



DPC: 24 / 30492184 DC

BSI Group Headquarters

389 Chiswick High Road London W4 4AL

Tel: +44 (0)20 8996 9000

Fax: +44 (0)20 8996 7400

www.bsigroup.com

Date: 30 April 2024

Origin: International

Latest date for receipt of comments: 21 June 2024

Project No. 2024/01276

Responsible committee: NCE/8 Instrumentation, Control & Electrical Systems of Nuclear Facilities

Interested committees:

Title: Draft of BS IEC/IEEE 62671 ED2 Nuclear power plants - Instrumentation and control important to safety - Selection and use of industrial digital devices of limited functionality

Please notify the secretary if you are aware of any keywords that might assist in classifying or identifying the standard or if the content of this standard

- i) has any issues related to 3rd party IPR, patent or copyright
- ii) affects other national standard(s)
- iii) requires additional national guidance or information

**WARNING: THIS IS A DRAFT AND MUST NOT BE REGARDED OR USED AS A BRITISH STANDARD.
THIS DRAFT IS NOT CURRENT BEYOND 21 June 2024**

This draft is issued to allow comments from interested parties; all comments will be given consideration prior to publication. No acknowledgement will normally be sent. **See overleaf for information on the submission of comments.**

No copying is allowed, in any form, without prior written permission from BSI except as permitted under the Copyright, Designs and Patent Act 1988 or for circulation within a nominating organization for briefing purposes. Electronic circulation is limited to dissemination by e-mail within such an organization by committee members.

Further copies of this draft may be purchased from BSI Shop <http://shop.bsigroup.com> or from BSI Customer Services, Tel: +44(0) 20 8996 9001 or email cservices@bsigroup.com. British, International and foreign standards are also available from BSI Customer Services.

Information on the co-operating organizations represented on the committees referenced above may be obtained from <http://standardsdevelopment.bsigroup.com>

Responsible Committee Secretary: Mr Andranik Ohanian (BSI)

Direct tel:

E-mail: andranik.ohanian@bsigroup.com

Introduction

This draft standard is based on national and international discussions. Your comments on this draft are invited and will assist in the preparation of the consequent standard.

For international standards, comments will be reviewed by the relevant UK national committee before sending the consensus UK vote and comments to the international committee, which will then decide appropriate action. If the international standard is approved, it is usual for the text to be published as a British Standard.

For national standards, comments will be reviewed by the relevant UK national committee and the resulting standards published as a British Standard.

UK Vote

Please indicate whether you consider the UK should submit a negative (with supporting technical reasons) or positive vote on this draft. Please indicate if you are aware of any reason why this draft standard should not be published as a British Standard.

Submission of Comments

- **Annotated drafts are not acceptable and will be rejected.**
- All comments should be submitted online at <https://standardsdevelopment.bsigroup.com/>. You will need to register in order to comment.

Template for comments and secretariat observations

Date: xx/xx/20xx	Document: ISO/DIS xxxx
------------------	------------------------

1	2	(3)	4	5	(6)	7
MB	Clause No./ Subclause No./Annex (e.g. 3.1)	Paragraph/Figure/ Table/Note	Type of comment	Commend (justification for change) by the MB	Proposed change by the MB	Secretariat observations on each comment submitted
	3.1	Definition 1	ed	Definition is ambiguous and needs clarifying.	Amend to read '...so that the mains connector to which no connection...'	
	6.4	Paragraph 2	te	The use of the UV photometer as an alternative cannot be supported as serious problems have been encountered in its use in the UK.	Delete reference to UV photometer.	



45A/1533/CD

COMMITTEE DRAFT (CD)

PROJECT NUMBER:

IEC/IEEE 62671 ED2

DATE OF CIRCULATION:

2024-04-26

CLOSING DATE FOR COMMENTS:

2024-06-21

SUPERSEDES DOCUMENTS:

45A/1448/RR

IEC SC 45A : INSTRUMENTATION, CONTROL AND ELECTRICAL POWER SYSTEMS OF NUCLEAR FACILITIES

SECRETARIAT:

France

SECRETARY:

Mr Alexander WIGG

OF INTEREST TO THE FOLLOWING COMMITTEES:

PROPOSED HORIZONTAL STANDARD:

☐

Other TC/SCs are requested to indicate their interest, if any, in this CD to the secretary.

FUNCTIONS CONCERNED:

☐ EMC☐ ENVIRONMENT☐ QUALITY ASSURANCE☒ SAFETY

This document is still under study and subject to change. It should not be used for reference purposes.

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

Recipients of this document are invited to submit, with their comments, notification of any local regulations or technical reasons that may exist and should be considered should this proposal proceed, recognizing that failure to address such requirements could result in the need for new or existing "In Some Countries" clauses. (See [AC/22/2007](#) or [NEW GUIDANCE DOC](#)).

TITLE:

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

NOTE FROM TC/SC OFFICERS:

Committee Draft prepared and circulated in accordance with Decision 45A/2023-20 from SC45A Plenary Meeting, see 45A/1509A/RM. Commenting period of 8 weeks to allow for preliminary discussions of comments during joint WGA3/A7 meeting scheduled from 24th - 27th June.

CONTENTS

1	Scope	9
1.1	General	9
1.2	Background	10
2	Normative references	10
3	Terms and definitions	11
4	Symbols and abbreviations	17
5	General requirements	18
5.1	General	18
5.2	Application of this standard	18
5.2.1	General	18
5.2.2	Applicability criteria for this standard	18
5.3	General requirements on the evaluation process	19
5.3.1	Evaluation process	19
5.3.2	Evaluation and Application Plan (EAP)	22
5.3.3	Evaluation and Application Report (EAR)	22
5.3.4	Application of clauses of this standard	24
6	Criteria for functional and performance suitability	24
6.1	General	24
6.2	Functional competence of the primary function	25
6.3	Ancillary functions	25
6.4	Configurability	25
6.5	Superfluous functions	26
6.6	Reliability, maintainability and testability	26
6.7	Hardware robustness	27
6.8	Cyber security	27
6.9	User documentation for safety	27
7	Criteria for dependability – Evidence of correctness	28
7.1	General	28
7.2	Previous certification	30
7.2.1	General	30
7.2.2	Previous Certification to IEC 61508	31
7.2.3	Previous certification to other non-nuclear standards	31
7.3	Avoidance of systematic faults	32
7.4	Evidence of quality in the design process	35
7.4.1	General	35
7.4.2	Product designer's QA program	35
7.4.3	Design and development process	37
7.4.4	Design configuration management	37
7.4.5	Design change control	38
7.4.6	Design documentation	39
7.5	Evidence of quality in manufacturing	41
8	Compensating measures	42
8.1	General	42
8.2	Product stability	42
8.3	Operating experience	42

8.4	Complementary testing and/or analysis (verification)	44
8.5	Documentation improvement	45
9	Criteria for integration into the application – limits and conditions of use	46
9.1	General	46
9.2	Restrictions on use.....	46
9.3	Modifications of the device required for the application	46
9.4	Modifications to the system to accommodate the device	47
9.5	Integration and commissioning of the device in the plant safety systems	47
10	Considerations for preserving acceptability.....	48
10.1	General	48
10.2	Notifications by the device designer and manufacturer	49
10.3	Manufacturing and support lifetime of the current version	49
10.4	Preservation of maintenance tools and documentation	49
10.5	Recommendations for the end-user	50
Annex A (informative)	Possible design features of a software system that could impact the dependability of the device	51
Annex B (informative)	Recommended Competencies for Personnel Assessing Candidate Devices	53
Figure 1 – Selection and evaluation process		21

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.

The contents of the corrigendum of September 2016 have been included in this copy.

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 complex¹ 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.

For more details on the structure of the IEC SC 45A standard series, see item d) of this introduction.

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.

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 IEC SC 45A standard series comprises a consistent set of documents organised in a hierarchy of four levels. The top-level documents of the IEC SC 45A standard series are IEC 61513 and IEC 63046, covering respectively general requirements for instrumentation and control (I&C) systems and general requirements for electrical power systems of NPPs. IEC 61513 and IEC 63046 adopt an overall system life-cycle framework and constitute, along with the relevant second-level standards, the nuclear implementation of the basic safety series IEC 61508.

IEC 61513 and IEC 63046 refer directly to other IEC SC 45A standards for general requirements for specific topics, such as categorization of functions and classification of systems, qualification, separation, defence against common cause failure, control room design, electromagnetic compatibility, human factors engineering, cybersecurity, software and hardware aspects for programmable digital systems, coordination of safety and security requirements and management of ageing.

At a third level, IEC SC 45A standards not directly referenced by IEC 61513 or by IEC 63046 are standards related to specific requirements for specific equipment, technical methods, or activities. Usually, these documents refer to second-level documents for general requirements and can be used on their own.

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

The IEC SC 45A standards series consistently implements and details the safety and security principles and basic aspects provided in the relevant IAEA safety standards and in the relevant documents of the IAEA nuclear security series (NSS). In particular this includes the IAEA requirements SSR-2/1, establishing safety requirements related to the design of nuclear power plants (NPPs), the IAEA safety guide SSG-30 dealing with the safety classification of structures, systems and components in NPPs, the IAEA safety guide SSG-39 dealing with the design of instrumentation and control systems for NPPs, the IAEA safety guide SSG-34 dealing with the

87 design of electrical power systems for NPPs, the IAEA safety guide SSG-51 dealing with human
88 factors engineering in the design of NPPs and the implementing guide NSS42-G for computer
89 security at nuclear facilities. The safety and security terminology and definitions used by the SC
90 45A standards are consistent with those used by the IAEA.

91 IEC 61513 and IEC 63046 refer to ISO 9001 as well as to IAEA GSR part 2 and IAEA GS-G-3.1
92 and IAEA GS-G-3.5 for topics related to quality assurance (QA).

93 At level 2, regarding nuclear security, IEC 62645 is the entry document for the IEC/SC 45A
94 security standards. It builds upon the valid high-level principles and main concepts of the generic
95 security standards, in particular ISO/IEC 27001 and ISO/IEC 27002; it adapts them and
96 completes them to fit the nuclear context and coordinates with the IEC 62443 series. At level 2,
97 IEC 60964 is the entry document for the IEC/SC 45A control rooms standards, IEC 63351 is the
98 entry document for the human factors engineering standards and IEC 62342 is the entry
99 document for the ageing management standards.

100 NOTE IEC TR 63400 provides a more comprehensive description of the overall structure of the IEC SC 45A
101 standards series and of its relationship with other standards bodies and standards.

102

103

**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 HDL Programmed Devices (HPD) which are candidates for use in nuclear power plants. It provides requirements for the selection and evaluation of such devices where they have dedicated, limited, and specific functionality and limited configurability.

The scope of this standard encompasses what the IAEA refers to as “Smart Devices” in Safety Reports Series No. 111, which draws from IEC 62671 (see 5.2.2 for Applicability). This standard is also applicable to devices that allow for application programming, in these cases specific requirements apply.

Digital devices of limited functionality (DDLFF) are a subset of smart devices. Generally, while smart devices can be tuned within very specific bounds to perform a simple, well understood function, they are not programmable after manufacturing. This is the definition used in this standard. Other definitions for smart devices do exist; for example, in the United Kingdom, a common smart device considered programmable, runs software that can change, and may attach to the internet. This type of system, more akin to a programmable controller, is outside of the scope of this standard, which deliberately limits the definition of smart device to that included in IEC 62671. Another common term is intelligent device, which maps directly to the term smart device in this context. Also note, smart devices in this context may be embedded into larger systems, but they may be standalone as well. The Nuclear Regulatory Commission uses the term Embedded Digital Device, defined as “a component consisting of one or more electronic parts that requires the use of software, software-developed firmware, or software-developed programmable logic, and that is integrated into equipment to implement one or more system safety functions.”

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. Such devices are very often developed to meet IEC 61508, and this standard provides a framework for qualification of IEC 61508 certified devices.

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. and assessment of components.

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.

– .

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

IEC 62003 (all parts), *Electromagnetic compatibility (EMC)*

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

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

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

198 IEC 62645 *Nuclear power plants - Instrumentation, control and electrical power systems -*
199 *Cybersecurity requirements*

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

201 **3 Terms and definitions**

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

203 **3.1**

204 **ancillary function**

205 any function provided by the candidate device that supports its primary functions

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

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

210 **3.2**

211 **auditable**

212 property of documented evidence that is readily available for review by independent personnel

213 **3.3**

214 **category of an I&C function**

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

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

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

225 [SOURCE: IEC 61513:2011, 3.4]

226 **3.4**

227 **class of an I&C system**

228 one of three possible assignments (1, 2, 3) of I&C systems important to safety resulting from
229 consideration of their requirement to implement I&C functions of different safety relevance. An
230 unclassified assignment is made if the I&C system does not implement functions important to
231 safety

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

233 [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 narrow range of closely related 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 narrow range of closely 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

371 opts to use the 4 mA to 20 mA signal for safety purposes, then this would be the primary function and the other
372 output would be superfluous.

373 **3.19** 374 **qualification**

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

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

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

385 [SOURCE: IEC 61513:2011, 3.38]

386 **3.20** 387 **quality**

388 degree to which a set of inherent characteristics fulfils requirements

389 [SOURCE: ISO 9000:2005]

390 **3.21** 391 **quality assurance**

392 the function of a management system that provides confidence that specified requirements will
393 be fulfilled

394 [SOURCE: IAEA Safety glossary, 2007 Edition]

395 **3.22** 396 **requirement**

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

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

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

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

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

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

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

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

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

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

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

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

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

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

424 [SOURCE: IEC 61513:2011, 3.44]

425 **3.23**

426 **restricted configurability**

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

429 **3.24**

430 **security**

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

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

437 [SOURCE: IEC 61513:2011, 3.48]

438 **3.25**

439 **self-supervision**

440 automatic testing of system hardware performance and software consistency of a computer
441 based I&C system

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

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

447 Note 3 to entry: The expression "self-surveillance testing" is equivalent.

448 [SOURCE: IEC 60671:2007, 3.8]

449 **3.26**

450 **software**

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

453 [SOURCE: IEC 61513:2011, 3.51]

454 **3.27**

455 **software criticality analysis**

456 analysis of software to classify each function within the software as to its potential to cause
457 unsafe failures

458 **3.28**

459 **software fault**

460 design fault located in a software component

461 [SOURCE: IEC 61513:2011, 3.53]