analyzers);
- manufacturing drawings;
- copies of all documentation (specifications, test reports, etc.); and
- a detailed description of the computer hardware and accessories required for use of the operating system, tool software and tool hardware, or the actual equipment.

### 9.5 Recommendations for the end-user

The following are recommended to support the long-term use of the candidate device, and would be implemented by the utility operating the nuclear plant outside of the evaluation of the device:

- maintain a configuration management system independently from the supplier to address:
  - all modifications to configuration parameters;

  - all initial modifications as documented in the EAR;
  - all versions received from the supplier and their installation and configuration status;
- maintain a change control system with effective impact analysis;
- perform validation tests after all configuration changes (even parameter changes);
- maintain copies of configuration tools such as editors, compilers;
- where a device is used in applications of different classes, maintain all supporting activities as appropriate for the highest class.

# Annex A
(informative)

## Possible design features of a software system that could impact the dependability of the device

This annex is intended to suggest possible guidance in verifying conclusions reached while evaluating the design for properties that tend to avoid systematic faults (7.3).

The information herein is particularly intended for applications of class 1 or class 2, but may be applied to class 3. It should be noted that in the case of software, the assurance regarding avoidance of systematic faults is obtained primarily via analysis. By contrast, however, environmental conditions can also lead to systematic faults, but qualification can use analysis or test following IEC 60780 as described in 6.6.

As described in 7.3, evaluation of the robustness of the design to avoid systematic faults starts with examining the overall system design. This may in the case of software lead to examining possible mechanisms in the design which are widely recognized to be sources of potential problems. This list below is not intended to be exhaustive, but can serve as a starting point.

a) Sensitivity to the demand profile can affect the CPU loading, the order of servicing of interrupts, etc. The following are examples of possible contributors to device failure that could be pertinent:

   - interaction between two or more inputs,
   - signal behaviour (e.g. short out-of-range bursts) due to EMI,
   - overload due to cascading events detected at inputs,
   - violation of worst-case timing considerations.

   NOTE IEC 60880 (applies to class 1 systems) imposes the requirement that the software scheduling shall be deterministic, and IEC 62138 (applies to class 2 systems) requires that the software shall enable predictable run-time behaviour. Effectively, this standard seeks that a suitable worst-case analysis demonstrates that the electronic component(s) providing the primary functionality will always run on time or respond within the specified time.

b) Where the architecture of the design suggests weaknesses in the fundamental approach that could reduce the level of assurance that the required system properties are met (taking into account the level of assurance appropriate to the class of the application), it may be of value to examine the design for the presence of specific design features that could be pertinent

   For intended applications of class 1, one may be concerned with:

   - pre-emptive scheduling, and
   - all causes listed for class 2 and class 3.

   For intended applications of class 2, one may be concerned with:

   - dynamic objects created in real time;
   - garbage collection;
   - any but the simplest use of pointers (e.g. use of pointer arithmetic);
   - asynchronous access to or locking of resources;
   - time or date dependencies affecting the primary function(s), and
   - all causes listed for class 3.

   For intended applications of class 3, one may be concerned with:

   - communication overloads affected by other devices (such as a chattering node);

- unmonitored or unconstrained use of stack or heap;
- scheduling dependent upon inputs;
- recursion;
- dynamic task priorities;
- high system loading, measured in terms of CPU time or memory utilisation.

c) For applications of class 1, it is difficult to ensure that the primary function will execute on time if the design relies upon any but the simplest use of interrupts, or where they are used in the design of secondary functions where they can impact system loading and thereby indirectly impact primary functions

d) Particularly for applications of class 1 and class 2, systematic faults are considered less likely where the software has been designed using:

- a naming convention;
- avoidance of potentially dangerous language constructs whose interpretation by the compiler or interpreter may be non-standard.

e) For intended applications of class 1 and class 2, it is desirable to use an appropriate static analysis of the source code.

f) Self-monitoring measures, such as logical program flow monitoring, assertions, etc., can be useful, especially where these features are used to issue an alarm or make the device fail safe.

## Bibliography

IEC 61508-1:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements*

IEC 61508-2:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems*

IEC 61508-3:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 3: Software requirements*

IEC 61508-4:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 4: Definitions and abbreviations*

IEC 62003:2009, *Nuclear power plants – Instrumentation and control systems important to safety – Requirements for electromagnetic compatibility testing*

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 62645, *Nuclear Power Plants – Instrumentation and control important to safety – Requirements for security programmes for computer-based systems* (to be published)

IAEA Safety Glossary Terminology Used in Nuclear Safety and Radiation Protection 2007 Edition

Licensing of safety critical software for nuclear reactors – Common position of seven European nuclear regulators and authorised technical support organisations, 2010 edition

_____

# SOMMAIRE

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

# CENTRALES NUCLÉAIRES DE PUISSANCE – INSTRUMENTATION ET CONTRÔLE-COMMANDE IMPORTANTS POUR LA SÛRETÉ – SÉLECTION ET UTILISATION DES APPAREILS NUMÉRIQUES À FONCTIONNALITÉS LIMITÉES

## AVANT-PROPOS

1) La Commission Electrotechnique Internationale (CEI) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de la CEI). La CEI a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. A cet effet, la CEI – entre autres activités – publie des Normes internationales, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de la CEI"). Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec la CEI, participent également aux travaux. La CEI collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
2) Les décisions ou accords officiels de la CEI concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de la CEI intéressés sont représentés dans chaque comité d'études.
3) Les Publications de la CEI se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de la CEI. Tous les efforts raisonnables sont entrepris afin que la CEI s'assure de l'exactitude du contenu technique de ses publications; la CEI ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.
4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de la CEI s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de la CEI dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de la CEI et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
5) La CEI 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 la CEI. La CEI 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 la CEI, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de la CEI, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de la CEI ou de toute autre Publication de la CEI, ou au crédit qui lui est accordé.
8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.
9) L'attention est attirée sur le fait que certains des éléments de la présente Publication de la CEI peuvent faire l'objet de droits de brevet. La CEI 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 CEI 62671 a été établie par le sous-comité 45A: Instrumentation et contrôle-commande des installations nucléaires, du comité d'études 45 de la CEI: Instrumentation nucléaire.

Le texte de cette norme est issu des documents suivants:

| FDIS | Rapport de vote |
|---|---|
| 45A/898/FDIS | 45A/907/RVD |

Le rapport de vote indiqué dans le tableau ci-dessus donne toute information sur le vote ayant abouti à l'approbation de cette norme.

Cette publication a été rédigée selon les Directives ISO/CEI, Partie 2.

Le comité a décidé que le contenu de cette publication ne sera pas modifié avant la date de stabilité indiquée sur le site web de la CEI sous "http://webstore.iec.ch" dans les données relatives à la publication recherchée. A cette date, la publication sera

- reconduite,
- supprimée,
- remplacée par une édition révisée, ou
- amendée.

# INTRODUCTION

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

La présente norme CEI s'intéresse plus particulièrement à la sélection et à l'évaluation des appareils dédiés prédéveloppés, présentant des fonctionnalités particulières et limitées ainsi que des possibilités de configuration limitées, devant être utilisés dans des centrales nucléaires de puissance. La conception de ces appareils intègre du logiciel ou des circuits numériques spécifiés à l'aide de langage de description du matériel. Lesdits appareils ont été produits en respectant des normes non nucléaires reconnues, mais pas des normes de la série du SC 45A de la CEI.

L'objectif de la présente norme est d'être utilisée par les concepteurs de centrales nucléaires, les exploitants de centrales nucléaires, les évaluateurs de système et par les régulateurs.

La présente norme s'intéresse à deux aspects qui ne sont pas couverts par les autres normes de la série du SC 45A de la CEI, en effet:

– d'autres de ces normes couvrent les aspects liés au matériel des appareils contenant du logiciel ou couvrent des appareils de type complexe tels que les PLCs qui contiennent du logiciel qui peut être beaucoup plus complexe[1] que celui contenu dans les appareils couverts par la présente norme,

– d'autres de ces normes s'intéressent aux appareils conçus spécifiquement pour les applications nucléaires alors que l'objectif de la présente norme est de s'intéresser aux points qu'il est nécessaire de considérer pour pouvoir utiliser dans des centrales nucléaires de puissance des appareils qui n'ont pas été conçus pour être utilisés dans ce cadre.

Les concepteurs des systèmes d'I&C des centrales nucléaires de puissance sont de plus en plus forcés d'avoir recours à ce type d'appareil pour des raisons liées par exemple à l'obsolescence des équipements, à la petite taille du marché nucléaire comparé à d'autres marchés industriels, et aussi à cause du nombre grandissant de fournisseurs qui choisissent de concevoir leurs produits en faisant référence à des normes génériques de sûreté telles que celles de la séries CEI 61508.

Ainsi, il devient vital pour les concepteurs de ces systèmes d'avoir les recommandations établies par la présente norme, afin d'être capable de choisir et d'évaluer les appareils candidats pour juger de leur aptitude à être employés dans les centrales nucléaires de puissance. La présente norme fournit des recommandations sans lesquelles les concepteurs seraient obligés de s'interroger sur la façon d'interpréter les CEI 60880, CEI 62138 ou CEI 62566 pour les sujets couverts.

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

La CEI 61513 est la norme du SC 45A de la CEI de premier niveau qui fournit des recommandations applicables à l'I&C au niveau système. Elle est complétée par des recommandations applicables au niveau appareil par la CEI 60987 pour la conception du matériel et par les CEI 60880 et CEI 62138 pour le logiciel et par la CEI 62566 pour des appareils potentiellement complexes. Toutes ces normes couvrent des conceptions qui sont spécifiquement nucléaires et appliquent le concept de cycle de vie.

La CEI 62671 est le document du SC 45A de la CEI de deuxième niveau qui traite de la question particulière du choix et de l'évaluation des appareils à utiliser dans les centrales

---

1 Il n'y a pas de définition reconnue de la « complexité », mais lorsque les appareils sont support de beaucoup de fonctionnalités, il s'en suit une augmentation de la quantité de code, des contraintes sur les ressources du système, des phénomènes liés à la synchronisation qui peuvent entraîner des défaillances non prévues. Cette norme traite de ces problèmes dans le cas des appareils à fonctionnalité très limitée.

nucléaires de puissance lorsque ces appareils ont été conçus pour être utilisés dans des applications non nucléaires (et qu'ils sont potentiellement certifiés conformes à une norme de sûreté générique largement reconnue telle que la CEI 61508). De plus, la norme CEI 62671 couvre seulement les appareils qui présentent des fonctionnalités dédiés, limitées et particulières et une possibilité de configuration limitée.

La CEI 62671 doit être lue avec la CEI 60880 (informative), la CEI 62138 (informative), la CEI 60987 (informative) et la CEI 62566 (informative) qui sont les autres documents pertinents du SC 45A de la CEI qui fournissent des recommandations applicables aux systèmes programmés réalisant des fonctions importantes pour la sûreté et qui sont utilisés dans les centrales nucléaires de puissance.

Pour plus de détails sur la collection de normes du SC 45A de la CEI, voir le point d) de cette introduction.

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

Il est important de noter que la présente norme n'établit pas d'exigence fonctionnelle supplémentaire pour les systèmes de sûreté de classe 1, 2 ou 3.

La présente norme fournit des exigences particulières pour les aspects suivants:

- l'utilisation d'un processus planifié pour choisir, et pour évaluer les appareils candidats à l'utilisation, de même que pour intégrer l'appareil dans les systèmes de tranche,
- les critères d'évaluation de l'aptitude fonctionnelle d'un appareil contenant des logiciels embarqués ou utilisant des circuits numériques conçus à l'aide d'outils logiciels tel que HDL (Langage de description de matériel),
- les critères à considérer lors d'une évaluation d'ensemble pour obtenir un niveau d'assurance suffisant concernant le fait que l'appareil fonctionnera tel que prévu lorsqu'il sera sollicité,
- les considérations relatives à l'emploi sûr de l'appareil retenu dans les systèmes de tranche.

Afin d'assurer la pertinence de la présente norme pour les années à venir, l'accent est mis sur les questions de principes plutôt que sur les technologies particulières.

Dans la présente norme, l'accent est mis sur la revue des preuves afférentes aux processus mis en place par les concepteurs et les fabricants (qui peuvent être des organisations différentes), sachant que ces deux organisations ont de l'influence sur décision d'accepter ou non l'appareil candidat pour réaliser l'application prévue. Ces preuves peuvent avoir été obtenues par le truchement du fournisseur avec lequel l'utilisateur final est en contact direct.

**d) Description de la structure de la collection des normes du SC 45A de la CEI et relations avec d'autres documents de la CEI, et d'autres organisations (AIEA, ISO)**

Le document de niveau supérieur de la collection de normes produites par le SC 45A de la CEI est la norme CEI 61513. Cette norme traite des exigences relatives aux systèmes et équipements d'instrumentation et de contrôle-commande (systèmes d'I&C) utilisés pour accomplir les fonctions importantes pour la sûreté des centrales nucléaires, et structure la collection de normes du SC 45A de la CEI.

La CEI 61513 fait directement référence aux autres normes du SC 45A de la CEI traitant de sujets génériques, tels que la catégorisation des fonctions et le classement des systèmes, la qualification, la séparation des systèmes, les défaillances de cause commune, les aspects logiciels et les aspects matériels relatifs aux systèmes programmés, et la conception des salles de commande. Il convient de considérer que ces normes, de second niveau, forment, avec la norme CEI 61513, un ensemble documentaire cohérent.

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

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

La CEI 61513 a adopté une présentation similaire à celle de la CEI 61508, avec un cycle de vie de sûreté d'ensemble et un cycle de vie de sûreté des systèmes. Au niveau sûreté nucléaire, elle est l'interprétation des exigences générales des parties 1, 2 et 4 de la CEI 61508 pour le secteur nucléaire, pour ce qui concerne le domaine de la sûreté nucléaire. Dans ce domaine, la CEI 60880 et la CEI 62138 correspondent à la CEI 61508-3 pour le secteur nucléaire. La CEI 61513 fait référence aux normes ISO ainsi qu'aux documents AIEA GS-R-3, AIEA GS-G-3.1 et AIEA GS-G-5.1 pour ce qui concerne l'assurance qualité.

Les normes produites par le SC 45A de la CEI sont élaborées de façon à être en accord avec les principes de sûreté fondamentaux du Code AIEA sur la sûreté des centrales nucléaires, ainsi qu'avec les guides de sûreté de l'AIEA, en particulier avec le document d'exigences NS-R-1 qui établit les exigences de sûreté relatives à la conception des centrales nucléaires et avec le guide de sûreté NS-G-1.3 qui traite de l'instrumentation et du contrôle commande importants pour la sûreté des centrales nucléaires. La terminologie et les définitions utilisées dans les normes produites par le SC 45A sont conformes à celles utilisées par l'AIEA.

NOTE Il est fait l'hypothèse que pour la conception des systèmes d'I&C qui sont supports de fonctions de sûreté conventionnelle (par exemple pour garantir la sécurité des travailleurs, la protection des biens, la prévention contre les risques chimiques, la prévention contre les risques liés au procédé énergétique) on applique des normes nationales ou internationales, dont les exigences sont comparables à des normes telles que la CEI 61508.

# CENTRALES NUCLÉAIRES DE PUISSANCE – INSTRUMENTATION ET CONTRÔLE-COMMANDE IMPORTANTS POUR LA SÛRETÉ – SÉLECTION ET UTILISATION DES APPAREILS NUMÉRIQUES À FONCTIONNALITÉS LIMITÉES

## 1 Domaine d'application

### 1.1 Généralités

La présente Norme internationale couvre les appareils qui contiennent des logiciels embarqués ou des circuits numériques configurés électroniquement qui n'ont pas été produits conformément aux normes CEI applicables aux systèmes et équipements importants pour la sûreté des centrales nucléaires de puissance, mais qui sont candidats pour être utilisés dans des centrales nucléaires de puissance. Elle établit des exigences pour le choix et l'évaluation de tels appareils lorsque ceux-ci présentent des fonctionnalités spécifiques, limitées et dédiées[2] et que leur configuration est limitée.

Conformément à la CEI 61513, les systèmes d'I&C importants pour la sûreté de classe 1, 2 ou 3 peuvent être mis en œuvre en utilisant des équipements câblés conventionnels, des équipements numériques (programmables ou intégrant des matériels programmés) ou en utilisant une combinaison des deux types d'équipement. La présente norme fournit des critères d'acceptation pour le choix, l'évaluation et l'utilisation de certains des appareils numériques qui n'ont pas été développés spécifiquement pour être utilisés dans les systèmes d'I&C nucléaires. De tels appareils sont souvent conformes à la CEI 61508 ce qui peut être un facteur clé positif lorsqu'on qualifie des équipements non conçus pour le nucléaire pour les employer dans le secteur nucléaire.

Les appareils couverts par la présente norme sont des appareils dédiés présentant des fonctionnalités limitées particulières, qui intègrent ou peuvent intégrer des composants pilotés par logiciel ou des circuits numériques conçus en utilisant des outils logiciel. Des exemples sont: les capteurs intelligents, les positionneurs de vanne, les appareils de protection électriques ou les onduleurs qui peuvent contenir des composants pilotés par logiciel ou des circuits numériques conçus en utilisant des outils logiciels. La présente norme ne couvre pas les aspects relatifs au logiciel des appareils "tous usages" complexes qui sont couverts par d'autres normes, telles que la CEI 60880 et la CEI 62138 pour le logiciel. La présente norme traite des questions qu'il convient de prendre en compte lorsqu'on fait l'évaluation de l'aptitude de ces appareils dédiés à fonctionnalités spécifiques limitées pour être utiliser dans des centrales nucléaires de puissance. L'objectif de la présente norme est de proposer une approche graduelle de ces questions, avec l'application d'exigences plus contraignantes pour les classes de sûreté les plus élevées.

Ces questions comprennent:

- L'aptitude fonctionnelle (Est-ce qu'un appareil réalise les fonctions prévues ? Ces fonctions sont-elles protégées de façon suffisamment sûre des interactions avec les autres fonctions ?),
- Les preuves exigées pour démontrer cette aptitude (telles que le processus de développement suivi, le retour d'expérience collecté sur le terrain et le niveau de maturité atteint par l'appareil),

---

2 « Dédiés » dans le sens utilisé dans la présente norme fait référence à une conception pour une fonction particulière qui ne peut pas être modifiée sur le terrain, voir 3.7.

- Les aspects ayant un impact sur l'intégration de l'appareil dans des systèmes existants (par exemple compatibilité fonctionnelle et impacts sur la maintenance et l'exploitation), et
- Les exigences relatives à l'assurance que l'aptitude de l'appareil sera maintenue dans le temps et ceci pour sa durée de vie requise (telle que la durée de vie de la centrale).

La présente norme s'appuie sur d'autres normes, plus particulièrement la CEI 60780, pour traiter des questions de qualification du matériel, sans lien avec la complexité du logiciel, à savoir les aspects de fiabilité liés à la qualification environnementale, aux défaillances dues au vieillissement ou à des dommages physiques. D'autres normes telles que la CEI 61508 peuvent être utilisées comme recommandations complémentaires pour l'évaluation et l'appréciation de la qualité des équipements, mais il est reconnu que la seule certification par rapport à des normes non nucléaires est insuffisante.

### 1.2 Contexte

Le besoin à l'origine du développement de la présente norme est né d'une tendance apparue dans le secteur industriel fournisseur des systèmes d'I&C; ce besoin est en particulier lié au problème grandissant de l'obsolescence des appareils existants qui sont couramment utilisés dans les centrales nucléaires. En effet, il devient de plus en plus difficile, sinon impossible, de trouver des systèmes analogiques ou de remplacer la plupart des appareils existants à l'identique car les fournisseurs emploient de plus en plus de microcontrôleurs, d'ASICs, etc., embarqués dans les appareils proposés en remplacement, et les appareils analogiques sont de moins en moins disponibles sur le marché.

Il existe différents risques techniques potentiels lorsqu'on choisit d'utiliser ces appareils dans des centrales nucléaires, car:

- beaucoup de ces appareils ne reproduisent pas la fonctionnalité exacte que réalisait l'appareil obsolète à remplacer, pêchant ainsi dans certains cas par défaut et dans d'autres par excès, ou même présentant des fonctionnalités qui peuvent être légèrement incompatibles avec les objectifs de conception originaux;
- ces différences de fonctionnalités ne sont pas toujours immédiatement apparentes. Des exemples existent de problèmes qui sont apparus du fait du manque de recommandations dans le domaine. Ces problèmes trouvent généralement leur origine dans les différences existant entre les objectifs de conception de la centrale nucléaire et ceux des applications industrielles pour lesquelles l'appareil est conçu;
- les appareils peuvent présenter des faiblesses ou des modes de défaillances qui n'existaient pas dans l'équipement d'origine et qui doivent être prise en compte.

### 1.3 Utilisation de la présente norme

La présente norme établit des exigences permettant de déterminer si un appareil numérique de qualité industrielle, qui présente des fonctionnalités limitées dédiées et particulières ainsi que des possibilités de configuration limitées, est apte à être utilisé dans le cadre d'une application nucléaire. Ceci nécessitera l'application de critères similaires à ceux utilisés pour les appareils non numériques, mais la présente norme fournit en plus des critères applicables aux systèmes numériques. Elle tiendra aussi compte les limites associées à la faisabilité, étant donné que l'appareil industriel qualifié ne peut pas être modifié ou seulement de façon limitée.

La présente norme est conçue pour pouvoir être utilisée dans le cadre d'une application définie pour laquelle le concepteur recherche des appareils aptes à servir pour sa mise en œuvre. Très souvent, néanmoins, le concepteur de l'application est forcé de considérer l'emploi d'appareils qui n'ont pas été conçus spécifiquement pour le domaine nucléaire. L'objectif de la présente norme est d'aider le concepteur d'application à choisir et à utiliser de tels appareils conformément au classement de sûreté et aux exigences de l'application considérée.

Ainsi la présente norme peut être appliquée à différents niveaux du cycle de vie de la conception du système tel que défini dans la CEI 61513. Elle peut être appliquée tôt dans le cycle de vie de conception de la centrale, lorsque l'architecture du système d'I&C en question est élaborée, et la disponibilité d'appareils adaptés peut avoir une influence sur sa conception. En cas d'application ultérieure lorsque la conception du système est terminée, la présente norme peut être utilisée pour évaluer les appareils candidats. Finalement, la présente norme peut aussi être appliquée pour des opérations de rénovation lorsque le système est déjà en exploitation et que certains appareils sont à remplacer.

Les classes de sûreté 1, 2 et 3 sont caractérisées par des ensembles d'exigences gradués. L'objectif de la présente norme est d'être interprétée dans le cadre de la catégorie d'une fonction de sûreté à réaliser et du classement du système. Ceci veut dire qu'une interprétation graduée des exigences est appropriée et attendue. Il est aussi reconnu que les modes de défaillance tolérables peuvent être notablement différents suivant les applications de tranche considérées, et que ceci peut déterminer l'acceptabilité d'un appareil ou de sa forme d'utilisation. L'interprétation et la rigueur dans l'application des exigences de la présente norme sont supposées être prises en compte de façon adaptée dans chacun des cas.

Un autre problème fréquemment rencontré est la résistance des fournisseurs à fournir des preuves concernant les caractéristiques précises et exactes de l'appareil, telles que les détails concernant les fonctions internes de l'appareil, ou la façon dont il a été développé. Il convient de traiter cette question dès que possible, si possible lors de la pré-qualification des fournisseurs, et celle-ci pouvant nécessiter le choix d'autres fournisseurs afin de satisfaire à la présente norme.

Le Plan d'Evaluation et d'Application (PEA)[3] définit les objectifs et est un guide d'interprétation de la présente norme pour un appareil particulier et une application particulière. Ce plan identifie et justifie les approches qui seront utilisées en cas de problèmes, y compris les types des mesures compensatoires qui seront mises en œuvre afin de corriger les problèmes rencontrés tels que les différences entre les fonctionnalités demandées et celles disponibles, ou encore le manque de preuves, concernant les caractéristiques précises et exactes de l'appareil habituellement demandées.

L'étape finale du processus d'évaluation est la préparation du Rapport d'Evaluation et d'Application (REA). Ce compte rendu identifie l'appareil qui a été qualifié, l'application pour laquelle il l'a été et toutes les contraintes s'appliquant à son utilisation.

### 1.4 Structure

La présente norme est organisée comme suit:

- L'Article 5 traite de l'applicabilité de la présente norme, et du processus d'évaluation en considérant:
  - les écarts au niveau des fonctionnalités de l'appareil couvert par la présente norme,
  - le degré de flexibilité et de configurabilité de l'appareil couvert par la présente norme,
  - les entrées et les sorties du processus d'évaluation et le PEA qui documente comment les évaluateurs appliqueront les exigences de présente norme,
  - le contenu du document REA, les preuves qui ont fait l'objet de revue, et les résultats d'analyse de ces preuves, les conclusions tirées sur l'adéquation des aptitudes de l'appareil.
- L'Article 6 traite des éléments relatifs aux fonctionnalités et autres exigences qui doivent être évalués, tels que

---

[3] L'exigence de la CEI 61513 concernant l'existence d'un Plan de Qualification est satisfaite par l'existence du Plan d'Evaluation et d'Application.

  - le niveau minimum de documentation de développement de l'appareil candidat,
  - l'aptitude de l'appareil candidat à réaliser la ou les fonctions attendues,
  - l'immunité de la fonction principale de l'appareil candidat vis-à-vis des influences non souhaitées des fonctions superflues,
  - l'aptitude de l'appareil candidat à fonctionner en présence de toutes les conditions environnementales prévues, conformément à la CEI 60780 ou aux autres normes identifiées,
  - la fiabilité et l'aptitude de l'appareil candidat à la maintenance,
  - la pertinence des mesures relatives à la cybersécurité mises en place, et
  - la documentation utilisateur fournie.
- L'Article 7 traite des critères permettant d'établir la confiance en ce qui concerne les caractéristiques relevant de la précision et de l'exactitude de la conception et de la fabrication de l'appareil, en considérant:
  - l'utilité des certifications précédemment acquises pour des applications non nucléaires,
  - les méthodes d'évitement des défauts systématiques,
  - l'application d'un cycle de vie de sûreté pour la conception de l'appareil, et
  - l'assurance qualité associée à la fabrication, et
  - les moyens autorisés pour afin de compenser l'éventuelle faiblesse des preuves apportées pour couvrir points ci-dessus, en complétant le dossier d'acceptation de l'appareil candidat sur sa base de la stabilité, de son expérience en exploitation, en améliorant sa documentation ou en réalisant des essais ou des analyses complémentaires.
- L'Article 8 traite des critères relatifs à l'intégration de l'appareil dans les systèmes d'I&C de la centrale, en considérant:
  - les restrictions concernant la façon d'utiliser l'appareil (telles que le classement maximum de sûreté de l'application pour laquelle l'appareil est qualifié),
  - les modifications qu'il peut être nécessaire de réaliser ou sur l'appareil ou sur le système cible pour pouvoir intégrer l'appareil dans le système cible, et
  - l'intégration et la recette de l'appareil au niveau des systèmes de sûreté de la centrale.
- Le paragraphe 9 traite de considérations visant à maintenir le caractère acceptable de l'appareil, telles que:
  - les notifications faites à l'utilisateur par le concepteur de l'appareil ou par le fabricant,
  - le support technique offert pour l'appareil pour sa durée de vie,
  - la préservation des outils et de la documentation de maintenance, et
  - les recommandations destinées à l'utilisateur final.

## 2 Références normatives

Les documents suivants sont cités en référence de manière normative, en intégralité ou en partie, dans le présent document et sont indispensables pour son application. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

CEI 60671:2007, *Centrales nucléaires de puissance – Systèmes d'instrumentation et de contrôle-commande importants pour la sûreté – Essais de surveillance*

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

CEI 60880:2006, *Centrales nucléaires de puissance– Instrumentation et contrôle-commande importants pour la sûreté – Aspects logiciels des systèmes programmés réalisant des fonctions de catégorie A*

CEI 60980, *Pratiques recommandées pour la qualification sismique du matériel électrique du système de sûreté dans les centrales électronucléaires*

CEI 60987:2007, *Centrales nucléaires de puissance – Instrumentation et contrôle-commande importants pour la sûreté*

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

CEI 61226, *Centrales nucléaires de puissance – Instrumentation et contrôle-commande importants pour la sûreté – Classement des fonctions d'instrumentation et de contrôle-commande*

CEI 61508-7:2010, *Sécurité fonctionnelle des systèmes électriques/électroniques/ électroniques programmables relatifs à la sécurité – Partie 7: Présentation de techniques et mesures*

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

CEI 62138:2004, *Centrales nucléaires – Instrumentation et contrôle-commande importants pour la sûreté – Aspects logiciels des systèmes informatisés réalisant des fonctions de catégorie B ou C*

ISO 9001:2008, *Systèmes d'assurance qualité - Exigences*

## 3 Termes et définitions

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

**3.1**
**fonction auxiliaire**
toute fonction fournie par l'appareil candidat qui est support de sa fonction principale

Note 1 à l'article: Des exemples sont les fonctions de l'appareil candidat utilisées en appui de la fonction importante pour la sûreté, telles que la fourniture de moyens appropriés pour surveiller ses paramètres opérationnels ou son fonctionnement correct tel que prévu pour l'application de sûreté.

Note 2 à l'article: Voir aussi "fonction principale" et "fonction superflue".

**3.2**
**auditable**
propriété d'une preuve documentée qui est immédiatement disponible pour une revue par un personnel indépendant

**3.3**
**catégorie d'une fonction d'I&C**
l'une des trois affectations de sûreté possibles (A, B, C) des fonctions d'I&C résultant de l'évaluation de l'importance pour la sûreté de la fonction exécutée. Une affectation "non classée" peut être délivrée si la fonction n'est pas importante pour la sûreté

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

Note 2 à l'article: La CEI 61226 définit les catégories de fonctions d'I&C. A chaque catégorie correspond un ensemble d'exigences relatives à la fois aux fonctions d'I&C (spécification, conception, intégration, vérification et validation) et à l'ensemble des composants nécessaires à la réalisation des fonctions (propriétés et qualification)

indépendamment de la manière suivant laquelle ces composants sont distribués dans plusieurs systèmes d'I&C interconnectés. Pour davantage de clarté, la présente norme définit des catégories de fonctions d'I&C et des classes de systèmes d'I&C. Elle établit une relation entre la catégorie d'une fonction et la classe minimale des systèmes et équipements associés.

[SOURCE: CEI 61513:2011, 3.4]

**3.4**
**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. Une affectation "Non Classé" est délivrée si le système d'I&C n'exécute pas de fonction importante pour la sûreté

Note 1 à l'article: Voir également "catégorie d'une fonction d'I&C", "constituant important pour la sûreté".

[SOURCE: CEI 61513:2011, 3.6]

**3.5**
**défaillance de cause commune**
**DCC**
défaillance de plusieurs structures, systèmes ou composants due à un évènement ou à une cause unique

[SOURCE: CEI 61513:2011, 3.8]

**3.6**
**système programmé**
système d'I&C dont les fonctions dépendent en grande partie, ou sont totalement effectuées à l'aide de microprocesseurs, d'un matériel électronique programmé ou d'ordinateurs

Note 1 à l'article: Equivalent à système numérique, système informatique.

[SOURCE: CEI 61513:2011, 3.11]

**3.7**
**fonctionnalité dédiée**
propriété des appareils qui ont été conçus pour réaliser seulement une fonction clairement définie ou bien un ensemble très réduit de fonctions, telles que par exemple, la capture et l'envoi d'un paramètre procédé, ou la transformation d'une source de courant alternatif en courant continu. Cette fonction (ou cet ensemble réduit de fonctions) est inhérent à l'appareil, et n'est pas le résultat d'une programmation par l'utilisateur

Note 1 à l'article: Les fonctions auxiliaires (par exemple, l'auto-surveillance, l'auto-étalonnage, la communication de données) peuvent aussi être réalisées dans l'appareil, mais pour autant cela ne change pas le domaine étroit d'application de l'appareil.

Note 2 à l'article: La présente norme s'applique aux appareils à fonctionnalité dédiée qui satisfont à toutes les exigences de 5.2.2.

Note 3 à l'article: «Dédiés» dans le sens utilisé dans la présente norme fait référence à une conception pour une fonction particulière qui ne peut pas être modifiée sur le terrain.

**3.8**
**appareil numérique**
appareils dont la mise en œuvre repose sur la base d'instructions réalisées en utilisant des signaux et des niveaux discrets définis ou qui intègrent des états internes discrets définis et qui passent d'un de ces états à un autre

Note 1 à l'article: Les fonctions de tels appareils sont habituellement définies par un processus qui comprend du développement et du test de logiciels ou de descriptions de matériel à base de langage, tels que des appareils qui sont contrôlés de façon interne par des logiciels ou qui peuvent comprendre des ASICs ou des FPGAs, etc., qui ont été configurés en utilisant des logiciels.

Note 2 à l'article: Les appareils, équipements ou systèmes qui sont contrôlés à partir de logiciel sont dits "programmés" alors que le qualificatif "numérique" est un terme plus large qui englobe tout appareil qui comprend un circuit mettant en œuvre une logique.

Note 3 à l'article: Les appareils numériques non développés pour les industries nucléaires sont appelés appareils numériques industriels.

**3.9**
**équipement**
une ou plusieurs parties d'un système. Un équipement est une partie déterminée et définissable (et généralement amovible) d'un système

Note 1 à l'article: Voir aussi «composant» et «système d'I&C»

Note 2 à l'article: Les équipements peuvent intégrer du logiciel.

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 dévie de celle donnée dans la CEI 60780. Cet écart est justifié par le fait que la CEI 61513 considère que «l'équipement» fait partie du système alors que la CEI 60780 considère que l'équipement est l'objet de la qualification.

[SOURCE: CEI 61513:2011, 3.16]

**3.10**
**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

Les langages HDL (Hardware Description Language) les plus utilisés sont VHDL (IEEE 1076) et Verilog (IEEE 1364).

[SOURCE: CEI 62566:2012, 3.6]

**3.11**
**circuit intégré programmé en HDL**
**HPD**
circuit intégré configuré (pour les systèmes d'I&C de la centrale nucléaire), à l'aide de langages de description de matériel et des outils logiciels associés

Note 1 à l'article: Les langages de description de matériel et les outils associés (par exemple simulateur, synthétiseur) sont utilisés pour implanter les exigences au niveau d'un assemblage particulier de ressources micro-électroniques prédéveloppées.

Note 2 à l'article: Le développement d'appareils programmés en HDL peut utiliser des blocs prédéveloppés.

Note 3 à l'article: Les langages de description de matériel reposent généralement sur des FPGA, des PLD vierge ou des technologies de type micro-électronique équivalentes.

[SOURCE: CEI 62566:2012, 3.7]

**3.12**
**fonction d'I&C**
fonction permettant de commander, exploiter et/ou surveiller une partie définie du procédé

Note 1 à l'article: Le terme "fonction d'I&C" est utilisé par les ingénieurs automaticiens pour mettre en forme les exigences de fonctionnalité relatives à l'I&C. Une fonction d'I&C est définie de manière à:

- donner une représentation complète d'un objectif fonctionnel,
- pouvoir être catégorisée en fonction de son degré d'importance pour la sûreté,
- englober tous les types d'éléments, du capteur jusqu'à l'actionneur, et réaliser ainsi son objectif fonctionnel.

Note 2 à l'article: Une fonction d'I&C peut être subdivisée en plusieurs sous-fonctions (par exemple mesure, commande, mise en marche) pour permettre l'affectation aux systèmes d'I&C.

[SOURCE: CEI 61513:2011, 3.28]

**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.

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. (Voir Note 2). Les différentes fonctions d'un système peuvent utiliser des ressources dédiées ou partagées

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

Note 2 à l'article: Les éléments contenus dans un système d'I&C donné sont définis dans la spécification des limites de ce système.

Note 3 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: CEI 61513:2011, 3.29]

**3.14**
**interruption**
suspension d'une opération, par exemple l'exécution d'un programme informatique, provoquée par un événement extérieur à cette opération

[SOURCE: CEI 61513:2011, 3.32]

**3.15**
**constituant important pour la sûreté**
constituant faisant partie d'un groupe de sûreté et/ou dont le mauvais fonctionnement ou la défaillance pourrait entraîner une exposition à des rayonnements du personnel du site ou de personnes du public

Les constituants importants pour la sûreté comprennent:

a) les structures, systèmes et composants dont le mauvais fonctionnement ou la défaillance pourraient entraîner une exposition indue à des rayonnements du personnel du site ou de personnes du public;
b) les structures, systèmes et composants qui empêchent les incidents de fonctionnement prévus d'aboutir à des conditions accidentelles;
c) les dispositifs prévus pour atténuer les conséquences d'un mauvais fonctionnement ou d'une défaillance de structures, systèmes ou composants.

Note 1 à l'article: L'objectif de cette définition est de couvrir tous les aspects relatifs à la sûreté nucléaire.

Note 2 à l'article: Dans la présente norme les constituants principalement pris en compte seront les systèmes d'I&C et les fonctions d'I&C.

Note 3 à l'article: Voir aussi "fonction d'I&C".

[SOURCE: Glossaire de sûreté de l'AIEA, Edition 2007]

**3.16**
**fonctionnalité limitée**
synonyme de fonctionnalité dédiée (voir 3.7)

**3.17**
**cycle de vie de sûreté de l'ensemble de l'I&C**
activités nécessaires à la mise en œuvre des systèmes et composants de l'architecture d'I&C importants pour la sûreté. Elles ont lieu entre la spécification des exigences d'I&C (lors de la phase de conception de sûreté de la centrale) et le retrait du service du dernier système d'I&C

[SOURCE: CEI 61513:2011, 3.34]

**3.18**
**fonction principale**
la fonction particulière (ou l'ensemble minimal de fonctions) de l'appareil candidat qui est nécessaire pour que le système important pour la sûreté réalise sa fonction telle que prévu dans l'analyse de sûreté, et sur laquelle on s'appuie pour avoir un fonctionnement autonome permettant de réaliser cette fonction

Note 1 à l'article: Comme défini en 5.2.2, un appareil multifonctions peut offrir la possibilité de se servir de plusieurs de ses fonctions principales comme "fonction principale", mais un tel appareil peut ne pas se situer dans le domaine de la présente norme, ou dans tous les cas sera moins apprécié qu'un appareil mono fonction.

Note 2 à l'article: Voir aussi "fonction auxiliaire" et "fonction superflue".

Note 3 à l'article: Par exemple un amplificateur utilisé dans une chambre d'ionisation peut être utilisé pour produire en sortie en même temps un enregistrement du courant et un signal de puissance linéaire, chacun d'eux étant utilisé par le signal d'arrêt rapide du réacteur. Ces deux fonctions forment l'ensemble de fonctions principales (et dans le cadre de la présente norme l'expression "fonction principale" s'applique à cet ensemble); alors que la fonctionnalité permettant de changer l'échelle de sortie ou de filtrer les sorties est une fonction auxiliaire. Les autres fonctions qui ne sont pas nécessaires pour choisir l'appareil, telles que l'affichage local, ou la signalisation à distance par une connexion réseau sont des fonctions superflues.

Note 4 à l'article: Par exemple un capteur intelligent peut être capable de produire un signal représentant le débit ou le niveau à partir d'une sortie analogique dans la gamme 4 mA à 20 mA ou par le protocole HART. Si le concepteur de l'application nucléaire a choisi d'utiliser le signal 4 mA à 20 mA pour des raisons de sûreté, alors ce sera une fonction principale et les autres sorties seront superflues.

**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 (par exemple développés dans le cadre d'un projet antérieur, pour des produits commercialement disponibles). Généralement, la qualification d'un système d'I&C est réalisée par étapes: d'abord la qualification de l'équipement individuel pré existant (habituellement tôt dans le processus de réalisation du système); et plus tard la qualification du système intégré (par exemple sur la conception finale).

[SOURCE: CEI 61513:2011, 3.38]

**3.20**
**qualité**
niveau de satisfaction d'exigence atteint par un ensemble inhérent de caractéristiques

[SOURCE: ISO 9000:2005]

**3.21**
**assurance qualité**
fonction d'un système de gestion qui garantit que des prescriptions spécifiques seront respectées

[SOURCE: Glossaire de sûreté de l'AIEA, Edition 2007]

**3.22**
**exigence**
expression dans le contenu d'un document formulant les critères à respecter afin de prétendre à la conformité avec le document, et avec lesquels aucun écart n'est permis

[Directive ISO/CEI, Partie 2, 2011, 3.3.1]

Note 1 à l'article: Dans les documents du SC 45A de la CEI on distingue les types d'exigences suivant:

*Exigences de sûreté* – Exigences imposées par les autorités (judiciaires, administratives ou les organisations de normalisation) et les autorités de conception en matière de sûreté de la centrale nucléaire, en ce qui concerne l'impact sur les personnes, la société et l'environnement pendant le cycle de vie de la centrale nucléaire.

*Exigences fonctionnelles et de performances* – Les exigences fonctionnelles indiquent les réactions du système par rapport à des conditions ou des signaux particuliers, et les exigences de performances définissent des caractéristiques telles que le temps de réponse et la précision.

*Exigences opérationnelles* – Exigences concernant l'aptitude et la capacité opérationnelles de la centrale imposées par le propriétaire.

*Exigences de conception de la centrale* – Exigences techniques portant sur la conception globale de la centrale afin de garantir le respect des exigences en matière de sûreté et les exigences opérationnelles de la centrale.

*Exigences de conception du système.* – Exigences de conception de systèmes individuels permettant que la conception de la centrale complète satisfasse aux exigences de conception de la centrale.

*Exigences de conception d'équipement* – Exigences concernant un équipement individuel qui lui permettent de respecter les exigences de conception du système.

Note 2 à l'article: Le glossaire de sûreté de l'AIEA édition 2007 contient la définition suivante:

*Prescrit, prescription* – Prescrit par une législation ou une réglementation (nationale ou internationale) ou par des fondements ou des prescriptions de sûreté de l'AIEA.

Cette définition AIEA utile dans le cadre des publications de l'AIEA est trop limitée pour être utilisée dans le cadre des normes techniques. Elle correspond à la définition "d'exigences de sûreté" telle que fournie dans la Note 1.

Note 3 à l'article: Il est bien entendu que tout écart par rapport à une exigence est à justifier.

Note 4 à l'article: Si on a des écarts par rapport aux exigences, les écarts et les justifications afférentes seront aussi clairement documentés dans le REA pour permettre à d'éventuels utilisateurs de l'appareil de justifier l'utilisation de celui-ci ou le choix d'un autre appareil.

[SOURCE: CEI 61513:2011, 3.44]

**3.23**
**configurabilité restreinte**
s'applique aux appareils qui peuvent être configurés seulement d'une façon très limitée en choisissant parmi un nombre relativement peu élevé d'options la manière suivant laquelle l'appareil va fonctionner dans l'application prévue

**3.24**
**sécurité**
capacité d'un système informatique à protéger les informations et les données afin que les personnes ou systèmes non autorisés ne puissent ni les lire, ni les modifier, ni qu'ils puissent passer ou inhiber des commandes et que les personnes ou systèmes autorisés puissent y accéder

Note 1 à l'article: Dans la présente norme la définition de la sécurité est à interpréter en substituant l'expression "système programmé" par l'expression "appareil numérique contenant du logiciel ou des circuits numériques dont la conception a été faite en utilisant des langages de description matériel".

[SOURCE: CEI 61513:2011, 3.48]

**3.25**
**auto-surveillance**
test automatique des performances matérielles et de la cohérence logicielle d'un système d'I&C informatisé

Note 1 à l'article: Telle qu'utilisée dans la présente norme, la définition est étendue au-delà des simples tests, et couvre les fonctions automatiques réalisées par les appareils programmables conçus pour détecter (principalement) les défaillances matériel qui peuvent être de façon inhérente sûre ou dangereuse (à savoir les défaillances qui peuvent empêcher l'appareil de réaliser sa fonction de sûreté) de façon à les transformer en évènements sûrs, ou bien en signalant la défaillance ou bien en forçant l'appareil dans un état sûr.

Note 2 à l'article: Voir aussi "essai de surveillance" qui n'est pas lancé automatiquement.

Note 3 à l'article: l'expression "essai d'auto-surveillance" est équivalente.

[SOURCE: CEI 60671:2007, 3.8]

**3.26**
**logiciel**
programmes (ensembles ordonnés d'instructions), données, règles et toute documentation associée relatifs au fonctionnement d'un système programmé

[SOURCE: CEI 61513:2011, 3.51]

**3.27**
**analyse de l'aspect critique du logiciel**
analyse du logiciel pour classer chaque fonction dans le logiciel par rapport à ses possibilités de provoquer des défaillances non sûres

**3.28**
**défaut logiciel**
défaut de conception situé dans un composant logiciel

Note 1 à l'article: Voir aussi "défaut".

[SOURCE: CEI 61513:2011, 3.53]

**3.29**
**fonction superflue**
toute fonction réalisée par un appareil candidat qui n'est pas une fonction requise

Note 1 à l'article: Par exemple, alors qu'une fonction principale peut être la transmission de la mesure de pression par un signal de 4 mA à 20 mA à un autre appareil, une fonction auxiliaire peut être celle qui réalise l'ajustement des paramètres de filtrage de cette sortie pour réaliser la fonction de sûreté souhaitée, et une fonction superflue peut être une deuxième sortie telle que le signal en tension qui n'est pas nécessaire à la fonction de sûreté.

Note 2 à l'article: Voir aussi "fonction principale" et "fonction auxiliaire".

**3.30**
**test de surveillance**
un test complet d'une fonction de sûreté lancé manuellement. Il peut être réalisé comme un test complet en une passe ou comme une série d'essais se chevauchant. Le test est lancé manuellement mais il peut être fait appel à des équipements d'essai automatiques ou semi-automatiques pour réaliser les tests et/ou enregistrer les résultats de tests. Les tests de surveillance sont réalisés pour les fonctions de sûreté principales d'un appareil

Note 1 à l'article: La CEI 60671 définit les "essais de surveillance" comme l'ensemble complet des activités 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 exigences de dimensionnement sont satisfaites". La présente norme reconnaît que les tests d'auto surveillance automatiques correspondent à une exigence de la CEI 61508 pour le plus haut des niveaux d'intégrité de sécurité (SIL) et que ceux-ci doivent être distingués des tests lancés manuellement car il existe de grandes différences au niveau des fréquences de lancement et des couvertures de tests.

Note 2 à l'article: Un synonyme est le « test d'épreuve ».

Note 3 à l'article: Voir aussi "auto surveillance" qui est lancée automatiquement.

**3.31**
**défaut systématique**
défaut relié de façon déterministe à une certaine cause, ne pouvant être éliminé que par une modification de la conception, du processus de fabrication, des procédures d'exploitation, de la documentation ou d'autres facteurs appropriés

[SOURCE: CEI 61513:2011, 3.60]

## 4 Symboles et abréviations

| | |
|---|---|
| ASIC | Circuit intégré conçu pour des applications spécifiques |
| CB | Programmé |
| MC | Mesure Compensatoire |
| COTS | Composants sur étagère du commerce |
| CPU | Unité centrale de traitement |
| PEA | Plan d'Evaluation et d'Application |
| REA | Rapport d'Evaluation et d'Application |
| IEM | Interférences électromagnétiques |
| AMDE | Analyse des Modes de Défaillances et de leurs Effets |
| AMDEC | Analyse des Modes de Défaillances, de leurs Effets et de leurs aspects Critiques |
| AMDED | Analyse des Modes de Défaillances, de leurs Effets et de leurs Diagnostiques |
| FPGA | Circuit intégré programmable par le fabricant de systèmes de contrôle-commande |
| AAD | Analyse des Arbres de Défaillances |
| HART | Highway addressable remote transducer (protocole) |
| HAZOP | HAZard and OPerability |
| HDL | Langage de description de matériel |
| IHM | Interface Homme Machine |
| HPD | Appareil programmé en HDL |
| I&C | Instrumentation et Contrôle-commande |
| E/S | Entrée/Sortie |
| CNP | Centrale Nucléaire de Puissance |
| PLC | Automate industriel programmable |
| PROM | Programmable read only memory |
| AQ | Assurance Qualité |
| VHDL | Langage de description de matériel pour circuit intégré très haute vitesse |

## 5 Exigences générales

### 5.1 Généralités

Le principal problème posé par les appareils numériques est qu'ils sont généralement complexes et que cette complexité peut être à l'origine de défauts systématiques dans leur conception, en particulier au niveau de la conception du logiciel ou des HPD. Ces défauts peuvent ne pas être détectés jusqu'à ce qu'un évènement survienne qui présente un profil opérationnel n'ayant pas fait l'objet d'un essai. Ainsi un des principaux objectifs de la présente norme est d'établir les critères permettant d'évaluer la conception de l'appareil

numérique pour atteindre un niveau d'assurance compatible avec le classement de sûreté de l'application prévue afin de s'assurer que, du fait de défauts systématiques, l'appareil ne manquera pas de réaliser sa fonction lorsqu'il sera sollicité dans les conditions prévues pour son utilisation.

Pour atteindre cet objectif, la présente norme identifie en 5.2.2 les exigences particulières qui doivent être satisfaites par l'appareil pour que cette norme puisse être appliquée. La présente norme définit le processus et les exigences permettant d'évaluer l'appareil candidat sur la base de l'aptitude de ses fonctions et du niveau de confiance qu'on peut avoir dans sa conception et son fonctionnement puis sur la confiance qu'on peut avoir dans la stabilité de la conception de l'appareil. Il est aussi recommandé que la probabilité du support à long terme soit prise en compte.

## 5.2 Application de la présente norme

### 5.2.1 Généralités

L'objet de ce paragraphe est de fournir de l'aide pour l'application de la présente norme à ceux chargés d'évaluer l'aptitude d'un appareil industriel à être utilisé dans le cadre d'une application importante pour la sûreté dans une centrale nucléaire de puissance.

Ce paragraphe décrit:

– les critères à utiliser pour décider si la présente norme est applicable, et
– les principes intervenant pour définir le caractère applicable de la présente norme.

### 5.2.2 Critères relatifs au caractère applicable de la présente norme

Un appareil auquel peut s'appliquer la présente norme doit satisfaire aux critères suivants:

a) l'appareil est un appareil numérique pré existant qui contient du logiciel ou une logique programmée (par exemple HPD) prédéveloppé et est candidat pour être utilisé dans le cadre d'une application importante pour la sûreté;
b) la fonction principale réalisée est bien définie et utilisable par seulement un type d'application supportée par un système d'I&C, telle qu'une mesure de température ou de pression, un positionneur de vanne, ou un contrôleur de vitesse d'un appareil mécanique, ou la réalisation d'une fonction d'alarme;
c) la fonction principale réalisée est conceptuellement simple et son domaine est réduit (bien que la façon de la réaliser puisse être complexe en interne);
d) l'appareil n'est pas conçu pour pouvoir être reprogrammé après sa fabrication, ni de manière générale pour permettre la modification profonde de ses fonctions lui permettant de réaliser une fonction conceptuellement différente de celle d'origine: seuls des paramètres définis à l'avance peuvent être configurés par les utilisateurs;
e) si la fonction principale de l'appareil peut être réglée ou configurée, alors cette possibilité est limitée aux paramètres associés au procédé (tels que des gammes procédé), aux performances (vitesse ou synchronisation), à l'ajustement de signaux d'interface (tels que la sélection des gammes de tension ou d'intensité), ou aux gains (tels que l'ajustement d'un gain proportionnel).

NOTE 1 L'intention est de préférer les appareils sans fonction auxiliaire et particulièrement sans fonction superflue. Si de telles fonctions existent dans l'appareil, elles seront identifiées et évaluées en termes de leur possibilité d'interférer avec la fonction principale de l'appareil conformément à 6.3 et 6.5 respectivement.

NOTE 2 L'intention est d'exclure les appareils qui offrent la possibilité de définir une fonctionnalité à l'aide d'un langage généraliste, tel que "C" ou en utilisant un langage spécifique applicatif tel que des blocs fonction ou un langage ladder de programmation d'automate industriel.

NOTE 3 Il n'est pas possible de définir tous les appareils qui relèvent de la présente norme, mais les fonctions dont la liste est fournie ci-dessous donnent des exemples, en supposant que les possibilités de configuration sont compatibles avec les objectifs prévus de la présente norme:

- capteur de température ou de pression,

- capteur intelligent (par exemple capteur de pression)
- positionneur de vanne,
- appareils de protection électrique, tels que relai de surtension ou de surpuissance,
- commande de moteur,
- unité d'affichage dédiée (par exemple affichage réalisé à partir de LED), ou
- interfaces de communication dédiées simples.

NOTE 4 Il n'est pas possible de définir tous les appareils qui sont hors du domaine de la présente norme, mais les équipements et les appareils dont la liste est fournie ci-dessous en sont des exemples:

- les PLC (automates industriels programmables),
- les appareils qui sont fournis avec un langage de programmation, et ceci quelle que soit la nature limitée du langage (en termes de nombre de blocs fonction (ou équivalents) ou d'entrées ou de sorties), lorsque ces appareils ont été conçus pour permettre leur configuration pour plus d'une application (par exemple automate numérique à fonctionnement cyclique avec un langage de blocs fonction).

## 5.3 Exigences générales portant sur le processus d'évaluation

### 5.3.1 Processus d'évaluation

L'objet de ce paragraphe est d'identifier les étapes principales nécessaires pour choisir et évaluer un appareil candidat pour qu'il soit utilisable dans une application cible. Ces étapes sont illustrées dans la Figure 1 et spécifiées dans les paragraphes suivants.

Le processus d'évaluation et d'application doit comprendre les étapes suivantes:

a) Le pré-requis nécessaire pour débuter le processus d'évaluation et d'application doit être l'existence de la documentation concernant toutes les exigences fonctionnelles et de performance applicables pour l'appareil à utiliser dans le cadre de l'application cible. Cela peut imposer de reconstruire la base de conception de l'application[4]. La définition des exigences applicables à l'appareil candidat doivent couvrir tous les aspects pertinents dont la liste est donnée ci-dessous:
   - définition de l'objectif de sûreté du système ou de l'application cible avec un niveau de détails suffisant pour permettre la catégorisation de la fonction de l'application cible conformément à la CEI 61226 ou à un processus équivalent à celui de la CEI 61226 accepté par les autorités de sûreté nationales;
   - catégorie de sureté de la fonction de l'application cible et la classe du système associé à l'application cible;
   - fonctionnalité principale nécessaire de l'appareil, y compris les exigences fonctionnelles et de performances telles que le temps de réponse, de façon cohérente avec les critères définis en 5.2.2;
   - toutes les autres propriétés de sûreté particulières et les caractéristiques exigées pour le produit, comme indiqué par l'Article 6;
b) un Plan d'Evaluation et d'Application (PEA) doit être préparé pour prendre en compte les exigences fonctionnelles et de performances documentées conformément aux exigences de 5.3.2 et de 5.3.4, et si cela est pertinent, il doit définir la stratégie de prise en compte les différentes utilisations de l'appareil candidat (pour savoir si on réalise une seule évaluation pour couvrir toutes les utilisations prévues ou si on réalise des évaluations individualisées);

---

4 Lorsque la présente norme est appliquée à l'occasion du remplacement de n'importe quel appareil par un appareil numérique, certaines questions particulières sont à prendre en compte lorsqu'on remplace des composants analogiques, telles que la fréquence d'échantillonnage ou le principe d'échantillonnage, l'impact de la discrétisation lors du passage analogique/numérique, dans une moindre mesure le bruit qui peut masquer un évènement pour un appareil numérique. D'autre part les possibilités de filtrage élaboré avec les appareils numériques peuvent lui permettre de détecter un phénomène qui n'était pas vu par les appareils analogiques. De telles questions doivent être prises en compte lorsqu'on reconstitue la base de conception et les exigences applicables à l'appareil numérique.

Lorsque le PEA est suivi, il peut être nécessaire de réviser le plan au vu des résultats obtenus ou de la disponibilité de preuves concernant l'exactitude et la précision.

c) le ou les appareils candidats doivent être sélectionnés et évalués à partir de la présente norme seulement s'il satisfait ou s'ils satisfont aux exigences de 5.2.2.

   Dans le cas d'un système déjà développé pour lequel un appareil doit être remplacé, les exigences fonctionnelles et de performances sont déjà relativement fixées; tandis que pour un système nouveau les exigences peuvent être plus flexibles du fait qu'il y a plus de degrés de liberté pour définir les interfaces entre les appareils. Pour les nouveaux systèmes, les concepteurs prendront en compte probablement à l'avance la possibilité de succès de l'évaluation de chacun des appareils candidats et les implications issues de leurs utilisations dans le système cible, ainsi on pourra réduire la sélection d'appareils candidats. Cela a tendance à faire disparaître la distinction entre les phases de sélection et d'évaluation des appareils candidats, mais il convient de ne pas saisir ce prétexte pour éviter de suivre le processus prescrit.

d) chaque appareil candidat doit être évalué conformément au PEA (décrit en 5.3.2) et 5.3.4, pour montrer qu'il satisfait aux exigences de la présente norme.

e) le résultat de l'évaluation doit être documenté dans le Rapport d'Evaluation et d'Application (REA). Ce rapport doit contenir les informations suivantes:

   1) l'évaluation de l'appareil candidat par rapport aux exigences concernant son utilisation pour l'application cible conformément au PEA; et

   2) une conclusion claire à propos de la possibilité d'accepter le candidat; à savoir l'appareil est acceptable tel que, il est acceptable sous certaines conditions et/ou contraintes particulières, ou il n'est pas acceptable;

      Pour cela, le REA doit donner les références de façon précise et complète à toutes les exigences dans des documents déjà existants et disponibles, ou il doit comprendre un document contenant les exigences satisfaites reconstituées.

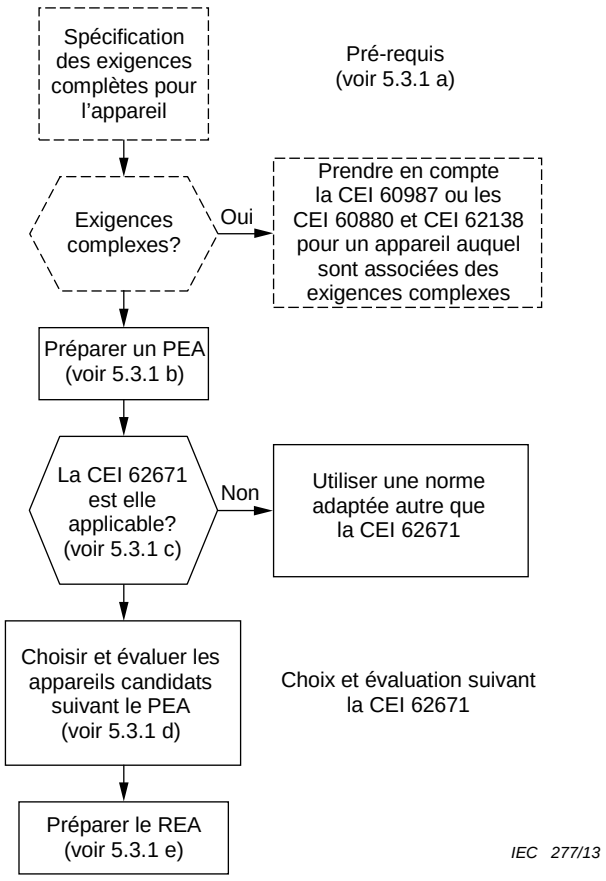


**Figure 1 – Processus de choix et d'évaluation**

### 5.3.2 Plan d'Evaluation et d'Application (PEA)

L'objet de ce paragraphe est d'identifier l'objectif et le domaine couvert par le PEA.

a) Le PEA doit identifier les justifications concernant le caractère applicable de la présente norme, pour ce qui est des critères associés en 5.2.

b) Le PEA doit identifier le domaine et le caractère applicable du travail d'évaluation pour ce qui relève:

- de l'application (fonction de sûreté) ou des applications et du ou des classements système correspondant;
- si plus d'une application est prise en compte, de la nécessité de qualifier seulement l'application de classe de sûreté la plus élevée ou bien chaque application;
- du ou des appareils candidats qui seront couverts par le REA.

c) Il convient que le PEA identifie les ressources techniques, et les qualifications nécessaires pour réaliser les travaux d'évaluation, telles que:

- les experts des applications de sûreté pour garantir que les spécifications d'exigences sont complètes, en particulier dans les cas de rénovation;
- les experts en logiciel pour examiner la sensibilité du logiciel aux défauts systématiques;
- les experts en matériel particuliers pour évaluer la qualification CEM/IEM, etc.

d) Le PEA doit identifier les critères définis par les paragraphes de l'Articles 6 qui sont pertinents pour l'application cible.

e) Le PEA doit identifier les critères dont l'application est recommandée dans les paragraphes de l'Article 7 (lorsque «il convient» s'applique) et qui doivent être appliqués; il doit donner des justifications pour les critères qui ont été écartés et pour l'utilisation de mesures compensatoires comme autorisé par l'Article 7.

f) Il convient que le PEA identifie les critères et les facteurs de pondération qui peuvent influencer la sélection des appareils candidats, tels que:

- la durée de vie requise de l'appareil dans l'application cible;
- le niveau de support du fournisseur qui peut être nécessaire, et la durée de celui-ci, et;
- le niveau de modification du système cible dans lequel l'appareil doit être intégré qui peut être nécessaire pour permettre l'utilisation de l'appareil en prenant en compte ses fonctions et ses modes de défaillance, etc.

g) Le PEA doit identifier les exigences de revue pour le REA.

### 5.3.3 Rapport d'Evaluation et d'Application (REA)

L'objet de ce paragraphe est d'identifier le domaine couvert par le REA et son contenu.

a) Le REA doit fournir les détails concernant les résultats de l'évaluation.

b) Le REA doit fournir les détails concernant les raisons ayant permis de justifier l'application de la présente norme suivant les critères indiqués en 5.2.2.

c) Le REA doit définir le domaine et le caractère applicable des travaux d'évaluation et de l'évaluation portée au REA, pour ce qui est de:

- l'application cible particulière (fonction de sûreté) et le classement de son système;
- lorsque cela est pertinent, la plus haute classe de sûreté pour laquelle l'appareil a été évalué;
- le ou les appareils candidats couverts par le REA, y compris l'identification précise du ou des appareils candidats, ceci comprenant le nom du produit, le numéro de version des composants logiciel et matériel, de la configuration et de tout autre composant ou option qui peut relever de cette évaluation.

d) Le REA doit faire la synthèse ou référencer les exigences clé fonctionnelles ou de performances (y compris celles qui peuvent avoir été reconstituées) ayant un impact sur les critères associés au caractère acceptable de l'appareil, au classement cible, aux modes de défaillance sûrs et aux conditions environnementales de fonctionnement en service.

NOTE 1 S'il y a des écarts par rapport aux exigences, les écarts et les justifications associés seront aussi clairement documentés dans le REA pour permettre à un éventuel utilisateur de justifier l'utilisation de l'appareil pour une application ou de sélectionner un autre appareil.

e) Le REA doit fournir les informations concernant les limites de fiabilité qui peuvent être atteinte en utilisant l'appareil ou seul ou dans une configuration redondante.

f) Le REA doit fournir les informations concernant les critères de choix identifiés dans le PEA.

g) Le REA doit comprendre (ou référencer s'ils sont disponibles à des fins d'inspection) tous les documents utilisés pour vérifier chaque phase de développement de l'appareil, y compris la stratégie de vérification et les essais réalisés; ou bien il doit comprendre des références à ces documents sous condition que ces documents soient accessibles à une tierce partie à des fins d'évaluation.

h) Le REA doit documenter la méthode utilisée pour appliquer les critères définis aux Articles 6 à 9 conformément à 5.3.4. Il doit fournir une justification de l'importance relative ou de l'omission de ces critères.

i) Le REA doit documenter les mesures compensatoires nécessaires pour la ou les applications cibles considérées afin de faire face aux cas où soit l'appareil candidat n'est pas totalement conforme aux exigences, soit les preuves originales de conformité ne sont pas considérées comme suffisantes.

Les mesures compensatoires possibles peuvent comprendre des essais complémentaires, l'amélioration de la documentation, des tests de surveillance supplémentaires en exploitation, des limitations strictes concernant l'utilisation de l'appareil (telles que l'utilisation seulement dans des systèmes présentant certaines propriétés fonctionnelles), en inhibant certaines options, en réalisant des modifications sur le système ou des modifications très limitées sur l'appareil lui-même, comme indiqué par l'Article 8.

j) Le REA doit identifier toutes les modifications correspondant aux 8.3 et 8.4 qu'il peut être nécessaire de réaliser sur l'appareil ou sur le système cible pour intégrer l'appareil candidat dans le ou les systèmes cibles et maintenir le caractère acceptable de celui-ci vis à vis des éléments précédents. De telles modifications de l'appareil doivent avoir un domaine limité et ne pas toucher à la conception du logiciel ou des HPD, ceci afin que l'appareil offre toujours la fonction d'origine; sinon l'appareil n'est plus un appareil industriel standard relevant de la présente norme.

NOTE 2 Des exemples de telles modifications sont le remplacement d'une résistance d'une impédance donnée par une autre, la modification de dispositifs de montage, ou la substitution de composant d'ajustement pour un commutateur ou pour un potentiomètre.

k) Le REA doit identifier toutes les restrictions concernant l'utilisation de l'appareil pour la classe de sûreté pour laquelle il est acceptable.

l) Le REA doit identifier les mesures (et leur pertinence) qu'il est recommandé de mettre en œuvre pour garantir que l'utilisation de l'appareil candidat pour l'application respecte toutes les restrictions et les recommandations apparaissant dans le REA.

m) Le REA doit présenter les conclusions finales pour ce qui est du caractère acceptable du ou des appareils candidats pour leur utilisation dans chacune des applications cibles, indiquant que:

- l'appareil candidat est acceptable tel quel, ou
- l'appareil candidat est acceptable sous les conditions dont la liste est fournie, ou
- l'appareil candidat n'est pas acceptable.

### 5.3.4 Application des articles de la présente norme

L'objet de ce paragraphe est d'indiquer comment appliquer les exigences fournies par les Articles 6 à 9 lors de l'évaluation d'appareils numériques industriels présentant des fonctionnalités dédiés telles que définies en 3.7 destinés à être utilisés pour une application donnée.

a) Le caractère applicable de la présente norme doit être justifié conformément aux critères d'application de 5.2.2.

b) L'évaluation de l'appareil candidat doit être réalisée sur la base de la fonction prévue et de sa catégorie ou de l'application prévue et de son classement.

c) Les preuves doivent être contenues dans des documents pour prouver l'aptitude de l'appareil candidat pour ce qui concerne les aspects fonctionnels ou de performance, comme défini dans l'Article 6, ceci reposant sur tous les critères applicables de cet Article.

d) Les preuves doivent montrer l'exactitude et la précision du PEA en se basant sur une évaluation qualitative combinée de tous les critères applicables de l'Article 7.

e) L'évaluation doit identifier toutes les restrictions à respecter qui restreindront l'utilisation de l'appareil aux limites associées aux preuves documentées conformément à l'Article 7.

f) L'évaluation doit identifier toutes les restrictions à respecter pour garantir l'utilisation sûre de l'appareil candidat dans l'application cible, voir l'Article 8.

g) Les preuves doivent montrer que les résultats de l'évaluation peuvent être garantis pour une période de temps appropriée, prenant en compte la durée de vie de la centrale et les prévisions de remplacement des matériels, sur la base des critères applicables établis par l'Article 9.

## 6 Critères concernant l'aptitude fonctionnelle et les performances

### 6.1 Généralités

Les critères concernant l'aptitude fonctionnelle et les performances répondent aux questions:

- L'appareil choisi[5] réalise-t-il les fonctions requises?
- L'appareil choisi réalise-t-il seulement celles-ci? (ou alors, est-ce qu'il est montré que les fonctionnalités non requises n'interfèrent pas avec les fonctions requises?)
- L'appareil choisi réalise-t-il ses fonctions avec une fiabilité appropriée et ses modes de défaillance sont-ils acceptables?
- Les fonctionnalités de l'appareil choisi sont-elles documentées de façon appropriée?

La satisfaction de chaque critère applicable doit être montrée par analyse et/ou par essai. La revue appropriée des spécifications des appareils s'interfaçant doit être faite. Les preuves de ces démonstrations doivent être documentées.

### 6.2 Capacité fonctionnelle de la fonction principale

La ou les fonctions principales de l'appareil candidat doivent satisfaire aux exigences fonctionnelles dérivant des exigences portant sur la centrale et des exigences système. Si l'appareil candidat est à utiliser dans le cadre de l'application prévue:

a) L'appareil candidat doit être capable de fonctionner pour la totalité de la gamme couverte par les signaux associés au procédé de la centrale et sur l'ensemble du domaine opérationnel spécifié pour l'application prévue.

---

5 Normalement, les appareils candidats sont évalués pour une application en tablant à l'avance sur la conformité de ceux-ci aux exigences fonctionnelles venant de l'application. Cet article établit des recommandations portant sur la liste des critères dont il faut faire la revue pour garantir que les critères appropriés sont pris en compte dans l'évaluation de l'appareil candidat.

b) L'appareil candidat doit présenter les caractéristiques requises concernant la précision et le caractère reproductible de son comportement sur toute la gamme.

c) Le temps de réponse de l'appareil candidat doit être conforme à celui demandé et le traitement numérique du signal doit être approprié (défini en termes de critères appropriés, tels que le taux d'échantillonnage, les retards, l'augmentation du temps, la bande passante, les caractéristiques des filtres telles que le cône de fréquence, l'élimination du bruit, etc.).

d) Lorsque la fonction de transfert du domaine de fréquence est à prendre en compte (comme par exemple dans le cas d'une application en boucle fermée), l'appareil candidat doit présenter des gains et des possibilités de changement d'états appropriés sur la gamme de fréquences en question.

e) Les modes de défaillance doivent être bien définis, et pour ces modes de défaillance les valeurs des sorties doivent être forcées à des états de sortie prédéterminés (par exemple circuit ouvert, ou une augmentation ou une réduction de la valeur de sortie, ou un maintien de la valeur de sortie), qui sont de façon inhérente sûre pour l'application cible, ou qui sont en même temps détectables et permettent d'atteindre un état sûr pour l'application, ou lorsqu'ils ne sont pas détectables et ne permettent pas d'atteindre un état sûr pour l'application ils doivent avoir une probabilité faible acceptable .

f) En lien avec le point e), les modes de défaillance doivent être analysés au niveau de l'impact qu'a l'appareil candidat sur le système au sein duquel il est installé, en prenant en compte tous les facteurs qui peuvent influencer les modes de défaillance (voir aussi 6.7). Il convient de faire particulièrement attention aux défaillances de cause commune, en particulier à celles relatives à d'autres appareils (éventuellement appartenant à d'autres classes) qui ont un rôle déclaré dans l'analyse de sûreté dans la protection contre les mêmes évènements initiateurs.

### 6.3 Fonctions auxiliaires

Les fonctions auxiliaires de l'appareil candidat sont des fonctions qui ne font pas partie de la fonction principale, mais qui sont nécessaires pour pouvoir ajuster les paramètres de la fonction principale afin que celle-ci puisse réaliser la fonction de sûreté requise, ou pour améliorer la fiabilité de l'appareil, telle que l'auto-surveillance.

a) Pour les applications de classe 1 et 2, on doit démontrer par analyse (et/ou par essai si cela peut être fait de manière concluante) qu'aucun fonctionnement ou mode de défaillance des fonctions auxiliaires ne peut interférer avec la fonction principale, hors de ce qui est spécifié (par exemple, par changement manuel d'un point de consigne) ou bien on doit démontrer que cela entraîne la défaillance dans un état sûr par rapport au contexte de l'application.

NOTE 1 Le mode de défaillance sûr dépend de l'application, et ne correspond pas toujours à l'arrêt sur défaillance ou à l'ouverture du contact sur défaillance. Certains exemples sont donnés en7.2.

b) Les fonctions auxiliaires associées au réglage des paramètres des fonctions principales doivent satisfaire aux critères de 6.4.

c) Pour les applications de classe 3, lorsqu'il est estimé que plusieurs appareils sont équivalents pour tous les autres aspects, l'appareil qui a la probabilité la plus faible d'être perturbé par les défaillances de fonctions auxiliaires doit être choisi. Les nombres, les probabilités et les sévérités associés aux défaillances des fonctions auxiliaires doivent être les facteurs utilisés pour la comparaison.

d) Lorsqu'un appareil externe d'une classe inférieure est utilisé pour communiquer avec l'appareil candidat, aucun fonctionnement ou défaillance de l'appareil externe ne peut interagir d'une façon non prévue avec la fonction principale de l'appareil candidat.

NOTE 2 Cette exigence repose sur l'exigence de la CEI 61513 applicable aux communications qui stipule qu'un système de classe plus élevé ne peut pas être perturbé de façon non prévue par un système de classe inférieure. Les communications entre classes sont donc habituellement faite à sens unique (comme par exemple pour les systèmes de surveillance qui ne peuvent pas perturber les systèmes de classes supérieures) ou bien les communications sont seulement temporairement autorisées. En outre, le système de niveau supérieur est généralement testé juste après la période pendant laquelle la communication dans les deux sens est autorisée, et la communication dans les deux sens est contrôlée pour que seulement un canal du système de niveau supérieur soit connecté à un instant donné.

### 6.4 Configurabilité

Les fonctions de l'appareil candidat qui sont configurables et les fonctions auxiliaires permettant d'assurer cette configuration doivent ensemble satisfaire aux exigences suivantes:

a) Les possibilités de configuration des paramètres des fonctions principales doivent être limitées à l'activation/désactivation d'un paramètre TOR ou à l'ajustement du paramètre dans sa gamme, comme: étalonnage dans une gamme procédé, augmentation ou réduction d'un seuil, etc.

b) Pour les applications des systèmes de classe 1 et 2, les fonctionnalités de protection associées à la configuration doivent intégrer de façon délibérée au niveau conception des mesures impliquant qu'il soit nécessaire que plus d'une faute ait été commise pour qu'une erreur soit introduite au niveau du réglage d'un paramètre de configuration.

NOTE 1 Il est de pratique courante de vérifier les impacts de tout changement de ses paramètres de configuration sur la fonction principale d'un appareil candidat.

c) La configuration des paramètres des fonctions principales doit être protégée des ajustements non autorisés, réalisés par inadvertance ou mal intentionnés de façon cohérente avec le plan de sécurité d'ensemble en vigueur pour l'installation nucléaire (voir 5.4.2 de la CEI 61513). Ces fonctionnalités de protection doivent comprendre une protection par mot de passe si cela est supporté par l'appareil candidat.

Il est ainsi permis d'avoir des accès non protégés en lecture seule aux paramètres de configuration, si ces accès en lecture seule satisfont aux exigences de non-interaction des fonctions auxiliaires établies par le point d) ci-après.

Pour les systèmes de classe 1, la limitation des accès physiques comprend aussi des contraintes d'accessibilité telles que le verrouillage des armoires ou des locaux électriques. (Cette exigence est applicable aux installations, pas à l'appareil candidat, ainsi elle relève donc de la responsabilité de l'utilisateur final.)

d) Lorsqu'il est nécessaire de configurer les fonctions auxiliaires ou superflues pour qu'elles ne puissent pas interagir avec les fonctions principales, ces configurations de paramètres doivent faire l'objet de mesures de protection comme indiqué aux points b) et c).

e) Il doit être possible de vérifier sur l'appareil, après que ses paramètres de configuration aient été changé que les modifications ont été faites correctement.

f) Si l'appareil fournit aux opérateurs des possibilités d'affichages ou permet de modifier ou autoriser l'accès à des paramètres de configuration, alors l'appareil doit permettre, par système d'autorisation d'accès, la lecture et la modification par les opérateurs des seuls paramètres nécessaires à la réalisation de leur travail.

g) Si l'appareil permet que les exploitants aient accès en modification aux paramètres de configuration, alors la validité et l'appartenance aux gammes applicables des données entrées par les exploitants doivent être vérifiées et/ou limitées de façon appropriée par rapport à l'application.

h) S'il est requis que les paramètres de configuration et tous les états logiques nécessaires puissent être automatiquement restaurés après une perte, partielle ou complète, des sources électriques, cette fonctionnalités doit être configurable, ces paramètres de configuration doivent être protégés conformément aux points b) et c).

Le terme d'intégration d'un filtre ou d'une régulation PID sont habituellement à l'origine d'à-coup lors de la reprise d'exploitation après un transitoire de puissance.

i) Si un appareil doit fonctionner dans un système comportant plusieurs canaux des dispositions doivent être prises pour garantir qu'un seul canal du système redondant puisse faire l'objet d'un changement de paramètre à un instant donné.

NOTE 2 Ceci est classique pour les systèmes de classe 1 ou 2.

### 6.5 Fonctions superflues

Les fonctions superflues de l'appareil candidat sont ces fonctions qui ne font pas partie des fonctions de sûreté requises de l'appareil, et qui ne sont pas nécessaires comme fonctions

auxiliaires. Etant donné que les fonctions superflues sont indissociables de l'appareil, leur présence correspond potentiellement à une complexité inutile et introduit de façon potentielle des modes de défaillances supplémentaires, ce qui est indésirable pour les applications de classes de sûreté les plus élevées.

a) Pour les applications de classe 1 et 2, il doit être démontré par analyse (et/ou par essai si cela peut être fait de façon concluante) qu'aucun mode de défaillance des fonctions superflues ne peut interagir avec la fonction principale.

b) Pour les applications de classe 1 et 2, il doit être démontré par analyse (et/ou par essai si cela peut être fait de façon concluante) qu'en toutes circonstances opérationnelles, les fonctions superflues peuvent être configurées (ou alors fonctionnent de façon native) pour qu'elles n'interagissent pas avec la fonction principale.

c) Pour les applications de classe 3, lorsqu'il est estimé que plusieurs appareils sont équivalents pour tous les autres aspects, l'appareil qui a la probabilité la plus faible d'être perturbé par les fonctions superflues ou par leurs défaillances doit être choisi. Les nombres, les probabilités et les sévérités associés aux défaillances hypothétiques des fonctions superflues doivent être les facteurs utilisés pour la comparaison.

d) Pour les applications de classe 1 et 2, s'il ne peut pas être prouvé qu'une fonction superflue n'interagit pas avec la fonction principale comme demandé par les points b) et c), alors celle-ci doit satisfaire aux exigences applicables pour une conception de sûreté comme cela est exigé pour la ou les fonctions principales.

e) Pour les applications de classe 1 et 2, il doit être démontré par analyse (et/ou par essai si cela peut être fait de façon concluante) que, pour toutes circonstances opérationnelles, aucun fonctionnement ou aucune défaillance d'un appareil externe en communication avec l'appareil candidat est capable d'interagir d'une façon non prévue avec la fonction principale de l'appareil candidat. Si ceci ne peut pas être démontré alors la fonction principale de l'appareil candidat doit être de testée en fonction des communications établies avec l'appareil externe.

NOTE 1 Voir la note relative à 6.3 d.

f) Les fonctions superflues doivent être éliminées de préférence par rapport à la réduction du nombre de fonctions auxiliaires.

NOTE 2 Le paragraphe 8.3 s'applique pour les modifications de l'appareil.

### 6.6 Robustesse du matériel

La robustesse du matériel est évaluée par la qualification fonctionnelle et environnementale (aussi appelée qualification matérielle); celle-ci est nécessaire pour garantir que l'appareil candidat réalisera ses fonctions dans tous les environnements (états de fonctionnement normal, accidentel et post-accidentel de la centrale) pour lesquels l'exécution des fonctions est requise.

La CEI 61513 traite de la robustesse du matériel en 6.4.2.1 et fait référence aux CEI 60780, et CEI 60980 qui à leur tour font référence à d'autre normes pertinentes sur le sujet. La CEI 61513 autorise la qualification à des conditions industrielles pour les appareils utilisés dans des applications de classe 3, mais demande des preuves documentées si ceux-ci sont réputés fonctionner dans des conditions d'environnement anormales. Une façon d'atteindre cet objectif est d'appliquer la CEI 60780.

NOTE 1 La CEI 61513 fait aussi référence à la CEI 60987 pour les systèmes programmés développés sur demande utilisés dans le cadre d'applications de classe 1 et 2.

a) La robustesse de l'appareil candidat doit être évaluée pour toutes les conditions environnementales (température, pression, taux d'humidité, rayonnement, IEM) et pour les périodes de temps associées à ces conditions, pendant lesquelles il est prévu que l'appareil réalise sa fonction (ceci peut comprendre les conditions prévalant à l'intérieure de l'enceinte de confinement).

b) Pour qualifier l'appareil candidat, on doit évaluer la robustesse de l'appareil suivant les exigences des normes auxquelles il est fait référence ci-dessous; et lorsque la conformité

à une norme n'est pas documentée, cette carence doit être analysée et justifiée ou bien des mesures compensatoires doivent être mises en œuvre pour prendre en compte les points suivant:

- température et taux d'humidité en conformité avec la CEI 60780 pour la classe 1 et 2 et en conformité à la CEI 61513 pour la classe 3,
- rayonnements,
- vibrations et conditions sismiques en conformité avec la CEI 60980,
- immunité aux interférences électromagnétiques en conformité avec les normes de la série CEI 61000,

NOTE 2 La norme CEI 62003 traite des interférences électromagnétiques et est applicable aux systèmes importants pour la sûreté utilisés dans les centrales nucléaires de puissance. Elle référence un bon nombre des différentes parties de la CEI 61000-4. La CEI 61000-6-2 est la norme couramment utilisée par l'industrie.

- Poussière et particules aérosol.

c) Pour qualifier l'appareil candidat, on doit aussi prendre en compte les effets produits par l'appareil candidat sur les autres appareils intégrés dans le système dans lequel l'appareil candidat doit être mis en œuvre. Cela peut nécessiter la modification de l'appareil ou de faire une évaluation des autres appareils suivant les recommandations du point a) qui précède, en considérant la présence de l'appareil candidat dans leurs environnements de fonctionnement. On doit prendre en compte:

- les vibrations produites par l'appareil candidat,
- la chaleur produite par l'appareil candidat,
- l'immunité aux interférences électromagnétiques produites par l'appareil candidat, et
- l'impact sur la qualification sismique des structures sur lesquelles les appareils seront installés.

### 6.7 Fiabilité, aptitudes à la maintenance et aux essais

La fiabilité et les aptitudes à la maintenance et aux essais sont des propriétés propres à l'appareil, du fait que la fréquence d'essai est principalement déterminée par le taux de défaillance inhérent de l'appareil ou du système en question et aussi par la probabilité de défaillance à la demande requise. L'aptitude à la maintenance joue un rôle en permettant de réduire le temps de réparation et d'éviter les défauts liés à la maintenance qui pourraient entraîner des défaillances.

Les exigences applicables pour la conception des essais périodiques et des autotests (auto surveillance) sont établies par la CEI 60671. Ce paragraphe met en exergue les questions relatives aux essais et à la maintenance à se poser pour la sélection, l'évaluation et l'utilisation de l'appareil candidat dans le cadre de l'application.

Les AMDE (Analyse des Modes de Défaillances et de leurs Effets), AMDEC (Analyse des Modes de Défaillances, de leurs Effets et de leurs aspects Critiques) et les AMDED (Analyse des Modes de Défaillances, de leurs Effets et de leurs Diagnostiques) sont des méthodes couramment acceptées pour réaliser des analyses systématiques de l'appareil et ainsi déterminer les modes de défaillance du matériel, leur fréquence et leur impact. Parmi les autres techniques utilisées il y a l'Analyse des Arbres de Défaillance (AAD).

L'appareil candidat doit être évalué par rapport aux critères dont la liste est donnée ci-dessous et le résultat de l'évaluation doit être consigné dans un document:

a) Une analyse doit être réalisée pour déterminer (ou confirmer) les modes de défaillance de l'appareil, et déterminer s'ils sont sûrs ou dangereux dans le contexte prévu de ou des applications.

Les modes de défaillance sont à interpréter par rapport aux objectifs fixés à l'appareil et à son impact sur la sûreté de la centrale. Pour cela il peut être nécessaire d'identifier les besoins et de choisir la polarisation ou la dépolarisation en cas de défaillance, de se replier sur la valeur

supérieure ou inférieure de la gamme ou encore de maintenir la valeur courante, ou bien de signaler immédiatement la défaillance pour que son impact sur la sûreté de la centrale puisse être évaluée par le personnel d'exploitation.

b) Pour les applications prévues de classe 1 et de classe 2, il convient de montrer par analyse qu'une part importante acceptable des modes de défaillance du matériel sont bien définis, qu'ils seront détectés et signalés.

c) Pour les applications prévues de classe 1 et de classe 2, il convient de montrer par analyse que les sous ensemble de défauts qui pourraient être dangereux dans le cadre de l'application ont été minimisés et que leur probabilité d'occurrences est acceptable pour l'application.

d) Dans le cas où les exigences liées aux applications font référence à des valeurs quantitatives de taux de défaillance, une analyse quantitative doit être utilisée pour déterminer les taux de défaillance. Il doit être démontré par cette analyse qu'une partie acceptable des modes défaillance qui pourraient être dangereux sont détectés et signalés ou sont gérés pour devenir des défaillances sûres en temps opportun et avec une probabilité suffisamment basse pour être acceptable dans le cadre de la satisfaction des exigences pertinentes pour les applications.

NOTE 1 Des exemples de méthodes quantitatives sont les AAD et les AMDED. Voir aussi 5.3 de la CEI 60987.

NOTE 2 Des normes telles que la CEI 61508 fournissent des recommandations applicables à ces techniques.

NOTE 3 L'importance donnée à la détection des défauts en un temps donné permet de lancer les actions correctives manuelles et le remplacement de l'appareil en défaut par un autre opérationnel dans un délai suffisamment court compatible avec les objectifs de disponibilité fixés pour les fonctions de sûreté.

e) Les disposition prévues au niveau de la conception pour l'auto-supervision et pour les tests de surveillance périodique ne doivent pas risquer d'interagir de façon intempestive avec les mesures de protection mises en place pour défendre la fonction principale de l'appareil contre des interactions avec les fonctions auxiliaires et superflues ni ne doivent risquer de modifier de façon inappropriée les paramètres de configuration.

f) Lorsqu'un appareil comprend des fonctionnalités d'auto-supervision, la détection d'une défaillance doit être signalée ou une position de repli des sorties correspondant à un état sûr dans le contexte de l'application doit être adoptée.

g) Les essais périodiques définis pour démontrer que l'appareil est disponible de façon continue doivent être conçus pour augmenter au maximum la probabilité que la fonctionnalité détecte les défauts non révélés par l'auto-supervision.

h) Il convient de prendre en compte dans l'évaluation de l'appareil les dispositions prises pour les essais, en particulier si ceux-ci sont compliqués, en considérant les critères suivants:

- procédures de maintenance et des essais de surveillance, ainsi que les intervalles associés,
- complexité et fréquences des essais requis,
- aspects pratiques pour effectuer les essais en fonctionnement en puissance,
- évaluation des outils logiciels nécessaires pour les essais.

i) Les composants particuliers dont la durée de vie est limitée (par exemple les capacités aluminium ou électrolytiques) doivent être identifiés pour pouvoir approvisionner des lots de remplacement de ces composants ou des appareils avant que le taux de défaillance prévu de l'appareil ne montre à l'évidence que la fin de la durée utile est atteinte.

NOTE 4 Les composants se dégradent plus ou moins suivant les différentes conditions d'environnement (par exemple: température, rayonnements, vibrations, etc.) et ceci peut avoir pour conséquence des différences pour l'identification des ensembles de composants à durée de vie limitée, en fonction de l'application.

### 6.8 Cybersécurité

L'appareil candidat et les outils d'essai, de maintenance ou de configuration associés doivent être couverts par l'évaluation relative à la cybersécurité faite au niveau du système dans lequel il est intégré.

NOTE 1 La norme CEI 62645 établit les exigences applicables pour les programmes de cybersécurité.

NOTE 2 La CEI 61513 fournit les exigences à prendre en compte pour la sécurité au niveau de l'architecture de l'I&C et des systèmes d'I&C individuels.

NOTE 3 La CEI 60880 fournit les exigences concernant la sécurité logiciel pour les applications de classe 1 et la CEI 62138 fournit les exigences concernant la sécurité logiciel pour les applications de classe 2 et 3.

### 6.9 Documentation de sûreté pour l'utilisateur

L'appareil candidat doit être accompagné des documentations de conception et de vérification (voir 7.4.6) et des instructions concernant l'utilisation sûre de celui-ci. L'utilisation sûre de l'appareil signifie que les objectifs de sûreté fixés pour l'application seront atteints, si l'appareil est installé, configuré et maintenu de façon appropriée, conformément à la documentation transmise par le fournisseur de l'appareil.

a) La documentation de sûreté pour l'utilisateur peut comprendre les documents suivant:

- Manuel de sûreté – document ou index pointant vers les documents dans lequel ou lesquels sont données les exigences pertinentes pour garantir l'utilisation sûre de l'appareil pour l'application, y compris l'indentification précise de l'appareil et l'identifiant précis de sa version.
- Manuel d'installation – document qui définit la façon suivant laquelle on doit installer l'appareil et on doit le brancher aux autres appareils pour que ses performances soient conformes aux spécifications fonctionnelles.
- Manuel utilisateur ou manuel d'exploitation – document qui définit la façon suivant laquelle l'utilisateur exploitant interagira avec l'appareil (ceci couvre par exemple l'interprétation des affichages des données par le personnel de conduite, et la procédure de modification de toutes les valeurs modifiables).
- Manuel de maintenance – document qui couvre tous les aspects liés à la maintenance de l'appareil sur le terrain: précautions de sûreté pour le personnel de maintenance, précautions de sûreté pour le système, essais de l'appareil in situ, retrait de l'appareil du service et remise en service.

NOTE Les exigences précises concernant la documentation, tel que le titre ou e domaine d'application spécifiques de chaque document dépendront des particularités de l'organisation d'exploitation.

La présente norme n'impose pas de titre ou de domaine d'application particuliers pour chaque document; par contre elle exige que tous les sujets soient documentés dans un ensemble documentaire.

b) Pour que l'appareil candidat soit utilisé correctement et de manière sûre, les documents décrits dans le point a) ci-dessus, considérés comme un ensemble, doivent fournir les informations suivantes:

- Version complète de l'information.
- Documentation exhaustive de la fonction principale pour ce qui est de ses fonctionnalités d'ensemble externes, ceci couvrant les effets particuliers liés aux paramètres de configuration, interfaces de l'appareil, le comportement au démarrage, le comportement lors de la perte d'alimentation, les effets des défaillances, le temps de réponse et le domaine de fréquence (le cas échéant), taux de rafraichissement, impédance des entrées et des sorties ainsi que les gammes associées, etc.
- Documentation complète de la fonction principale pour ce qui concerne les modes de défaillance et l'indication des défaillances.
- Documentation complète des fonctions auxiliaire et superflues pour ce qui concerne les fonctionnalités, y compris lorsque cela est pertinent les moyens de configuration pour prévenir les interactions avec la fonction principale.
- Les exigences portant sur l'intégrité fonctionnelle, telles que l'auto-surveillance pour détecter les défaillances du matériel ainsi que les actions à déclencher suite à la détection d'une défaillance (ceci étant distinct des exigences fonctionnelles).
- Les limitations environnementales et en termes de robustesse de l'appareil, les composants susceptibles de limiter la durée de vie.

- Toutes les procédures de maintenance et les précautions de bon aloi.
- Toutes les procédures d'exploitation et les précautions de bon aloi.
- Toutes les procédures et les exigences applicables pour les essais de surveillance périodiques et les précautions de bon aloi,
- Toutes autres informations importantes relatives à l'utilisation sûre de l'appareil et les précautions de bon aloi.

# 7 Critères liés à la sûreté de fonctionnement – preuves d'exactitude et de précision

## 7.1 Généralités

L'objet de ce paragraphe est de fournir des recommandations sur:

- la collecte et l'évaluation des preuves démontrant que l'appareil candidat est apte à être utilisé dans une application importante pour la sûreté dans une centrale nucléaire de puissance du fait du processus suivi pour sa conception et pour sa fabrication, et
- les moyens qui peuvent être utilisés pour compenser les faiblesses de cet ensemble de preuves qui concerne l'exactitude et la précision de la conception et de la fabrication de l'appareil.

NOTE 1 L'évaluation des preuves concernant la précision et l'exactitude de la conception et de la fabrication de l'appareil est habituellement qualitative car il n'y a pas de moyens communément reconnu pour la quantifier, et aussi car il peut ne pas être possible d'obtenir le genre de preuves définies dans cet article. Cette évaluation repose sur une estimation équilibrée du produit et des éléments relevant des processus: de la conception comme de la fabrication qui ont été documentés; cette évaluation prend en compte la possibilité que certains éléments de preuve de la précision et de l'exactitude de la conception et de la fabrication puissent individuellement ou en combinaison compenser la faiblesse limitée d'autres preuves dans les paragraphes correspondant.

Les preuves concernant la précision et l'exactitude de la conception et de la fabrication de l'appareil doivent être fournies par:

- l'évaluation du processus de production de l'appareil et celui par lequel la conception est maintenue de façon courante (y compris sa vérification et sa validation pour la conception courante comme pour les modifications),
- l'évaluation de la documentation de développement de l'appareil,
- l'évaluation du processus de fabrication de l'appareil, et
- l'évaluation des attributs de l'appareil lui-même.

Les preuves concernant la précision et l'exactitude traitent de façon séparée la conception et la fabrication car les moyens adaptés permettant de compenser les faiblesses des preuves sont différents pour la conception et pour la fabrication.

En outre, des mesures particulières compensatoires ne peuvent pas être appliquées de façon générale; les mesures particulières compensatoires sont appliquées seulement pour des carences particulières portant sur les principaux éléments de preuve de l'exactitude et de la précision.

Les principaux éléments de preuves relatifs à la précision et l'exactitude de la conception comprennent:

- les preuves liées au cycle de vie rigoureux employé pour le développement et pour la maintenance lors de la conception,
- les preuves de l'utilisation d'outils en support du cycle de vie rigoureux (par exemple contrôle des modifications, gestion des configurations),
- les preuves supportant la présomption d'une faible probabilité de présence de défauts systématiques,

- la revue de la documentation du développement, y compris sa vérification et sa validation,
- la revue de la documentation de conception et d'exploitation de l'appareil.

NOTE 2 Si une pré-évaluation générique ou une certification de l'appareil candidat a eu lieu, celle-ci peut constituer une source pratique de références à des preuves ou contenir des analyses utiles.

Les moyens qui peuvent être utilisés pour compenser certaines faiblesses des principaux éléments de preuve relatifs à la précision et l'exactitude de la conception comprennent:

- le retour d'expérience du terrain pertinent et crédible, qui peut être utilisé comme justification pour compenser la faiblesse d'autres éléments,
- les preuves de stabilité du produit (à savoir un taux de modification bas) durant un temps significatif au niveau fabrication et utilisation du produit,
- les essais complémentaires particuliers réalisés sur l'appareil pour combler des manques au niveau de la documentation d'essai ou pour étendre la couverture d'essai, tenant compte de l'application prévue et des autres preuves relatives à la précision et à l'exactitude,
- les mesures compensatoires prises au niveau système pour limiter les conséquences de la défaillance de l'appareil ou pour que les défaillances deviennent sûres,
- les améliorations de la documentation fournie initialement par le concepteur.

Les principaux éléments de preuves relatifs à la précision et l'exactitude de la fabrication comprennent:

- les preuves liées au cycle de vie rigoureux employé pour le développement et pour la maintenance lors de la fabrication, y compris le contrôle des modifications et la gestion de configuration,
- la revue de la documentation de fabrication et d'exploitation de l'appareil.

Les moyens qui peuvent être utilisés pour compenser certaines faiblesses des principaux éléments de preuve relatifs à la précision et l'exactitude de la fabrication comprennent:

- les preuves de stabilité du produit (à savoir un taux de modification bas) durant un temps significatif au niveau fabrication et utilisation du produit,
- des inspections ciblées de l'appareil, des essais fonctionnels et des essais concernant le vieillissement adaptés aux faiblesses des preuves de précision et d'exactitude concernant la fabrication qui sont à compenser,
- l'approvisionnement d'un nombre suffisant d'appareils provenant du même lot de fabrication pour garantir la disponibilité de pièces de rechange pour la durée de vie de la centrale nucléaire de puissance.

Le PEA (voir 5.3) identifie et justifie comment il convient de classer les exigences des paragraphes suivants en termes d'importance, et quelles mesures compensatoires permises seront prises en compte.

Certains paragraphes ci-dessous utilisent des tableaux pour définir plus clairement les exigences relatives aux trois classes de sûreté et les mesures compensatoires permises. Ces tableaux doivent être interprétées de la façon suivante:

a) «O» indique le caractère obligatoire de l'application du critère décrit, correspondant à l'utilisation de «doit» dans la formulation de l'exigence.

b) «R» indique le caractère recommandé de l'application du critère décrit, correspondant à l'utilisation de «il est recommandé, il convient» dans la formulation de l'exigence.

c) Les colonnes repérées par «MC» indique les mesures compensatoires qui peuvent être permises, et

- «SP» indique que l'application de la mesure relative à la stabilité du produit conformément à 7.6 est permise pour compenser jusqu'à un certain degré la faiblesse de la preuve principale,
- «REX» indique que l'application de la mesure relative au retour d'expérience conformément à 7.7 est permise pour compenser jusqu'à un certain degré la faiblesse de la preuve principale,
- «EC» indique que l'application de la mesure relative aux essais et/ou aux analyses complémentaires conformément à 7.8 est permise pour compenser jusqu'à un certain degré la faiblesse de la preuve principale,
- «AD» indique que l'application de la mesure relative à l'amélioration de la documentation conformément à 7.9 est permise pour compenser jusqu'à un certain degré la faiblesse de la preuve principale,

Les mesures compensatoires possibles ne doivent pas être interprétées comme des moyens permettant d'échapper de façon importante à la nécessité attachée à la fourniture des principales formes de preuves; les indications fournies par les tableaux offrent plutôt la possibilité d'appliquer des mesures compensatoires qui doivent être utilisées avec parcimonie.

NOTE 3 Un besoin important de recourir aux mesures compensatoires indique des carences au niveau processus de développement bien défini ou une adhérence forte au processus déclaré, et ceci peut remettre en cause l'acceptation de l'appareil candidat.

NOTE 4 A titre d'exemple, la présence de «O» dans la colonne correspondant à la «classe 3» et la présence de «EC» dans la colonne MC pour la classe 3 veut dire que l'application du critère est obligatoire pour la classe 3 mais que certaines faiblesses au niveau de la satisfaction de ce paragraphe par le concepteur ou par le fabricant peuvent être compensées en produisant une documentation pour des essais et/ou des analyses complémentaires conformément à 7.8.

### 7.2 Certification préalable

En général, le fait de choisir un appareil qui a déjà été certifié par rapport à une norme de sûreté appropriée présente des avantages significatifs. Les modes de défaillance de tels appareils ont généralement été bien définis; ils ont généralement été développés en suivant un processus de développement rigoureux pour le logiciel ou pour les HPD; ainsi il est probable que la documentation support existe, même si elle peut être propriétaire.

NOTE 1 La CEI 61508 est une norme de sûreté appropriée.

Cela est souvent très différent pour les produits non certifiés, car généralement ils ont été développés avec l'objectif de les mettre rapidement sur le marché et ils sont fréquemment modifiés pour ajouter de nouvelles fonctionnalités. Ainsi les produits non certifiés peuvent comprendre des fonctionnalités non requises par l'application nucléaire prévue. De plus, il se peut que les produits contiennent des fonctionnalités qui ne sont pas seulement non requises mais qui ne sont également pas définies de façon transparente (à savoir que la fonctionnalité est cachée) dans les spécifications du produit. A contrario, les appareils développés conformément à des normes de sûreté, ont plus de chance d'avoir leurs fonctionnalités particulières bien définies.

Le second avantage d'un appareil certifié par rapport à une norme de sûreté sur un produit non certifié est que le processus de sélection peut s'engager avec l'assurance que les preuves relatives à la précision et à l'exactitude qui sont nécessaires seront disponibles, car le processus de développement suivi dans le cadre de telles normes peut exiger la production d'une documentation similaire à celle requise par les normes nucléaires.

NOTE 2 La CEI 62138 et la CEI 60880 sont des normes nucléaires qui imposent ce genre d'exigence pour la documentation.

On doit néanmoins faire attention lors de l'évaluation des produits certifiés comme de ceux non certifiés pour ce qui concerne les modes de défaillance. Même si les modes de défaillance des appareils certifiés par rapport à une norme de sûreté non nucléaire peuvent avoir été bien définis, ils ont généralement été considérés suivant le principe d'arrêt du

processus, tel que l'arrêt réacteur, alors que pour d'autres applications nucléaires la position de repli qui peut être requise après défaillance n'est pas l'arrêt. Par exemple, le fonctionnement des générateurs diesel et des contrôleurs des compresseurs est nécessaire une fois qu'un accident est survenu; dans ce cas il convient que le contrôleur de l'appareil signale simplement les alarmes relatives à l'état de l'appareil, telles que la présence de vibrations importantes qui entraînerait l'arrêt de l'appareil dans le cas d'une application non nucléaire.

Ainsi en général, l'évaluation d'un appareil industriel est facilitée et peut être simplifiée si l'appareil a été au préalable certifié par rapport à une norme de sûreté non nucléaire, mais cela n'est pas suffisant, et il y a plusieurs conditions à satisfaire pour qu'on puisse utiliser en confiance cette certification.

La certification par rapport à une norme de sûreté non nucléaire, peut être utilisée comme preuve pour satisfaire aux critères de l'Article 7, dans ce cas la certification doit satisfaire aux critères suivant:

a) Si une certification par rapport à une norme de sûreté non nucléaire qui n'est pas largement reconnue est utilisée en appui pour obtenir la conformité aux exigences d'un paragraphe de la présente norme, alors cette utilisation doit faire l'objet de justifications.

b) Si une certification est utilisée en appui pour obtenir la conformité aux exigences d'un paragraphe de la présente norme, alors cette certification doit fournir les preuves relatives à la précision et à l'exactitude qui sont directement pertinentes pour ce qui concerne les exigences dudit paragraphe.

c) Les éléments matériels supports des preuves de la certification doivent être disponibles pour faire l'objet de revues. Ces preuves doivent couvrir tous les éléments nécessaires pour évaluer de façon indépendante le domaine d'application et les limites de la certification, en particulier:

   - la documentation évaluée,
   - les hypothèses faites concernant l'utilisation prévue de l'appareil et son comportement attendu dans tous les cas d'utilisation,
   - la certification des méthodes et des outils,
   - les propriétés de l'appareil évaluées (si la conclusion de l'évaluation a été positive ou non) et les résultats.

d) La certification doit être en cours de validité et doit être valable pour l'appareil candidat, en particulier:

   - Pour les applications prévues de classe 1 et 2, pour lesquelles la défaillance de l'appareil candidat entraînerait une défaillance du système cible (comme par exemple s'il est installé dans tous les systèmes redondants), la certification doit correspondre à la version particulière qui a été certifiée.
   - Pour les applications prévues de classe 1 et 2, pour lesquelles la défaillance de l'appareil candidat n'entraînerait pas une défaillance du système cible, la certification doit correspondre à une version particulière qui au maximum présente des différences avec la version qu'il est prévu d'utiliser, pour des points mineurs qui sont bien documentés et validés et qui ne peuvent pas porter atteinte à la fonction principale.
   - Pour les applications prévues de classe 3, la certification doit correspondre à une version particulière qui au maximum présente des différences avec la version qu'il est prévu d'utiliser, pour des points mineurs qui sont bien documentés et validés.
   - Lorsque la version qu'il est prévu d'utiliser n'est pas identique à la ou aux versions certifiées, la conclusion indiquant que les différences sont mineures doit s'appuyer sur des analyses adaptées et pouvant faire l'objet d'audit. Les différences qui touchent les concepts fondamentaux de conception employés au niveau de l'appareil, tel que le principe physique exploité, la technologie utilisée et les moyens de lutter contre les fautes systématiques ne sont pas mineures. Les différences relatives à l'initialisation des paramètres qui correspondent aux gammes des signaux pourraient être jugées potentiellement mineures.

e) Les conditions d'utilisation prises en compte pour la certification doivent être pertinentes par rapport aux conditions d'utilisation prévues dans le cadre nucléaire (voir aussi 7.7).

f) L'autorité de certification doit être identifiée et doit être indépendante du concepteur de l'appareil et du fabricant.

g) L'autorité de certification doit être compétente pour les propriétés et/ou les mesures certifiées, et sa compétence doit être évaluée sur la base de toutes les informations disponibles par rapport à son expérience et à sa qualification.

### 7.3 Evitement des défauts systématiques

Le critère présenté dans ce paragraphe doit être plus particulièrement appliqué pour les applications prévues de classe 1 et de classe 2, et il convient de l'appliquer pour les applications prévues de classe 3. Il convient de noter que dans le cas de logiciel ou de HPD, l'assurance concernant l'évitement des défauts systématiques est principalement obtenue sur la base d'analyses. A contrario, cependant, les conditions environnementales peuvent aussi entraîner l'apparition de défauts systématiques, dans ce cas la qualification peut reposer sur des analyses ou sur des essais réalisés conformément à la CEI 60780, comme décrit en 6.6.

Les preuves justifiant l'absence de causes potentielles de défauts systématiques pour l'appareil doivent être documentées. Pour définir cela pour chaque classe, ce paragraphe utilise des tableaux dans lesquels «O» veut dire obligatoire et correspond à l'utilisation de «doit» dans une formulation d'exigence, et «R» veut dire recommandé et correspond à l'utilisation de «il est recommandé de» ou «il convient de» dans la formulation d'exigence.

Ceci doit être démontré par l'évaluation de l'architecture d'ensemble de l'appareil, afin d'obtenir l'assurance que:

a) La conception du contrôleur numérique de l'appareil (à savoir la partie numérique de l'appareil) doit être évaluée. Les informations suivantes, telles que définies dans le tableau ci-dessous pour chaque classe, doivent être disponibles pour réaliser cette évaluation:

| | Informations à tenir à disposition | Classe 1 | | Classe 2 | | Classe 3 | |
|---|---|---|---|---|---|---|---|
| | | | MC | | MC | | MC |
| 1 | Fonctionnement d'ensemble du contrôleur de l'appareil numérique, en conditions normales et anormales (y compris en condition de défaut) | O | AD | O | AD | O | AD |
| 2 | Architecture d'ensemble du contrôleur de l'appareil numérique, identifiant et décrivant les rôles des principaux éléments matériel (y compris les circuits intégrés programmable) et les composants logiciel. | O | AD | O | AD | R | AD |
| 3 | Tous les documents nécessaires pour vérifier la conformité aux exigences de l'Article 6, y compris ceux concernant la stratégie de vérification et les essais et les analyses réalisés. | O | EC | O | EC | O | EC |
| 4 | Tous les documents nécessaires pour montrer que la vérification de chaque phase de développement a été faite, y compris ceux concernant la stratégie de vérification, les essais et les analyses réalisés. | O | EC | O | EC | R | EC |

NOTE 1 Les explications pour l'interprétation des indicateurs "O", "R", "AD" et "EC" sont données en 7.1.

NOTE 2 "AD" indique que l'amélioration de la documentation réalisée conformément 7.9 est une mesure compensatoire possible permettant d'apporter des clarifications pour ce qui concerne la conception système.

NOTE 3 "EC" indique que la réalisation d'essais ou d'analyse documentés complémentaires conformément à 7.8 est une mesure compensatoire possible permettant de combler des manques au niveau de la documentation de vérification.

b) Les informations concernant le fonctionnement d'ensemble de l'appareil numérique doivent en particulier couvrir les points particuliers décrits dans la table ci-dessous tels que définis pour chaque classe:

| | Informations à tenir à disposition | Classe 1 | | Classe 2 | | Classe 3 | |
|---|---|---|---|---|---|---|---|
| | | | MC | | MC | | MC |
| 1 | Approche générale de conception (par exemple, conception en fonction du temps versus une conception évènementielle, gestion des ressources statique versus une gestion dynamique, conception électronique synchrone versus une conception asynchrone) | O | AD | O | AD | R | AD |
| 2 | Entrées (y compris les interruptions) et sortie du contrôleur de l'appareil. | O | | O | | O | |
| 3 | Description des traitements permettant de produire, à partir des entrées, les sorties. | O | EC | O | EC | O | EC |
| 4 | Identification précise et caractérisation de tous les facteurs d'influence pouvant affecter le fonctionnement de l'appareil durant l'exploitation. | O | EC | O | EC | R | EC |
| 5 | Différentes tâches (y compris le traitement des interruptions) réalisées au sein de l'appareil. | O | | O | | | |
| 6 | Séquencement et synchronisation des tâches. | O | | O | | | |
| 7 | Protection/séparation des tâches réalisant la fonction principale de l'appareil par rapport à celles réalisant les fonctions auxiliaires. | O | | O | | R | |
| 8 | Facteurs d'influence du temps de réponse et variabilité du temps de réponse de la fonction principale. | O | | O | | R | |
| 9 | Capacités d'essais en ligne et hors ligne et de diagnostique offertes par l'appareil. | O | | O | | R | |
| 10 | Conditions de démarrage, d'arrêt et de réinitialisation, couvrant les transitoires électriques en particulier les pertes d'alimentation, le redémarrage et la réponse de l'appareil. | O | | O | EC | O | EC |

NOTE 4 Les explications pour l'interprétation des indicateurs "O", "R" et "EC" sont données en 7.1.

c) Conformément à le tableau ci-dessous, les preuves indiquées doivent être fournies pour chaque appareil afin de montrer que:

| | Informations à tenir à disposition ou critères à satisfaire | Classe 1 | | Classe 2 | | Classe 3 | |
|---|---|---|---|---|---|---|---|
| | | | MC | | MC | | MC |
| 1 | La fonction principale ne sera pas perturbée par aucune condition d'interruptions. | O | | O | | R | EC |
| 2 | Sur base documentaire il est prouvé que la conception de n'importe quelle mesure d'auto-surveillance est telle que sur détection de faute par les mesures d'auto-surveillance l'appareil produit une alarme ou se met en position de repli sûre. | O | | O | EC | O | EC |
| 3 | Les défauts qui touchent la fonction principale sont détectés par les mesures d'auto-surveillance ou par d'autres moyens tels que les essais périodiques. | O | EC | O | EC | R | EC |
| 4 | Des analyses ont été réalisées et documentées pour identifier les mécanismes de défaillance et les modes de défaillance résiduels (par exemple en utilisant des ADD, AMDE ou des analyses de criticalité), et pour démontrer que les mesures ont été prises pour limiter les probabilités associées aux mécanismes et aux modes de défaillance considérés ici. | O | | O | | | |

NOTE 5 Pour le point 2, la référence à la position de repli sûre repose sur les exigences du point e) de 6.2.

NOTE 6 Pour le point 4, les mesures possibles pourraient comprendre des essais particuliers complémentaires, des limitations au niveau de l'utilisation de l'appareil ou de la surveillance externe.

NOTE 7 Pour le point 4, l'Annexe A fournit des recommandations portant sur les caractéristiques de conception logicielle qui pourraient poser problème au niveau de la satisfaction des exigences de ce paragraphe.

## 7.4 Preuves de la qualité du processus de conception

### 7.4.1 Généralités

L'application des critères présentés dans ce paragraphe fournit l'assurance que le processus de conception présente un caractère systématique et qu'il suit les principes généraux illustrés par les cycles de vie définis dans les normes nucléaires.

Pour l'ensemble des sujets, l'approche générale doit être la suivante:

- obtenir les preuves de l'utilisation par les concepteurs de l'appareil d'un cycle de développement basé sur la qualité,
- comparer les preuves disponibles avec les exigences correspondantes de la CEI 61513, de la présente norme et des autres normes CEI pertinentes pour les centrales nucléaires de puissance, et
- déterminer si les carences, les omissions et les discordances sont acceptables ou non et si, le cas échéant, des mesures compensatoires indiquées pour chaque exigences peuvent être mises en place pour satisfaire à l'exigence et conclure que le candidat peut être accepté.

Les paragraphes ci-dessous présentent les critères qui doivent être pris en compte conformément au présent paragraphe.

### 7.4.2 Programme d'AQ du concepteur du produit

Le tableau ci-dessous définit les exigences applicables pour le programme d'AQ de la conception pour ce qui concerne les informations à tenir à disposition et les critères devant être satisfaits. Les exigences doivent être appliquées en remplaçant "___" par «doit» lorsque l'indication «O» apparait et pour la version française l'exigence doit être reformulée avec «Il est recommandé» ou «Il convient» lorsque l'indication «R» apparait, en conformité avec le tableau ci-dessous:

| | Informations à tenir à disposition ou critère à satisfaire | Classe 1 | | Classe 2 | | Classe 3 | |
|---|---|---|---|---|---|---|---|
| | | | MC | | MC | | MC |
| a | Le concepteur ___ avoir maintenu, suivi et continuer à suivre, un programme d'AQ documenté qui ___ être évalué par rapport aux exigences d'AQ de la CEI 61513. Cette évaluation ___ identifier tous les écarts et les traiter ou fournir une justification concernant leur caractère acceptable. | O | | O | | R | |
| b | Si des parties du processus de développement du logiciel ou du matériel (y compris les HPD) sont spécifiées dans des documents qualité hors du programme d'AQ (par exemple Plan AQ logiciel) ceux-ci ___ être cohérent avec le programme d'AQ d'ensemble. | O | | O | | R | |
| c | Si des parties du processus de développement du logiciel ou du matériel (y compris les HPD) sont spécifiées dans des documents qualité hors du programme d'AQ, alors les exigences de ce paragraphe ___ s'appliquer à tous ces documents qualité subsidiaires. | O | | O | | R | |
| d | Le programme d'AQ **doit** exiger que les recommandations suivantes soient satisfaites au niveau des processus de conception et de développement en fonction du degré indiqué par «O» ou «R»: | -- | | -- | | -- | |
| | 1) Les personnels réalisant les activités de conception et de développement ___ être compétents pour le travail qui leur est attribué. | O | | O | REX EC | R | REX EC |
| | 2) La conception finale ____ être validée indépendamment avec le niveau d'indépendance approprié à la classe de sûreté de l'application prévue. | O | | O | | O | |
| | 3) Chaque phase de conception et de développement ___ permettre de vérifier que les exigences de la phase considérée ont été satisfaites. | O | | O | | R | |

| | Informations à tenir à disposition ou critère à satisfaire | Classe 1 | | Classe 2 | | Classe 3 | |
|---|---|---|---|---|---|---|---|
| | | | MC | | MC | | MC |
| | 4) La gestion de configuration ___ être en place conformément aux exigences de 7.4.4. | O | | O | | O | |
| | 5) Le contrôle des modifications ___ être en place conformément aux exigences de 0. | O | | O | | O | |
| | 6) Les pratiques documentaires ___ être en place conformément aux exigences de 7.4.6. | O | | O | | O | |
| e | Lorsque des outils sont utilisés pour la conception et le développement, le programme d'AQ du concepteur doit avoir demandé leur justification en fonction des objectifs, avec les niveaux indiqués par «O» ou «R». Lorsque les justifications relatives aux outils sont jugées insuffisantes par la personne en charge de la qualification ou par le concepteur de l'application, alors celui-ci doit considérer quelle mesure compensatoire peut être et sera appliquée. | -- | | -- | | -- | |
| | 1) L'historique d'utilisation des outils, les informations relatives à leur stabilité, à leur documentation utilisateur, les comptes-rendus de défaut, etc. | O | REX EC | R | REX EC | | |
| | 2) Possibilités d'introduire défauts ou de ne pas en détecter les défaillances dans la conception de l'appareil, de même que la probabilité que de telles défaillances des outils soient révélées par d'autre moyens. | O | EC | O | EC | | |
| f | Lorsque le concepteur et/ou le fabricant autorise le recours à des sous-contractants, toutes les exigences de la présente norme qui s'appliquent au fabricant de l'appareil ou à son concepteur ___ également s'appliquer aux sous-contractants. | O | | O | | O | |

NOTE Concernant le point e), un outil peut introduire un défaut qui peut ne pas être détecté par d'autres moyens (par exemple par une revue humaine) ce qui impliquerait une justification de même niveau que celle associée à la classe de l'application pour laquelle on a prévu d'utiliser l'appareil dont la conception est dépendante de l'outil. Un outil qui peut présenter une défaillance au niveau de la détection d'un défaut mais qui ne peut pas introduire de défaut pourrait être considéré à un niveau de classe inférieure.

### 7.4.3 Processus de conception et de développement

Le tableau ci-dessous définit les exigences applicables aux processus de conception et de développement en ce qui concerne les informations à tenir à disposition et les critères devant être satisfaits. Les exigences doivent être appliquées en remplaçant "___" par «doit» lorsque l'indication «O» apparaît et l'exigence doit être reformulée avec «Il est recommandé» ou «Il convient» lorsque l'indication «R» apparait, en conformité avec le tableau ci-dessous:

| | Informations à tenir à disposition ou critère à satisfaire | Classe 1 | | Classe 2 | | Classe 3 | |
|---|---|---|---|---|---|---|---|
| | | | MC | | MC | | MC |
| a | Les plans de développement pour le logiciel ou pour le matériel (y compris les HPD) ___ exiger que les processus de conception et de développement suivent un cycle de vie divisant la conception et le développement en phases; | O | | O | | R | |
| b | Pour chaque phase du cycle de vie de conception et de développement, le plan d'AQ ____ exiger la fourniture de détails pour les point suivants:<br>– objectifs,<br>– entrées et sorties,<br>– outils utilises. | O | | O | | R | |
| c | Les preuves concernant la satisfaction de toutes les exigences précédemment citées durant le développement de l'appareil visé ___ être tenues à disposition. Ces preuves ___ être documentées sous une forme permettant de les retrouver et d'en faire la revue. | O | EC | O | EC | R | EC REX |

NOTE Les normes qui exigent la mise en place de cycles de vie adaptés sont en particulier: la CEI 61513 (pour la conception système), la CEI 62138 et la CEI 60880 (pour le logiciel), la CEI 60987 (pour le matériel des systèmes numériques développés sur demande), la CEI 61508 (pour le logiciel et le matériel), ou la CEI 62566 pour les HPD.

### 7.4.4 Gestion des configurations durant la conception

Le tableau ci-dessous définit les exigences applicables à la gestion de configuration pour la conception en ce qui concerne les informations à tenir à disposition et les critères devant être satisfaits. Les exigences doivent être appliquées en remplaçant "___" par «doit» lorsque l'indication «O» apparaît et l'exigence doit être reformulée avec «Il est recommandé» ou «Il convient» lorsque l'indication «R» apparaît, en conformité avec le tableau ci-dessous:

| | Informations à tenir à disposition ou critère à satisfaire | Classe 1 | | Classe 2 | | Classe 3 | |
|---|---|---|---|---|---|---|---|
| | | | MC | | MC | | MC |
| a | Les preuves ____ fournir les détails portant sur l'utilisation du système de gestion de configuration en ce qui concerne le développement de l'appareil candidat, son logiciel et son matériel (y compris les HPD). Ce système de gestion de configuration ___ couvrir toute la documentation de conception et les procédures d'essais de validation ainsi que les rapports d'essai et ceux-ci ___ être en relation avec les versions matérielles, logicielles et des HPD. | O | EC | O | EC | O | EC |
| b | Le système de gestion de configuration ___ avoir été en place pour gérer tous les éléments (documents, revue de conception, logiciel et conceptions des HPD, plans matériel, résultats d'essais, etc.) dès le début du développement de l'appareil. | R | | R | | | |
| c | Le système de gestion de configuration ___ avoir été en place pour gérer tous les éléments (documents, revue de conception, logiciel et conceptions des HPD, plans matériel, résultats d'essais, etc.) dès le début des essais de validation de l'appareil. | O | | O | | O | |

### 7.4.5 Contrôle des modifications en conception

Les preuves doivent fournir les informations montrant que le concepteur continue à maintenir opérationnel un système de contrôle des modifications, qui couvre en particulier les outils logiciel et les procédures, au niveau désigné par les indicateurs «O» et «R» conformément au tableau fourni ci-dessous:

| | Informations à tenir à disposition ou critère à satisfaire | Classe 1 | | Classe 2 | | Classe 3 | |
|---|---|---|---|---|---|---|---|
| | | | MC | | MC | | MC |
| a | Supporter et exiger la convocation du comité de revue qui opère sous un processus défini de gestion et d'approbation des modifications et qui doit donner son autorisation pour toutes les modifications et enregistrer ses décisions. | O | | O | | O | |
| b | Supporter et exiger que les documents correspondant à toutes les modifications de conception matériel, logiciel ou portant sur celle des HPD comprennent les références des autorisations de modifications. | O | | O | | R | |
| c | Systématiquement collecter et enregistrer les rapports concernant les problèmes rencontrés sur le terrain, les problèmes de fabrication qui ont un impact sur la conception et les anomalies d'essai dans le but de les inclure aux données d'entrée du processus de contrôle des modifications.<br>NOTE La présente norme ne peut pas établir d'exigences concernant les mécanismes relatifs aux rapports de retour d'expérience portant sur des problèmes rencontrés sur le terrain pour le cas où un utilisateur final rapporterait un problème au distributeur, au fabricant ou au concepteur de l'appareil. L'essentiel est qu'il soit fourni à l'utilisateur final un point de contact permettant d'établir la communication avec les intervenants les plus à même de traiter le problème décrit. | O | | O | | R | |

| | Informations à tenir à disposition ou critère à satisfaire | Classe 1 | | Classe 2 | | Classe 3 | |
|---|---|---|---|---|---|---|---|
| | | | MC | | MC | | MC |
| d | Enregistrer toutes les versions et les mises à disposition de logiciel, de conception de HPD ou de configuration matériel et pouvoir lister les modifications qui ont été identifiées et qui ont été rectifiées à chaque version ou mise à disposition. | O | | O | | R | |
| e | Supporter et exiger une analyse d'impact pour chaque modification proposée, et utiliser cette analyse d'impact au niveau du processus d'approbation des modifications. Cette analyse d'impact doit prendre en compte l'étendue de la modification, son impact sur les fonctions principales de l'appareil candidat, les possibilités que cela affecte la fiabilité des fonctions principales, la phase du cycle de vie pour laquelle doit débuter le travail, l'étendue et la rigueur nécessaires des essais de validation. | O | | R | | | |
| f | Supporter et exiger une deuxième revue des modifications autorisées par le comité de revue des modifications pour autoriser la mise en production, durant cette revue le comité doit s'appuyer pour donner son approbation sur une revue de complétude et de précision concernant:<br>– la modification de la documentation;<br>– la re-validation de la documentation;<br>– la documentation utilisateur. | O | | R | | | |
| g | Le contrôle des modifications est en place depuis le début du développement du modèle visé de l'appareil. | R | | R | | | |
| h | Le contrôle des modifications est en place depuis le début des essais de validation du modèle visé de l'appareil. | O | | O | | O | |

Il est tout à fait possible de concevoir un processus de contrôle des modifications qui comprenne deux niveaux pour le comité de revue des modifications, s'il y a des procédures et des règles claires permettant au comité de niveau inférieur de reconnaître que la prise en compte d'une modification relève l'autorité du comité supérieur. Ces règles peuvent prendre en compte la classe du système impacté par la modification, l'étendue de la modification ou d'autres critères adaptés.

### 7.4.6 Documentation de conception

La documentation de conception fait partie de la «documentation de sûreté» qui est examinée comme une partie de l'évaluation. L'autre partie de la «documentation de sûreté», qui est fournie aux utilisateurs qui concevront les systèmes qui utiliseront l'appareil ou bien qui feront fonctionner et assureront la maintenance de ces systèmes, est traitée en 6.9.

Le tableau ci-dessous définit les exigences applicables à la documentation de conception en ce qui concerne les informations à tenir à disposition et les critères devant être satisfaits. Les exigences doivent être appliquées en remplaçant "___" par «doit» lorsque l'indication «O» apparaît et l'exigence doit être reformulée avec «Il est recommandé» ou «Il convient» lorsque l'indication «R» apparait, en conformité avec le tableau ci-dessous:

| | Informations à tenir à disposition ou critère à satisfaire | Classe 1 | | Classe 2 | | Classe 3 | |
|---|---|---|---|---|---|---|---|
| | | | MC | | MC | | MC |
| a | Tous les documents ___ être vérifiés et approuvés par des personnels autorisés. | O | | O | | R | |
| b | Tous les documents ___ être complets, corrects et non ambigus. | O | AD | O | AD | R | AD |
| c | Documentation des exigences fonctionnelles:<br>Un document d'exigences fonctionnelles définit les fonctions de l'appareil, qu'elles soient mises en œuvre dans le matériel, dans le logiciel ou sur un HPD. Ce document spécifie en langage explicite les fonctions principales, les fonctions auxiliaires et les fonctions superflues (le cas échéant) ainsi que toutes limitations d'usage de l'appareil.<br>Le concepteur de l'appareil doit avoir produit une documentation couvrant les exigences fonctionnelles qui fournit les informations suivantes en fonction du niveau correspondant aux indicateurs «O» ou «R»: | -- | | -- | | -- | |
| | 1) Les fonctions principales, auxiliaires et superflues supportées par l'appareil | O | | O | | O | |
| | 2) Lorsque ceci est pertinent, les moyens pour garantir que les fonctions principales sont protégées contre toutes actions intentionnelles ou non intentionnelles de la part des fonctions auxiliaires ou superflues. | O | | O | | R | |
| | 3) Les fonctions d'auto-surveillance offertes et les actions lancées sur détection des défaillances. | O | | O | | R | |
| | 4) Les interfaces internes entre les modules de l'appareil. | O | | R | | - | |
| | 5) Les interfaces externes de l'appareil. | O | | O | | O | |
| | 6) Les rôles, types, formats, gammes et limitations relatifs aux entrées, aux sortie, aux signaux d'exception, aux paramètres et aux données de configuration, lorsque pertinent. | O | | O | | O | |
| | 7) Les différents modes de fonctionnement et les conditions de transition correspondantes. | O | | O | | O | |
| | 8) Toutes les contraintes à respecter lors de l'utilisation de l'appareil. | O | | O | | O | |
| | 9) Les temps de réponse, la bande passante et les autres paramètres dynamiques nécessaires pour complètement comprendre les fonctions de l'appareil et ses limitations. | O | EC | O | EC | O | EC |
| | 10) Les limitations liées à l'environnement (voir 6.6) | O | EC | O | EC | O | EC |
| | 11) Lorsque cela est pertinent, les mesures de sécurité pour protéger les valeurs initialisées de modifications accidentelles ou malveillantes. | O | AD | O | AD | O | AD |
| d | Documentation portant sur les principes de fonctionnement:<br>La documentation décrit la théorie sous jacente aux principes de fonctionnement de l'appareil et à la conception de l'appareil et au fonctionnement d'ensemble du matériel, du logiciel et des HPD avec suffisamment de détails pour qu'on puisse évaluer l'efficacité de la vérification et de la validation de l'appareil. | O | AD | O | AD | O | AD |
| e | Documentation matériel:<br>La documentation matériel décrit la structure d'ensemble du matériel, les fonctions de chaque composant matériel et leurs propriétés (y compris les propriétés de robustesse – voir 6.6) qui sont utilisées en conception, en interaction avec le logiciel ou les HPD, avec le niveau de détail nécessaire pour pouvoir sous réserve des compétences nécessaires modifier le matériel pour faire face au remplacement d'un composant qui n'est pas complètement identique à l'original. | O | AD | O | AD | O | AD |

| | Informations à tenir à disposition ou critère à satisfaire | Classe 1 | | Classe 2 | | Classe 3 | |
|---|---|---|---|---|---|---|---|
| | | | MC | | MC | | MC |
| f | Description logiciel et des HPD<br>Cette documentation décrit la structure d'ensemble des fonctions logiques mises en œuvre par le logiciel ou les HPD. Leur décomposition au niveau modulaire sont suffisantes pour fournir la connaissance et les détails nécessaires concernant les interactions entre le matériel conventionnel, le logiciel et les HPD pour réaliser des modifications ou la maintenance. | O | AD | O | AD | R | AD |
| g | Enregistrements relatifs à la vérification et aux essais pour chaque phase de la conception. Pour le logiciel et les HPD, cela comprend les essais unitaires (pour la classe 1), les essais d'intégration et les essais de validation. | O | EC | O | EC | R | EC |
| h | Information d'identification des versions qui peuvent être authentifiées durant l'installation sur site | O | | O | | O | |
| i | Documentation utilisateur de sûreté telle que décrite en 6.9. | O | AD | O | AD | O | AD |
| j | Historique des modifications – un rapport ou un rapport extrait du système de gestion de configuration qui identifie l'historique des révisions du produit tel que requis par 7.4.4 | O | | O | | R | |

## 7.5 Preuves de la qualité de la fabrication

L'assurance qualité en fabrication est importante car elle fournit la base sur laquelle sont acceptés les appareils du même modèle ou d'un modèle similaire qui peuvent être fabriqués ultérieurement, même si des facteurs tels que la disponibilité de composants identiques peuvent avoir un impact sur l'appareil.

Le tableau ci-dessous définit les exigences applicables aux preuves de la qualité de la fabrication en ce qui concerne les informations à tenir à disposition et les critères devant être satisfaits. Les exigences doivent être appliquées en remplaçant "___" par «doit» lorsque l'indication «O» apparaît et l'exigence doit être reformulée avec «Il est recommandé» ou «Il convient» lorsque l'indication «R» apparait, en conformité avec le tableau ci-dessous:

| | Informations à tenir à disposition ou critère à satisfaire | Classe 1 | | Classe 2 | | Classe 3 | |
|---|---|---|---|---|---|---|---|
| | | | MC | | MC | | MC |
| a | Les preuves ___ être documentés pour que le fournisseur puisse maintenir un programme d'AQ de fabrication similaire à celui de l'ISO 9001. | O | | O | | O | REX SP |
| b | Les preuves de conformité au programme d'AQ de fabrication ____ documentées. | O | | O | | R | |
| c | Les preuves ___ fournir les détails montrant que le fabricant maintient un programme de qualification fournisseur qui couvre:<br>– La réalisation d'inspections externes,<br>– La réalisation de la première inspection et/ou des essais,<br>– La réalisation du contrôle des modifications et des substitutions de composants, et<br>– La préparation de rapports sur les modifications et les substitutions par rapport à la conception. | O | | O | | R | REX |
| d | Les preuves ___ fournir les détails montrant que le fabricant réalise les essais opérationnels adaptés ainsi que ceux de vieillissement pour l'appareil.<br>NOTE "EC" fait dans ce cas référence à des essais de vieillissement réalisés par l'utilisateur final. | R | EC | R | EC | R | EC |
| e | Les preuves ___ fournir les détails concernant les versions et les numéros de série des matériels d'essai utilisés pour les essais fonctionnels, et ceux montrant que les matériels de calibration satisfont aux normes d'étalonnage adaptées. | O | EC | O | EC | R | EC |

| | Informations à tenir à disposition ou critère à satisfaire | Classe 1 | | Classe 2 | | Classe 3 | |
|---|---|---|---|---|---|---|---|
| | | | MC | | MC | | MC |
| f | Les preuves ___ fournir les détails montrant que des mécanismes sont en place pour garantir que seules des configurations logiciel et de HPD connues et vérifiées sont installées sur l'appareil en fabrication. | O | | O | | O | |
| g | Les preuves ___ fournir les détails montrant que le fabricant maintient les enregistrements concernant les dates de fabrication, l'information relative aux versions et aux numéros de série des appareils dès qu'ils sont fabriqués. | O | | O | | R | |
| h | Les preuves ___ fournir les détails montrant que le fabricant appose sur toute unité livrée l'identité complète de la version ou de la mise à disposition associée à cette unité (ceci peut être une étiquette lisible à l'œil nu ou un paramètre interne lisible électroniquement). | O | | O | | O | |
| i | Les preuves ___ fournir les détails montrant que le fabricant facilite la collecte du retour d'expérience sur le terrain concernant l'appareil, et recueille et enregistre systématiquement les rapports d'incident relatif à la conception de l'appareil, et fait un rapport au concepteur de l'appareil.<br>NOTE La présente norme ne peut pas établir d'exigences concernant les mécanismes relatifs aux rapports de retour d'expérience portant sur des problèmes rencontrés sur le terrain pour le cas où un utilisateur final rapporterait un problème au distributeur, au fabricant ou au concepteur de l'appareil. L'essentiel est qu'il soit fourni à l'utilisateur final un point de contact permettant d'établir la communication avec les intervenants les plus à même de traiter le problème décrit. | O | | O | | R | |
| j | L'impact de la stabilité du processus de fabrication ___ être pris en compte. | O | REX<br>SP<br>EC | O | REX<br>SP<br>EC | R | REX<br>SP<br>EC |

### 7.6 Stabilité du produit

Le critère présenté dans ce paragraphe permet d'examiner les preuves associées à la maturité du produit et à la probabilité que le produit ne sera pas modifié et que le fournisseur sera capable d'apporter son support durant la durée de vie pendant laquelle il sera installé dans la centrale nucléaire. Il est aussi une mesure de la pertinence avec laquelle l'analyse est utilisée au niveau du contrôle des modifications et de l'application pleinement rigoureuse du processus de conception aux modifications, y compris des essais de non-régression. La stabilité du produit est étroitement liée au retour d'expérience, et comme le retour d'expérience est un des facteurs d'évaluation sur lequel on se repose, la stabilité du produit est essentielle.

a) La stabilité du produit doit être évaluée par rapport au volume de modifications portant sur la fonction principale, par rapport au volume de modifications qui ont un impact potentiel sur la fonction principale, par rapport au volume de modifications qui ont un impact sur les autres fonctions, par rapport à l'impact de toutes les modifications sur la fonction principale et par rapport aux raisons ayant entraîné ces modifications (telles que les corrections d'erreurs logiciel, la substitution de composants obsolètes, des modifications réglementaires, etc.).

   NOTE Une fréquence peu élevée de modifications correctives durant une période de temps significative peut indiquer un degré de stabilité et de correction et/ou une bonne conception du produit.

b) L'évaluation par rapport au point a) doit reposer sur les rapports de maintenance qui s'appuient sur les outils de gestion de configurations et de contrôle des modifications et les procédures qui doivent satisfaire aux exigences des 7.4.4, 7.4.5 et 7.5.

c) La stabilité du produit doit être évaluée en prenant en compte le nombre d'installations et d'application, et doit être prise en compte seulement si l'échelle à laquelle le produit a été fabriqué et utilisé est significative.

d) Lorsqu' on applique la stabilité du produit, celle-ci doit être utiliser pour compenser des faiblesses ou des carences de preuves au niveaux des critères établis en 7.3, 7.4 et 7.5, lorsque les paragraphes pertinents permettent de l'utiliser, ou lorsque elle vient en appui de la mesure compensatoire portant sur le retour d'expérience.

### 7.7 Retour d'expérience

Le critère présenté dans ce paragraphe permet d'examiner les preuves associées à la robustesse du produit face aux environnements d'exploitation et à des profils opérationnels comparables, et posant au moins autant de problèmes que ceux prévus pour l'application. De telles preuves sont importantes car elles représentent la mise à l'épreuve de l'appareil avec de réels profils d'exploitation qui complète les essais réaliser sur l'appareil candidat en allant au-delà du nombre limité de cas d'essais avec lequel on peut faire des tests au cours du développement.

a) Toutes les preuves concernant le retour d'expérience soumises pour être prises en compte doivent pouvoir faire l'objet d'audit.

b) L'identité de l'organisation ou des organisations à l'origine du rapport doit être documentée.

c) Les preuves concernant le retour d'expérience doivent être précisément documentées pour connaître précisément les versions de logiciel et des HPD.

d) Les preuves concernant le retour d'expérience doivent être précisément documentées pour connaître précisément les valeurs d'initialisation du matériel, du logiciel et de HPD.

e) Si le retour d'expérience qui correspond à des versions différentes doit être pris en compte au niveau du logiciel, des HPD ou du matériel, on doit fournir les justifications qui permettent l'analyse des différences entre ces versions, et ces analyses doivent être utilisées pour déterminer à quel point le retour d'expérience associé à chaque version de l'appareil peut être pris en compte.

Des essais complémentaires peuvent être utiles pour permettre la prise en compte du retour d'expérience associé à des versions antérieures de logiciel ou des HPD.

f) L'analyse des preuves associées au retour d'expérience doit considérer si les fonctions particulières de l'appareil candidat fonctionnent en continu ou de façon intermittente sur demande. Dans le premier cas, les preuves doivent reposer sur le nombre réel d'heures de fonctionnement, dans l'autre cas, les preuves doivent reposer sur le nombre d'exécutions de la fonction (y compris les essais de surveillance) sans défaillance pour les fonctions à la demande.

g) Tous les aspects relatifs aux fonctions de l'appareil candidat prévus pour l'application doivent être couverts par le retour d'expérience.

h) La couverture et le volume du retour d'expérience doit être suffisant pour acquérir un niveau de confiance suffisant dans l'appareil candidat par rapport à la classe de l'application prévue.

i) La couverture et le volume du retour d'expérience doit être suffisant pour acquérir un niveau de confiance suffisant dans l'appareil candidat en prenant en compte son niveau de complexité, et en considérant ensemble le logiciel, les HPD et le reste du matériel.

j) Si le retour d'expérience est un des critères principaux et prépondérant au niveau de la preuve de la précision et de l'exactitude, le volume et l'étendue du retour d'expérience est crucial. Alors le volume et l'origine des données de retour d'expérience exigées doivent être justifiés.

   Il convient de déterminer la durée en exploitation qui sera jugée suffisante au cas par cas en utilisant le jugement de l'ingénieur. Il convient que ce jugement prenne en particulier en compte le niveau de fiabilité prévu au niveau du système pour les fonctions pour lesquelles l'appareil est utilisé.

   Pour les applications prévues de classe 1, il convient que le retour d'expérience repose sur plusieurs applications provenant des rapports de plusieurs organisations.

Il n'est pas exigé que le retour d'expérience provienne d'une installation nucléaire. L'objectif de cette exigence est que la couverture et le volume du retour d'expérience soit soigneusement documentés (ce qui peut ne pas être le cas dans des environnements industriels) et pertinents par rapport au profil opérationnel qui sera rencontré par l'appareil candidat utilisé dans le cadre de l'application prévue (voir le point k) ci après).

NOTE L'Annexe D de la CEI 61508-7 fournit des informations relatives au volume de retour d'expérience pour ce qui concerne le critère de fiabilité.

k) Le retour d'expérience pris en compte doit comprendre les conditions de fonctionnement qui ont autant éprouvé l'appareil candidat que le fera l'application prévue. Ces conditions doivent couvrir lorsque cela est pertinent les points suivants:

- états du procédé (par exemple, température, pression, viscosité, particules présentes, etc.) pour les appareils fluide tels que des vannes ou des capteurs (voir 6.6),
- environnement de fonctionnement du matériel (par exemple, température, humidité, vibrations, IEM, rayonnements, etc.) (voir 6.6),
- profil opérationnel ou méthode d'utilisation (tel que la vitesse des transitoires comme le démarrage d'un compresseur ou les harmoniques vues par un onduleur alimenté par un générateur à la place du réseau), si cela peut d'une façon ou d'une autre avoir un impact sur le fonctionnement de l'appareil candidat en termes de charge pour le logiciel,
- interfaces avec les autres appareils.

l) Les preuves démontrant qu'un système fiable de comptes-rendus des défaillances a été mis en place et est en service, afin que le retour d'expérience puisse être estimé avec un degré de confiance élevé, doivent être documentées. Si toutes les défaillances ou tous les fonctionnements dégradés peuvent ne pas avoir fait l'objet de comptes-rendus, alors l'importance accordée à l'estimation du retour d'expérience doit être réduite pour refléter l'incertitude entachant la précision du système de comptes-rendus des défaillances.

   Par exemple, lorsqu'il n'y a pas de preuves fiables que toutes les défaillances ont fait l'objet de compte-rendu, le nombre d'heures de fonctionnement peut être réduit de 30 % pour les périodes de garantie et de 50 % au-delà.

m) Si le retour d'expérience indique l'apparition de défaillances aléatoires liées au matériel dépassant le taux de défaillances prévu, alors on doit prendre en compte le fait qu'un défaut systématique peut exister au niveau de l'appareil, tel qu'un défaut dans la conception du logiciel ou des HPD, une faiblesse au niveau des sous composants liée à l'environnement, etc.

n) Lorsque on applique le retour d'expérience, celle-ci doit être utilisée pour compenser des faiblesses ou des carences de preuves au niveaux des critères établis en 7.3, 7.4 et 7.5, lorsque les paragraphes pertinents permettent de l'utiliser.

### 7.8 Essais et/ou analyses complémentaires (vérification)

Des essais complémentaires peuvent être réalisés pour différentes raisons. Celles-ci peuvent comprendre la confirmation de la pertinence d'anciennes de versions de l'appareil pour qu'elles soient considérées dans le retour d'expérience, la confirmation de modifications de l'appareil, la couverture de manques au niveau des essais de validation, la compensation de certaines carences au niveau du retour d'expérience, ou la confirmation de l'exactitude et de la précision ou encore de la robustesse en présence des conditions opérationnelles.

Des essais complémentaires peuvent être aussi utilisés pour compenser des écarts ou des manques au niveau du processus de conception (ou au niveau de la connaissance de celui-ci), de la documentation de conception (en particulier pour les omissions dans les exigences fonctionnelles et les essais de validation), de la documentation traitant des réponses apportées pour les états des entrées particuliers (tels que des anomalies en entrée), et pour le manque de retour d'expérience, en identifiant en détail la réponse à des entrées spécifiques, en testant la robustesse de l'appareil par rapport à des contraintes particulières.

Les types d'essais suivants qui peuvent être réalisés sont des exemples:

- tests d'insertion de défauts pour confirmer que les fonctions d'auto-supervision détectent chaque défaut et mettent les sorties de l'appareil en position de repli sûre,
- tests particuliers pour confirmer les performances des fonctions qui sont faiblement sollicitées (par exemple celles qui attendent qu'un évènement particulier soit détecté, en opposition aux fonctions qui fonctionnent en continu) pour lesquelles le retour d'expérience est par définition difficile à accumuler,
- tests particuliers pour confirmer les différentes facettes du comportement fonctionnel de l'appareil qui ont fait l'objet d'une documentation ambigüe ou incomplète,
- tests particuliers liés à une modification pour confirmer qu'il est acceptable de prendre en compte une ancienne version dans le retour d'expérience,
- tests particuliers pour déterminer le temps de réponse de l'appareil pour des sorties hors-gamme ou invalides (telles que mettre moins de 4 mA sur une entrée de 4 mA à 20 mA, ou faire dériver de façon décroissante l'alimentation électrique d'une entrée analogique ou d'une boucle d'instrumentation) et déterminer si la réponse de l'appareil est acceptable compte tenu de l'application cible,
- tests statistiques aléatoires dans le domaine de validité, tels que décrits dans l'Annexe D de la CEI 61508-7. Noter qu'il peut être assez difficile de remplir les conditions pré-requises de réalisation de tels tests,
- tests complémentaires pour confirmer que pour une ou des configurations et dans des conditions prévues d'utilisation, l'appareil satisfait à ses exigences fonctionnelles et de performances,
- tests particuliers pour confirmer que la fonction principale n'est pas perturbée par les fonctions auxiliaires et les fonctions superflues,
- tests particuliers pour confirmer l'efficacité des mécanismes de sûreté et de sécurité.

NOTE La référence de la position de repli sûre repose sur les exigences du point e) de 6.2.

Si des essais complémentaires sont utilisés dans le cadre de l'évaluation de l'appareil candidat, les exigences suivantes sont applicables et doivent être documentées et disponibles pour des revues:

a) La documentation relative aux essais doit faire apparaître l'identification précise de la version du produit testé.

b) Les fonctions testées doivent être documentées (ceci doit couvrir les procédures d'essai, les données d'essai, et les résultats d'essai attendus et observés).

c) Les essais doivent être conçus par rapport à l'application prévue pour démontrer que le comportement de l'appareil est consistant par rapport aux exigences portant sur l'application, ceci couvrant les conditions marginales et exceptionnelles.

d) Les résultats d'essai doivent faire l'objet de revues par rapport à l'application prévue pour démontrer que le comportement de l'appareil est consistant par rapport aux exigences portant sur l'application.

e) Les essais relatifs à l'environnement doivent être représentatifs pour l'application prévue, ou les raisons pour lesquelles les écarts sont acceptables doivent être documentées.

f) Pour une application prévue de classe 1 ou de classe 2, la base sur laquelle repose les essais doit être documentée pour expliquer pourquoi les résultats des tests vont démontrer la satisfaction des exigences (ceci peut par exemple comprendre une analyse ou une modélisation des caractéristiques de conception du logiciel, du matériel ou des HPD, objets des essais).

g) L'identité de l'organisation réalisant les essais doit être enregistrée dans la documentation.

h) Lorsque on utilise des analyses ou des essais complémentaires, ceci doit être utilisé pour compenser des faiblesses ou des carences de preuves au niveaux des critères établis en 7.3, 7.4 et 7.5, lorsque les paragraphes pertinents permettent de l'utiliser.

### 7.9 Amélioration de la documentation

Dans de nombreux cas, il est possible de compenser des faiblesses apparaissant au niveau de la documentation disponible fourni par le concepteur ou le fabricant en améliorant le corpus documentaire au cours du processus d'évaluation ou conformément au REA.

Un des types d'amélioration de la documentation est souvent nommé «reconstitution de documentation». Il repose habituellement sur l'utilisation d'essais complémentaires pour réaliser une sorte de «reverse-engineering» visant à apporter des éclaircissements au niveau de la spécification de conception et des procédures d'essais de validation. Lors de la reconstitution de documentation, le produit final n'est modifié en aucune façon; un projet de spécification boîte noire du produit est préparé à base de toutes les informations disponibles, y compris l'appui des concepteurs. On développe, à partir de ce projet de spécification une procédure d'essai et on la déroule. Les différences observées entre les résultats attendus d'essai et les résultats d'essai sont utilisées pour modifier le projet de spécification du produit et la spécification d'essai. Tout le processus est répété itérativement jusqu'à ce que la confirmation de la justesse et de l'exactitude de la spécification produite soient confirmées par des essais couronnés de succès.

Si on a recours à la l'amélioration de la documentation en tant que mesure compensatoire alors les exigences suivantes doivent être appliquées:

a) Il doit y avoir une base solide pré existante pour réaliser les améliorations de la documentation; celles-ci correspond soit à une description fonctionnelle complète ou bien à une description du logiciel et du matériel, ainsi qu'à une description des principes de fonctionnement.

NOTE 1 L'objectif est d'élaborer à partir de la documentation préparée par le concepteur, et non pas de créer une documentation en partant de rien. Ceci du fait que l'existence de carences majeures au niveau de la documentation cohérente qui explique le fonctionnement de l'appareil est une indication de faiblesse de l'approche des concepteurs qui remet en cause la conception elle-même.

b) Toutes les améliorations de la documentation qui décrit les fonctionnalités de conception doivent être revues par le concepteur de l'appareil candidat.

NOTE 2 L'objectif est de garantir l'exactitude et la justesse technique des éléments concernant les zones critiques de la conception du produit, qui sont les garanties de la protection de la fonction principale par rapport aux fonctions auxiliaires ou superflues pour tous les profils de sollicitation.

c) Lorsqu'on applique la mesure compensatoire d'essais complémentaires dans le cadre de la reconstitution de la documentation, ces essais doivent être réalisés conformément à 7.8.

d) Lorsqu'on applique l'amélioration de la documentation en tant que mesure compensatoire, celle-ci doit être utilisée pour compenser des descriptions insuffisantes au niveaux des critères particuliers établis en 7.3, 7.4 et 7.5, lorsque les paragraphes pertinents permettent de l'utiliser.

## 8 Critères portant sur l'intégration dans l'application – limites et conditions d'utilisation

### 8.1 Généralités

Cet article traite des limites et des conditions qui peuvent potentiellement restreindre l'utilisation de l'appareil. Ces conditions et ces limites peuvent provenir des résultats de l'évaluation de l'aptitude de l'appareil, ou peuvent être imposées pour pouvoir partiellement qualifier l'appareil afin qu'il soit utilisé suivant des conditions et des limitations. Le REA (voir 5.3.3) et la documentation utilisateur de sûreté (voir 6.9) associés à l'appareil doivent donner les détails concernant toutes les limitations.

### 8.2 Restrictions d'utilisation

Un appareil candidat peut être déclaré qualifié pour un usage défini dans le cadre de certaines applications si cet usage respecte certaines limitations et conditions.

Les éléments suivants doivent apparaître dans le REA:

- la plus haute classe de sûreté pour laquelle l'appareil candidat est qualifié pour être utilisé,
- lorsque cela est applicable, les applications particulières pour lequel l'appareil candidat est qualifié pour être utilisé,
- les limites de fiabilité qui peuvent être atteintes avec l'appareil, en configuration isolée ou redondante,
- les options particulières ou les fonctions secondaires qui doivent être actives ou inhibées, y compris les paramètres d'initialisations particuliers pour chaque classe de sûreté,
- les limites associées à l'environnement d'exploitation (tel que défini en 6.6) pour lequel l'appareil candidat est qualifié,
- les facteurs limitant impactant la durée de vie opérationnelle (comme l'utilisation de capacité aluminium),
- toutes mesures particulières à respecter durant l'exploitation ou les essais de façon à garantir une utilisation sûre de l'appareil.

### 8.3 Modifications de l'appareil nécessaires pour son utilisation dans le cadre de l'application

Un appareil candidat peut être déclaré qualifié pour certaines applications si certaines modifications du matériel ou si certaines modifications très mineures du logiciel de l'appareil sont réalisées avant utilisation. Ceci peut être parfois nécessaire, par exemple, dans des applications de rénovation où l'adaptation des volumes est un problème ou un niveau d'impédance peut être exigé. Mais il est essentiel que de telles modifications n'aient pas pour résultat la création d'un nouveau produit car dans ce cas la présente norme ne pourrait plus s'appliquer.

Par exemple, certains appareils candidats potentiels peuvent présenter des fonctions secondaires telles que HART, qui est mis en œuvre en rajoutant des signaux hautes fréquences sur le signal procédé 4 mA à 20 mA. Il peut être nécessaire d'inhiber cette option ou d'utiliser des filtres passe-bas pour que les hautes fréquences n'aient pas d'effets sur les autres appareils du système cible.

Lorsqu'il est nécessaire de modifier l'appareil, et ceci de quelque façon que ce soit, les exigences suivantes s'appliquent:

a) Le REA doit:
   - identifier les modifications requises, et
   - vérifier le niveau d'appui qui peut être fourni par le concepteur de l'appareil pour ces modifications.

b) Toutes les modifications portant sur la conception de l'appareil doivent être telles qu'elles ne rendent pas caduque le retour d'expérience pris en compte pour l'évaluation. Les modifications ne doivent pas modifier conceptuellement la fonction principale de l'appareil candidat.

c) Toutes les modifications doivent se faire sur une petite échelle, elles doivent avoir une étendue limitée et elles doivent être simples à vérifier et à valider.

d) Toutes les modifications doivent être réalisées conformément à toutes les exigences établies par 7.4, et de façon consistante avec la classe de l'application prévue.

e) Le REA doit être révisé pour prendre en compte les modifications et cette révision doit considérer tous les facteurs qui peuvent avoir un impact sur les conclusions du rapport.

### 8.4 Modifications du système pour s'adapter à l'appareil

Un appareil candidat peut avoir été jugé qualifié pour une utilisation pour certaines applications si certaines modifications ont été réalisées auparavant sur le système. Ce

paragraphe est plus particulièrement applicable aux opérations de rénovation pour lesquelles par exemple l'introduction d'un relai peut être nécessaire au niveau des interfaces entre l'appareil candidat et d'autres composants du système.

Dans de tels cas, on doit considérer les questions suivantes et documenter les évaluations réalisées pour l'appareil candidat:

a) Le REA doit couvrir les modifications possibles apportées à la conception du système qui peuvent être nécessaires, y compris:
   - les équipements supplémentaires pour la surveillance des défaillances,
   - les redondances ou diversités supplémentaires nécessaires,
   - les besoins de validation inter-canaux par comparaisons,
   - la réallocation des fonctions dans différents sous système,
   - les modifications dues à la protection contre les conditions environnementales telles que des blindages, de la ventilation, du refroidissement, etc.
   - les modifications ayant un impact sur la maintenance et/ou sur les pratiques d'exploitation.

b) Le REA doit couvrir les exigences de formation sur le système découlant de l'utilisation de l'appareil candidat.

c) Le REA doit être révisé par rapport aux modifications réalisées et cette révision doit prendre en compte tous les facteurs qui pourraient avoir un impact sur ses conclusions.

### 8.5 Intégration et mise en service de l'appareil dans les systèmes de sûreté de la tranche

Un appareil candidat qualifié pour être utilisé dans une application donnée sera au final mis en service et intégré dans le système de sûreté d'une nouvelle construction ou dans celui d'une tranche en rénovation.

Il convient de distinguer deux situations:

- Les applications pour lesquelles l'appareil nouvellement qualifié est utilisé de façon isolée; par exemple d'une façon qui ne présente pas le risque d'entraîner une défaillance totale de la fonction de sûreté de la centrale, et
- Les applications pour lesquelles l'appareil nouvellement qualifié est utilisé dans les canaux d'un système ou en un point de passage unique critique tel qu'on ait le risque que cet appareil puisse entraîner la défaillance totale de la fonction de sûreté de la tranche, telle qu'un appareil de protection d'une alimentation électrique d'un système de sûreté.

Tenant compte du REA, le plan de mise en service et d'intégration doit être préparé et il doit:

a) Comprendre les exigences pertinentes de l'Article 6 de la CEI 61513.

b) Comprendre les recommandations et les limitations pour lesquelles les détails sont fournis dans le REA et dans les instructions de mise en service du fournisseur.

c) Pour le second cas précédent, ou bien s'il reste certains aspects des fonctionnalités de l'appareil à valider, le plan de mise en service et d'intégration doit aussi:
   1) considérer une introduction prudente graduelle de l'appareil candidat dans le système, considérant la possibilité d'une période initiale de validation pendant laquelle l'appareil candidat est mis en service dans un seul canal ou train du système redondant, pour permettre une évaluation de l'appareil en exploitation sur le système cible réel;
   2) définir les moyens adaptés pour garantir et vérifier l'initialisation correcte des paramètres dans tous les appareils mis en œuvre dans le système, y compris ceux spécifiés dans le REA;
   3) spécifier les cas d'essai de mise en service prenant en compte les aspects dynamiques propres aux systèmes de sûreté (transitoires), pour lesquels:

- il convient que la sélection des scénarii d'essai particuliers soient basés sur des modèles et des simulations système;
- ces essais doivent prendre en compte le temps de réponse de l'appareil et les séquences et les priorités associées aux actions de protection; et
- pour les appareils utilisés pour des systèmes de protection des alimentations électriques, il convient que les cas test couvrent complètement les séquences de démarrage des systèmes, et il convient de réaliser des stress tests des systèmes de sûreté sélectionnés.

4) exiger l'enregistrement des éléments suivants durant la mise en service:

- tous les écarts constatés au niveau des fonctions de l'appareil par rapport aux données fournies par le REA. Les petits écarts ne doivent pas être négligés car ils peuvent indiquer la présence de déficiences sérieuses au niveau de la conception du logiciel ou des HPD de l'appareil.
- les valeurs d'initialisation des paramètres dans l'appareil,
- tous les résultats d'essai, et ceci jusqu'à l'intégration finale dans l'appareil.

# 9 Considérations pour maintenir le caractère acceptable de l'appareil

## 9.1 Généralités

Lors de son évaluation, l'appareil peut apparaître comme idéal pour ce qui est de son aptitude fonctionnelle et des preuves portant sur la précision et l'exactitude qui l'accompagnent, mais il convient de prendre aussi en compte la durée de vie de l'appareil et le support à long terme qui peut être apporté par le fournisseur. Ce sont des facteurs d'importance du fait de la longueur de la durée de vie en service des centrales nucléaires.

Cet article identifie les critères nécessaires pour évaluer l'appareil candidat de ce point de vue particulier, et spécialement pour la maintenance du logiciel et des HPD.

## 9.2 Notifications faites par le concepteur et le fabricant

Des mesures adaptées doivent être mises en place pour garantir que l'utilisateur sera formellement averti de toute modification de l'appareil qualifié. Si une modification matériel, logiciel ou des HPD est réalisée, une analyse d'impact doit être faite et l'appareil doit être requalifié conformément à la présente norme.

Il convient d'évaluer l'appareil candidat par rapport aux notifications portant sur des défaillances faites par le fabricant ou par le concepteur qui sont survenues suite à la période d'évaluation du retour d'expérience et depuis que l'appareil peut être en service. Les leçons apprises des défaillances survenues sur d'autres installations peuvent être utilisées pour lancer des actions de maintenance préventives ou des remplacements d'appareils.

Il convient que l'évaluation prenne en compte les facteurs suivants et que le compte-rendu soit fait des tentatives d'obtenir un accord avec le fabricant ou le concepteur pour:

- fournir en temps utile les notifications pour chacune des défaillances survenues sur d'autres installations,
- ajouter à chaque notification les analyses qui pourraient aider à déterminer si un défaut pourrait avoir un impact sur la fonction principale ou limiter son immunité par rapport aux défaillances des fonctions auxiliaires ou superflues,
- mettre à disposition la liste de défauts courants qui identifie les effets potentiels qui ont fait l'objet de comptes-rendus de défaillance, l'état de résolution courant de chaque défaut, et l'identification précise versions touchées,
- fournir une notification pour chaque modification, que ce soit pour une substitution de composant matériel, une modification du processus de fabrication ou une modification du logiciel ou des HPD.

### 9.3 Fabrication et support technique pour la durée de vie de la version courante

Il convient d'évaluer l'appareil candidat par rapport à la durée de vie prévue du support produit pour l'appareil candidat, comme par rapport à la durée de vie de l'appareil lui-même. Dans le premier cas, des durées de support technique plus longues sont souhaitables et il est possible de les négocier. Dans le second cas, la connaissance de cette donnée sert pour établir le plan de remplacement de l'appareil avant d'atteindre la fin de la durée de vie en service de l'appareil.

Il convient que l'évaluation prenne en compte les facteurs suivants et que ceux-ci apparaissent dans le REA:

- engagement de durée pour la fabrication de la version courante du produit et de l'appareil en général,
- durée de vie en service de la version courante et de l'appareil en général,
- volonté du fabricant ou du concepteur d'avertir à l'avance du retrait de la version courante et de l'appareil en général,
- volonté du fabricant de prendre l'engagement de fournir dans le futur des appareils de remplacement compatibles par branchement,
- volonté du fabricant de prendre l'engagement de fournir dans le futur des appareils de remplacement fonctionnellement compatibles,
- impact des modifications client requises par l'application.

### 9.4 Préservation des outils de maintenance et de la documentation

La durée de vie des centrales nucléaires de puissance est bien trop longue pour les systèmes numériques, aussi il convient de prendre en compte le phénomène d'obsolescence lors de l'évaluation de l'appareil. Il convient que l'évaluation prenne en compte la volonté ou non du concepteur de l'appareil de prendre un engagement contractuel (par exemple un accord de mise en dépôt légal) ou bien de donner l'assurance que les éléments suivants seront disponibles si le concepteur ou si le fabricant décide d'interrompre le support technique de l'appareil candidat:

- copies d'installation des outils de configuration tels que les éditeurs et les compilateurs,
- copie de l'environnement de fonctionnement de ces outils (par exemple une version particulière d'Unix ou de Windows),
- copies de tous les fichiers source, les fichiers d'édition de liens, des librairies, etc., fournis à partir du système de gestion des configurations,
- outils matériel particuliers (par exemple claqueurs de PROM, analyseurs logiques),
- plans et dessins de fabrication,
- copies de toute la documentation (spécifications, rapports d'essais, etc.); et
- description détaillée du matériel informatique et des composants nécessaires pour utiliser le système d'exploitation, outils logiciel et outil matériel, ou bien l'élément réel.

### 9.5 Recommandations à destination de l'utilisateur final

La réalisation des actions suivantes est recommandée pour pouvoir assurer un support technique à long terme de l'appareil candidat, celles-ci sont à réaliser par l'organisation exploitante de la centrale nucléaire de puissance en dehors de l'évaluation de l'appareil candidat:

- maintenir le système de gestion des configurations indépendamment du fournisseur pour gérer:
  - toutes les modifications des paramètres de configuration,
  - toutes les modifications initiales telles que documentées dans le REA,

  - toutes les versions reçues du fournisseur et leurs statuts d'installation et de configuration,
- maintenir le système de contrôle des modifications avec des analyses d'impact pertinentes,
- réaliser des essais de validation après chaque changement de configuration (même pour des changements de paramètres),
- maintenir des copies des outils de configuration tels que les éditeurs et les compilateurs,
- si l'appareil est utilisé dans des applications de différentes classes de sûreté, maintenir toutes les activités adaptées à la plus haute classe de sûreté.

# Annexe A
(informative)

## Caractéristiques de conception d'un système programmé qui peuvent avoir un impact sur la sûreté de fonctionnement de l'appareil

Cette annexe a pour objectif de donner des pistes concernant des recommandations pour vérifier les conclusions tirées de l'évaluation des propriétés de conception qui ont pour but l'évitement des défauts systématiques (7.3).

Ces informations sont plus particulièrement destinées aux applications de classe 1 et de classe 2, mais elles peuvent aussi être utilisées pour des applications de classe 3. Il convient de noter que pour le logiciel, l'assurance concernant l'évitement des défauts systématiques peut principalement être obtenue sur la base d'analyses. Au contraire, pour ce qui concerne les conditions environnementales qui peuvent aussi être à l'origine de défauts systématiques, la qualification peut utiliser des analyses ou bien des essais conformément aux prescriptions de la CEI 60780 comme indiqué en 6.6.

Comme décrit en 7.3, l'évaluation de la robustesse de la conception en ce qui concerne l'évitement des défauts systématiques débute par l'examen de la conception d'ensemble du système. Ceci peut dans le cas du logiciel amener à s'interroger sur les mécanismes potentiels de la conception qui sont bien connus pour être des sources de problèmes potentiels. La liste ci-dessous n'est pas à considérer comme exhaustive, mais peut servir de point de départ.

a) La sensibilité au profil de demande peut avoir un effet sur la charge du CPU, l'ordre de traitement des interruptions, etc. Les exemples suivants de contributeurs potentiels aux défaillances de l'appareil peuvent être pertinents:

   - interaction entre plusieurs entrées,
   - comportement des signaux dû aux IME (par exemple salves courte hors gamme),
   - surcharge due à une avalanche d'évènements détectés en entrée,
   - dépassement des pires considérations de temps.

   NOTE La CEI 60880 qui s'applique aux systèmes de classe 1 impose que le comportement au niveau logiciel soit déterministe, et la CEI 62138 (qui s'applique aux systèmes de classe 2 )demande que le logiciel permette d'avoir un comportement prédictible en exécution. En pratique, la présente norme demande qu'une analyse adaptée des cas les plus pénalisants démontre que les composants électroniques réalisant la fonction principale s'exécuteront toujours en temps voulu ou répondront toujours dans le laps de temps prévu.

b) Si l'analyse de l'architecture de la conception semble indiquer une faiblesse dans l'approche fondamentale qui pourrait limiter le niveau d'assurance atteint concernant le fait que les propriétés requises pour le système sont garanties (prenant en compte le niveau d'assurance adapté à la classe de l'application), il peut être intéressant d'examiner la conception pour rechercher des caractéristiques particulières qui peuvent être significatives.

   Pour les applications prévues de classe 1, on peut se soucier:

   - des ordonnanceurs préemptifs,
   - de toutes les caractéristiques données pour les classes 2 et 3.

   Pour les applications prévues de classe 2, on peut se soucier:

   - des objets dynamiques créés en temps réel,
   - des ramasses-miettes,
   - de l'utilisation des pointeurs, sauf des plus simples (par exemple utilisation des pointeurs arithmétiques),

- de l'accès asynchrone aux ressources ou du verrouillage de celles-ci,
- des dépendances à l'heure et à la date impactant la ou les fonctions principales, et
- de toutes les caractéristiques données pour les Classes 3.

Pour les applications prévues de Classe 3, on peut se soucier:

- des surcharges des communications liées à d'autres appareils (tels qu'un nœud bavard),
- des utilisations non surveillées ou non gérées de pile ou de tas,
- des ordonnancements dépendants des entrées,
- des appels récursifs,
- de la gestion dynamique de la priorité des tâches,
- des systèmes surchargés, en termes de charge d'exécution CPU ou d'utilisation mémoire.

c) Pour des applications de classe 1, il est difficile de garantir que la fonction principale sera exécutée en temps voulu si la conception repose simplement sur l'utilisation d'interruptions, si celles-ci sont utilisées dans la conception de fonction secondaires qui peuvent avoir une influence sur la charge du système et par là même de façon indirecte sur la fonction principale.

d) En particulier pour les applications prévues de classe 1 et de classe 2, la présence de défauts systématiques est considérée comme moins probable si le logiciel a été conçu en utilisant:

- une convention de nommage;
- et en évitant les constructions de langage potentiellement dangereuses dont l'interprétation par le compilateur ou l'interpréteur peut être non standard.

e) Pour les applications prévues de classe 1 et de classe 2, il est souhaitable d'utiliser une analyse statique du code source adaptée.

f) Les mesures d'auto-surveillance, telles que la surveillance des flots de contrôle, les assertions, etc., peuvent être utiles, en particulier si celles-ci sont utilisées pour produire des alarmes ou pour qu'un appareil passe en position de repli sûre.

# Bibliographie

CEI 61508-1:2010, *Sécurité fonctionnelle des systèmes électriques/électroniques/ électroniques programmables relatifs à la sécurité – Partie 1: Exigences générales*

CEI 61508-2:2010, *Sécurité fonctionnelle des systèmes électriques/ électroniques/électroniques programmables relatifs à la sécurité – Partie 2: Exigences pour les systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité*

CEI 61508-3:2010, *Sécurité fonctionnelle des systèmes électriques/électroniques /électroniques programmables relatifs à la sécurité – Partie 3: Exigences concernant les logiciels*

CEI 61508-4:2010, *Sécurité fonctionnelle des systèmes électriques/électroniques/ électroniques programmables relatifs à la sécurité – Partie 4: Définitions et abréviations*

CEI 62003:2009, *Centrales nucléaires de puissance – Instrumentation et contrôle-commande importants pour la sûreté – Exigences relatives aux essais de compatibilité électromagnétique*

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

CEI 62645, *Centrales nucléaires de puissance – Instrumentation et contrôle-commande importants pour la sûreté – Exigences relatives à la sécurité des programmes des systèmes programmés*[6]

Glossaire de sûreté de l'AIEA terminologie employée en sûreté nucléaire et radioprotection, édition 2007

Licensing of safety critical software for nuclear reactors – Common position of seven European nuclear regulators and authorised technical support organisations, 2010 edition

_____

6 A publier

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

3, rue de Varembé
PO Box 131
CH-1211 Geneva 20
Switzerland

Tel: + 41 22 919 02 11
Fax: + 41 22 919 03 00
info@iec.ch
www.iec.ch