BS IEC 62671:2013

BSI Standards Publication

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

...making excellence a habit.™

National foreword

This British Standard is the UK implementation of IEC 62671:2013.

The UK participation in its preparation was entrusted to Technical Committee NCE/8, Reactor instrumentation.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

Published by BSI Standards Limited 2013

ISBN 978 0 580 71956 1

ICS 27.120.20

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 March 2013.

Amendments issued since publication

Amd. No.	Date	Text affected

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

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

CONTENTS

FOREWORD ... 4
INTRODUCTION ... 6
1 Scope ... 9
1.1 General ... 9
1.2 Background ... 10
1.3 Use of this standard ... 10
1.4 Framework ... 11
2 Normative references ... 12
3 Terms and definitions ... 13
4 Symbols and abbreviations ... 19
5 General requirements ... 19
5.1 General ... 19
5.2 Application of this standard ... 20
5.2.1 General ... 20
5.2.2 Applicability criteria for this standard ... 20
5.3 General requirements on the evaluation process ... 21
5.3.1 Evaluation process ... 21
5.3.2 Evaluation and Application Plan (EAP) ... 22
5.3.3 Evaluation and Application Report (EAR) ... 23
5.3.4 Application of clauses of this standard ... 24
6 Criteria for functional and performance suitability ... 25
6.1 General ... 25
6.2 Functional competence of the primary function ... 25
6.3 Ancillary functions ... 26
6.4 Configurability ... 26
6.5 Superfluous functions ... 27
6.6 Hardware robustness ... 28
6.7 Reliability, maintainability and testability ... 28
6.8 Cyber security ... 30
6.9 User documentation for safety ... 30
7 Criteria for dependability – Evidence of correctness ... 31
7.1 General ... 31
7.2 Previous certification ... 33
7.3 Avoidance of systematic faults ... 34
7.4 Evidence of quality in the design process ... 36
7.4.1 General ... 36
7.4.2 Product designer’s QA program ... 36
7.4.3 Design and development process ... 37
7.4.4 Design configuration management ... 38
7.4.5 Design change control ... 38
7.4.6 Design documentation ... 39
7.5 Evidence of quality in manufacturing ... 40
7.6 Product stability ... 41
7.7 Operating experience ... 42
7.8 Complementary testing and/or analysis (verification) ... 43

7.9 Documentation improvement 44
8 Criteria for integration into the application – limits and conditions of use 45
8.1 General 45
8.2 Restrictions on use 45
8.3 Modifications of the device required for the application 45
8.4 Modifications to the system to accommodate the device 46
8.5 Integration and commissioning of the device in the plant safety systems 46
9 Considerations for preserving acceptability 47
9.1 General 47
9.2 Notifications by the device designer and manufacturer 47
9.3 Manufacturing and support lifetime of the current version 48
9.4 Preservation of maintenance tools and documentation 48
9.5 Recommendations for the end-user 48
Annex A (informative) Possible design features of a software system that could impact the dependability of the device 50
Bibliography 52

Figure 1 – Selection and Evaluation Process 22

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.

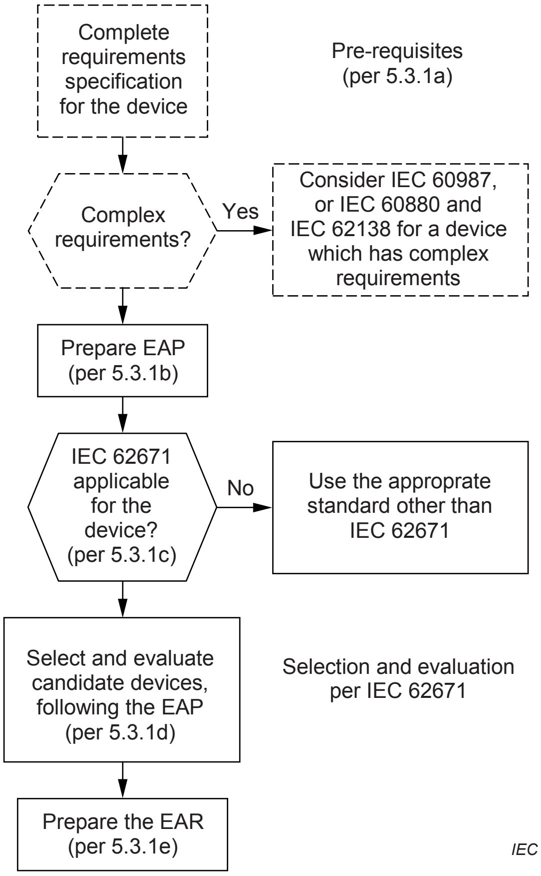
d) Each candidate device shall be evaluated according to the EAP (described in 5.3.2) and 5.3.4 to demonstrate that it complies with the requirements of this standard.

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.


Complete requirements specification for the device
Pre-requisites (per 5.3.1a)
Complex requirements?
Yes
Consider IEC 60987, or IEC 60880 and IEC 62138 for a device which has complex requirements
Prepare EAP (per 5.3.1b)
IEC 62671 applicable for the device? (per 5.3.1c)
No
Use the appropate standard other than IEC 62671
Select and evaluate candidate devices, following the EAP (per 5.3.1d)
Selection and evaluation per IEC 62671
Prepare the EAR (per 5.3.1e)

IEC 277/13

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: – objectives, – inputs and outputs, – 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. 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: – the change documentation; – the re-validation documentation; and – 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: 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. 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: 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 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 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: – performs incoming inspection, – performs first issue inspection and/or testing, – controls changes and substitutions of components, and – 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 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. 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 PS CT	M	OE PS CT	R	OE PS 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

____

This page deliberately left blank

British Standards Institution (BSI)

BSI is the national body responsible for preparing British Standards and other standards-related publications, information and services.

BSI is incorporated by Royal Charter. British Standards and other standardization products are published by BSI Standards Limited.

About us

We bring together business, industry, government, consumers, innovators and others to shape their combined experience and expertise into standards -based solutions.

The knowledge embodied in our standards has been carefully assembled in a dependable format and refined through our open consultation process. Organizations of all sizes and across all sectors choose standards to help them achieve their goals.

Information on standards

We can provide you with the knowledge that your organization needs to succeed. Find out more about British Standards by visiting our website at bsigroup.com/standards or contacting our Customer Services team or Knowledge Centre.

Buying standards

You can buy and download PDF versions of BSI publications, including British and adopted European and international standards, through our website at bsigroup.com/shop, where hard copies can also be purchased.

If you need international and foreign standards from other Standards Development Organizations, hard copies can be ordered from our Customer Services team.

Subscriptions

Our range of subscription services are designed to make using standards easier for you. For further information on our subscription products go to bsigroup.com/subscriptions.

With **British Standards Online (BSOL)** you'll have instant access to over 55,000 British and adopted European and international standards from your desktop. It's available 24/7 and is refreshed daily so you'll always be up to date.

You can keep in touch with standards developments and receive substantial discounts on the purchase price of standards, both in single copy and subscription format, by becoming a **BSI Subscribing Member**.

PLUS is an updating service exclusive to BSI Subscribing Members. You will automatically receive the latest hard copy of your standards when they're revised or replaced.

To find out more about becoming a BSI Subscribing Member and the benefits of membership, please visit bsigroup.com/shop.

With a **Multi-User Network Licence (MUNL)** you are able to host standards publications on your intranet. Licences can cover as few or as many users as you wish. With updates supplied as soon as they're available, you can be sure your documentation is current. For further information, email bsmusales@bsigroup.com.

Revisions

Our British Standards and other publications are updated by amendment or revision.

We continually improve the quality of our products and services to benefit your business. If you find an inaccuracy or ambiguity within a British Standard or other BSI publication please inform the Knowledge Centre.

Copyright

All the data, software and documentation set out in all British Standards and other BSI publications are the property of and copyrighted by BSI, or some person or entity that owns copyright in the information used (such as the international standardization bodies) and has formally licensed such information to BSI for commercial publication and use. Except as permitted under the Copyright, Designs and Patents Act 1988 no extract may be reproduced, stored in a retrieval system or transmitted in any form or by any means – electronic, photocopying, recording or otherwise – without prior written permission from BSI. Details and advice can be obtained from the Copyright & Licensing Department.

Useful Contacts:

Customer Services
Tel: +44 845 086 9001
Email (orders): orders@bsigroup.com
Email (enquiries): cservices@bsigroup.com

Subscriptions
Tel: +44 845 086 9001
Email: subscriptions@bsigroup.com

Knowledge Centre
Tel: +44 20 8996 7004
Email: knowledgecentre@bsigroup.com

Copyright & Licensing
Tel: +44 20 8996 7070
Email: copyright@bsigroup.com

BSI Group Headquarters

389 Chiswick High Road London W4 4AL UK

bsi.

...making excellence a habit.™