



DPC: 25 / 30509912 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: 07 February 2025

Origin: International

Latest date for receipt of comments: 26 March 2025

Project No. 2024/01276

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

Interested committees:

Title: Draft 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 26 March 2025**

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/1585/CD

COMMITTEE DRAFT (CD)

PROJECT NUMBER:
IEC/IEEE 62671 ED2

DATE OF CIRCULATION:
2025-01-31

CLOSING DATE FOR COMMENTS:
2025-04-25

SUPERSEDES DOCUMENTS:
45A/1533A/CD, 45A/1551A/CC

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

SECRETARIAT:
France

SECRETARY:
Mr Alexander WIGG

OF INTEREST TO THE FOLLOWING COMMITTEES:
SC 65A

HORIZONTAL FUNCTION(S):

ASPECTS CONCERNED:
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:

CD2 circulated in accordance with working group recommendations following resolution of comments on CD1 during joint A3/A7 meeting which took place in Leatherhead, UK, from 24th to 27th June 2024 (see 45A/1561/INF). This CD also incorporates results of the IEEE NPEC 25-01 meeting which took place in January 2025. Comments on the CD2 will be discussed during the IEC SC45A technical meetings to take place in Knoxville, USA, in June 2025 (see 45/987/AC).

Copyright © 2025 International Electrotechnical Commission, IEC. All rights reserved. It is permitted to download this electronic file, to make a copy and to print out the content for the sole purpose of preparing National Committee positions. You may not copy or "mirror" the file or printed version of the document, or any part of it, for any other purpose without permission in writing from IEC.

CONTENTS

3	1	Scope	10
4	1.1	General	10
5	1.2	Background	10
6	2	Normative references	11
7	3	Terms and definitions	11
8	4	Symbols and abbreviations	18
9	5	General requirements	19
10	5.1	General	19
11	5.2	Application of this standard	19
12	5.2.1	General	19
13	5.2.2	Applicability criteria for this standard	19
14	5.3	General requirements on the evaluation process	20
15	5.3.1	Evaluation process	20
16	5.3.2	Evaluation and Application Plan (EAP)	23
17	5.3.3	Evaluation and Application Report (EAR)	23
18	5.3.4	Application of clauses of this standard	24
19	6	Criteria for functional and performance suitability	25
20	6.1	General	25
21	6.2	Functional suitability of the primary function	25
22	6.3	Ancillary functions	26
23	6.4	Configurability	26
24	6.5	Superfluous functions	26
25	6.6	Reliability, maintainability and testability	27
26	6.7	Hardware robustness	27
27	6.8	Cybersecurity	28
28	6.9	User documentation for safety	28
29	7	Criteria for dependability – Evidence of correctness	29
30	7.1	General	29
31	7.2	Previous certification	31
32	7.2.1	General	31
33	7.2.2	Previous Certification to IEC 61508	31
34	7.2.3	Previous certification to other non-nuclear standards	32
35	7.3	Avoidance of systematic faults	33
36	7.4	Evidence of quality in the design process	35
37	7.4.1	General	35
38	7.4.2	Product designer's QA program	35
39	7.4.3	Design and development process	37
40	7.4.4	Design configuration management	37
41	7.4.5	Design change control	38
42	7.4.6	Design documentation	39
43	7.5	Evidence of quality in manufacturing	40
44	8	Compensating measures	41
45	8.1	General	41
46	8.2	Product stability	41
47	8.3	Operating experience	42

48	8.4	Complementary testing and/or analysis (verification)	43
49	8.5	Documentation improvement	45
50	9	Criteria for integration into the application – limits and conditions of use	45
51	9.1	General	45
52	9.2	Restrictions on use	45
53	9.3	Modifications of the device required for the application	46
54	9.4	Modifications to the system to accommodate the device	46
55	9.5	Integration and commissioning of the device in the plant safety systems	47
56	10	Considerations for preserving acceptability	47
57	10.1	General	47
58	10.2	Notifications by the device designer and manufacturer	48
59	10.3	Manufacturing and support lifetime of the current version	48
60	10.4	Preservation of maintenance tools and documentation	48
61	10.5	Recommendations for the end-user	49
62	Annex A (informative)	Possible design features of a software system that could impact	
63		the dependability of the device	50
64	Annex B (informative)	Recommended Competencies for Personnel Assessing	
65		Candidate Devices	52
66	Annex C (informative)	AFCEN method for the qualification of DDLFs with IEC 61508	54
67	C.1	General	54
68	C.2	Objective of the method	54
69	C.3	Method of evaluation	54
70	C.4	Device selection	54
71	C.4.1	Respect of the definition of a DDLF	54
72	C.4.2	Development and certification according to the requirements of the	
73		standard IEC 61508	55
74	C.4.3	Compatibility of the safety function	55
75	C.4.4	Required SIL	55
76	C.5	General process for audits	56
77	C.6	Audit guidelines	56
78	C.6.1	Class 3	56
79	C.6.2	Class 2	56
80	C.6.3	Class 1	57
81	C.6.4	Summary	57
82	C.7	Evaluation and application report (EAR)	58
83	C.8	Modification management	58
84	Annex D (informative)	US requirements for use of IEC 61508 certifications as laid out	
85		by NEI 17-06 and RG 1.250	59
86	Annex E (informative)	Canadian Standards Association qualification methodologies for	
87		digital items	60
88	E.1	Canadian Regulatory Implications	60
89	E.2	Overview of CSA N290.14-15	60
90	E.3	CSA N290.14-15 Recognized Program method	60
91	E.4	Methodology for qualification of digital items	60
92	E.5	Qualification concerns	61
93			
94	Figure 1 –	Selection and evaluation process	22
95			
96	a		

97	Table 1 – Requirements regarding the design of the digital controller	33
98	Table 2 – Requirements regarding overall functioning of the DDLF	33
99	Table 3 – Requirements regarding the avoidance of systematic faults	34
100	Table 4 – Requirements regarding the product designer's QA program	35
101	Table 5 – Requirements regarding the design and development process	37
102	Table 6 – Requirements regarding design configuration management	37
103	Table 7 – Requirements regarding design change control	38
104	Table 8 – Requirements regarding design documentation	39
105	Table 9 – Requirements regarding evidence of quality in manufacturing	40
106	Table C.1 – DDLF qualification process according to the standard IEC 61508	54
107	Table C.2 – Summary of inspection points during the audit according to the safety	
108	class	57
109		
110		

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 document(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.

IEEE Standards documents are developed within IEEE Societies and Standards Coordinating Committees of the IEEE Standards Association (IEEE SA) Standards Board. IEEE develops its standards through a consensus development process, approved by the American National Standards Institute, which brings together volunteers representing varied viewpoints and interests to achieve the final product. Volunteers are not necessarily members of IEEE and serve without compensation. While IEEE administers the process and establishes rules to promote fairness in the consensus development process, IEEE does not independently evaluate, test, or verify the accuracy of any of the information contained in its standards. Use of IEEE Standards documents is wholly voluntary. *IEEE documents are made available for use subject to important notices and legal disclaimers (see <https://standards.ieee.org/ipr/disclaimers.html> for more information).*

IEC collaborates closely with IEEE in accordance with conditions determined by agreement between the two organizations. This Dual Logo International Standard was jointly developed by the IEC and IEEE under the terms of that agreement.

2) The formal decisions 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. The formal decisions of IEEE on technical matters, once consensus within IEEE Societies and Standards Coordinating Committees has been reached, is determined by a balanced ballot of materially interested parties who indicate interest in reviewing the proposed standard. Final approval of the IEEE standards document is given by the IEEE Standards Association (IEEE SA) Standards Board.

3) IEC/IEEE Publications have the form of recommendations for international use and are accepted by IEC National Committees/IEEE Societies in that sense. While all reasonable efforts are made to ensure that the technical content of IEC/IEEE Publications is accurate, IEC or IEEE 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 (including IEC/IEEE Publications) transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC/IEEE Publication and the corresponding national or regional publication shall be clearly indicated in the latter.

5) IEC and IEEE do not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC and IEEE are 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 IEEE or their directors, employees, servants or agents including individual experts and members of technical committees and IEC National Committees, or volunteers of IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Association (IEEE SA) Standards Board, 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/IEEE Publication or any other IEC or IEEE 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 implementation of this IEC/IEEE Publication may require use of material covered by patent rights. By publication of this standard, no position is taken with respect to the existence or validity of any patent rights in connection therewith. IEC or IEEE shall not be held responsible for identifying Essential Patent Claims for which a license may be required, for conducting inquiries into the legal validity or scope of Patent Claims or determining whether any licensing terms or conditions provided in connection with submission of a Letter of Assurance, if any, or in any licensing agreements are reasonable or non-discriminatory. Users of this standard are expressly advised that determination of the validity of any patent rights, and the risk of infringement of such rights, is entirely their own responsibility.

IEC/IEEE 62671 was prepared by subcommittee 45A: Instrumentation, control and electrical power systems of nuclear facilities, of IEC technical committee 45: Nuclear instrumentation, in

176 cooperation with the Nuclear Power Engineering Committee of the IEEE, under the IEC/IEEE
177 Dual Logo Agreement between IEC and IEEE. It is an International Standard.

178 This document is published as an IEC/IEEE Dual Logo standard.

179 This second edition cancels and replaces the first edition published in 2013 and Corrigendum
180 1 published in 2016. This edition constitutes a technical revision.

181 This edition includes the following significant technical changes with respect to the previous
182 edition:

- 183 a) Adaptation of the content to ensure compatibility with IEEE NPEC,
- 184 b) Adaptation to accommodate recent IAEA publications,
- 185 c) Improved compatibility with the generic functional safety standard series IEC 61508,
- 186 d) Addition of informative annexe to facilitate the use of the standard in multiple regulatory
187 contexts,

188 The text of this International Standard is based on the following IEC documents:

Draft	Report on voting
XX/XX/FDIS	XX/XX/RVD

189
190 Full information on the voting for its approval can be found in the report on voting indicated in
191 the above table.

192 The language used for the development of this International Standard is English.

193 This document was drafted in accordance with the rules given in the ISO/IEC Directives, Part 2,
194 available at www.iec.ch/members_experts/refdocs. The main document types developed by IEC
195 are described in greater detail at www.iec.ch/publications/.

196 The IEC Technical Committee and IEEE Technical Committee have decided that the contents
197 of this document will remain unchanged until the stability date indicated on the IEC website
198 under webstore.iec.ch in the data related to the specific document. At this date, the document
199 will be

- 200 • reconfirmed,
- 201 • withdrawn, or
- 202 • revised.

203

204

205

206 INTRODUCTION

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

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

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

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

- 217 • This standard only covers devices with very restricted functionality, and
- 218 • This standard focuses on the considerations necessary to apply devices in NPPs that
219 have not been specifically designed for nuclear use.

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

224 Hence it has become vital for designers of these systems to have the guidance provided by this
225 standard to be able to select and evaluate candidate devices for their suitability to applications
226 in NPPs. This standard provides such guidance without which I&C designers would be required
227 to consider how to interpret IEC 60880, IEC 62138, IEC 62556/IEC 62566-2 or IEC 60987 for
228 this purpose.

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

230 IEC 61513 is a first level IEC SC 45A document and gives guidance applicable to I&C at the
231 system level. It is supplemented by guidance at the device level by IEC 60987 for design of
232 hardware, by IEC 60880 and IEC 62138 for software and by IEC 62566 and IEC 62566-2 for
233 potentially complex devices. All of these standards focus on nuclear-specific designs and apply
234 the concept of a life cycle.

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

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

242 c) Recommendations and limitations regarding the application of the Standard

243 It is important to note that this Standard establishes no additional functional requirements for
244 systems of class 1, 2 or 3.

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

- 246 • The use of a planned process to select, and then evaluate candidate devices for use,
247 as well as to include considerations of the integration of the device into plant systems.
- 248 • Criteria for evaluating the functional suitability of a device that contains embedded
249 software or uses digital circuits designed with software-based tools such as HDL
250 (Hardware Description Language).

251 • Criteria to consider and balance in an overall evaluation to obtain an appropriate level
252 of assurance that the device will perform as specified when called upon.

253 • Considerations for the safe application of the selected device in plant systems.

254 To ensure that the Standard will continue to be relevant in future years, the emphasis has been
255 placed on issues of principle, rather than specific technologies.

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

261 **d) Description of the structure of the IEC SC 45A standard series and relationships with**
262 **other IEC documents and other bodies documents (IAEA, ISO)**

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

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

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

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

282 The IEC SC 45A standards series consistently implement and details the safety and
283 cybersecurity principles and basic aspects provided in the relevant IAEA safety standards and
284 in the relevant documents of the IAEA nuclear security series (NSS). In particular this includes
285 the IAEA requirements SSR-2/1, establishing safety requirements related to the design of
286 nuclear power plants (NPPs), the IAEA safety guide SSG-30 dealing with the safety
287 classification of structures, systems and components in NPPs, the IAEA safety guide SSG-39
288 dealing with the design of instrumentation and control systems for NPPs, the IAEA safety guide
289 SSG-34 dealing with the design of electrical power systems for NPPs, the IAEA safety guide
290 SSG-51 dealing with human factors engineering in the design of NPPs, the implementing guide
291 NSS 42-G and technical guidance NSS 17-T for computer security at nuclear facilities. The
292 safety and cyber security terminology and definitions used by SC 45A standards are consistent
293 with those used by the IAEA.

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

296 At level 2, regarding nuclear security, IEC 62645 is the entry document for the IEC SC 45A
297 security standards. It builds upon the valid high-level principles and main concepts of the
298 generic security standards, in particular ISO/IEC 27001 and ISO/IEC 27002; it adapts them and
299 completes them to fit the nuclear context and coordinates with the IEC 62443 series. At level
300 2, IEC 60964 is the entry document for the IEC SC 45A control rooms standards, IEC 63351 is

301 the entry document for the human factors engineering standards and IEC 62342 is the entry
302 document for the ageing management standards.

303 Note 1: IEC TR 63400 provides a more comprehensive description of the overall structure of the IEC SC 45A
304 standards series and of its relationship with other standards bodies and standards.

305

306

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 document 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).

I&C systems important to safety of classes 1, 2 and 3 (in the IEC 61513 context) and class 1E (in the IEEE 603 context) 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 industrial safety standards such as IEC 61508. This standard provides a framework for qualification of the devices for use in a nuclear power plant.

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, IEC 62138, and IEEE 7-4.3.2 for software. This standard addresses the aspects 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 aspects, with more demanding requirements applied for higher classes.

These aspects 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/IEEE 60780-323, IEC 62003, IEEE 2425, and IEC/IEEE 60980-344 to address hardware qualification aspects not related to the complexities of software, namely reliability aspects related to environmental qualification and failures due to aging or physical degradation.

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.

355 embedded within the candidate replacement devices, and analog devices are becoming
356 increasingly unavailable.

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

- 359 • many of these devices do not duplicate the precise functionality of the obsolete device
360 to be replaced, having in some cases less and in other cases more functionality, or even
361 subtly different functionality that may be inconsistent with the original design intent,
- 362 • these differences in functionality are not always readily apparent.
- 363 • they may have specific vulnerabilities or failure modes that did not exist with the original
364 equipment and that need to be considered.

365 **2 Normative references**

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

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

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

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

377 IEC 62645:2019 Nuclear power plants - Instrumentation, control and electrical power systems
378 - Cybersecurity requirements

379 ISO 9001:20015, Quality management systems – Requirements

380 IEC/IEEE 60780-323:2016, Standard for Nuclear facilities- Electrical Equipment important to
381 safety- Qualification

382 IEEE 603:2018, Standard Criteria for Safety Systems for Nuclear Power Generating Stations

383 IEEE 7-4.3.2:2016, Standard Criteria for Programmable Digital Devices in Safety Systems of
384 Nuclear Power Generating Stations

385 **3 Terms and definitions**

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

387 **3.1**

388 **ancillary function**

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

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

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

394 **3.2**

395 **auditable**

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

3.3**Class 1E**

The safety classification of the electric equipment and systems that are essential to emergency reactor shutdown, containment isolation, reactor core cooling, and containment and reactor heat removal, or are otherwise essential in preventing significant release of radioactive material to the environment.

Note to entry: Users of this standard are advised that Class 1E is a functional term. Equipment and systems are to be classified Class 1E only if they fulfill the functions listed in the definition. Identification of systems or equipment as Class 1E based on anything other than their function is an improper use of the term and should be avoided.

[SOURCE: IEEE 603:2018]

3.4**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 uncategorized 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 there corresponds a set of requirements applicable on both the I&C function (concerning its specification, design, implementation, verification and validation) and the whole the I&C chain (concerning the properties and the related qualification). The requirements are regardless of how the items of the I&C chain are distributed in a number of interconnected I&C systems. For more clarity, this document 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 61513:20XX 3.4]

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

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

[SOURCE: IEC 61513:20XX 3.6]

3.6**common cause failure****CCF**

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

[SOURCE: IAEA Nuclear Safety and Security Glossary, 2022 Edition]

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

3.7**computer-based item**

item that relies on software instructions running on microprocessors or microcontrollers

[SOURCE: IEC 62138:2018, 3.8]

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

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

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

Note 4 to entry: The IEC definition differs from the IAEA definition for "computer-based systems" because it needs to be more specific on the kind of digital technology which is covered.

3.8**cybersecurity**

set of activities and measures the objective of which is to prevent, detect, and react to:

- malicious modifications (integrity) of functions that may compromise the delivery or integrity of the required service by I&C programmable digital systems (incl. loss of control) which could lead to an accident, an unsafe situation or plant performance degradation
- malicious withholding or prevention of access to or communication of information, data or resources (incl. loss of view) that could compromise the delivery of the required service by I&C systems (availability) which could lead to an accident, an unsafe situation or plant performance degradation
- malicious disclosures of information (confidentiality) that could be used to perform malicious acts which could lead to an accident, an unsafe situation or plant performance degradation

[SOURCE: IEC 62645:2019]

Note 1 to entry: The IAEA Nuclear Safety and Security Glossary, 2022 Edition uses the terms “cyber security”, “IT security” and “computer security” as equivalent terms and in a wider sense, i.e. without restricting them to programmable I&C systems.

3.9**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.

3.10**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

[SOURCE: IEC 61513:20XX, 3.19]

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

Note 2 to entry: Equipment can be a programmable digital item and include software and configuration data.

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/IEEE 60780-323. The deviation is justified by the fact that IEC 61513 considers “equipment” as part of a system whereas IEC/IEEE 60780-323 considers equipment as the object of qualification.

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

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

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

[SOURCE: IEC 62566:2012, 3.6]

493 3.12**494 HDL-Programmed Device****495 HPD**

496 integrated circuit configured (for NPP I&C systems), with Hardware Description Languages and
497 related software tools

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

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

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

502 [SOURCE: IEC 62566:2012, 3.7]

503 3.13**504 I&C function**

505 function to control, operate and/or monitor a defined part of the power plant processes

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

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

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

513 [SOURCE: IEC 61513:20XX, 3.33]

514 3.14**515 I&C system**

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

519 Note 1 to entry: The term is used as a general term which encompasses all elements of the system such as internal
520 power supplies, sensors and other input devices, data highways and other communication paths, interfaces to
521 actuators and other output devices (see Note 3). The different functions within a system may use dedicated or shared
522 resources.

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

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

527 Note 4 to entry: See also “system” and “I&C function”.

528 [SOURCE: IEC 61513:20XX, 3.36]

529 3.15**530 interrupt**

531 suspension of a process to handle an event external to the process

532 [SOURCE: ISO/IEC/IEEE 24765]

533 3.16**534 item important to safety**

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

537 [SOURCE: IAEA Nuclear Safety and Security Glossary, 2022 Edition]

538 Note 1 to entry: Items important to safety include:

- 539 a) those structures, systems and components whose malfunction or failure could lead to undue radiation
540 exposure of the site personnel or members of the public;
- 541 b) those structures, systems and components that prevent anticipated operational occurrences from leading to
542 accident conditions;
- 543 c) safety features for design extension conditions;
- 544 d) those features that are provided to mitigate the consequences of malfunction or failure of structures,
545 systems or components.

546 Note 2 to entry: This definition is intended to encompass all aspects of nuclear safety and addresses equipment and
547 systems performing functions of categories A, B and C according to IEC 61226.

548 Note 3 to entry: In IEC 61513, the items considered will be mainly I&C systems or I&C functions.

549 **3.17**
550 **limited functionality**

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

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

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

560 Note 3 to entry: "Dedicated" in the sense in which it is used in this standard refers to design for a specific
561 functionality that cannot be changed in the field.

562 **3.18**
563 **overall I&C safety life cycle**

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

568 [SOURCE: IEC 61508-4:2010, 3.7.1, modified, from "safety lifecycle", replacement of term
569 "safety-related" by "important to safety" and removal of term "E/E/PE"]

570 Note 1 to entry: The overall safety lifecycle of the I&C induces requirements for the individual system safety lifecycles.

571 Note 2 to entry: See also "system safety lifecycle".

572 **3.19**
573 **primary function**

574 singular function (or narrow range of closely related functions) of the candidate device which is
575 required for the system important to safety to perform its function claimed in the safety analysis,
576 and which is relied on to operate autonomously to achieve this function

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

580 Note 2 to entry: See also "ancillary function" and "superfluous function"

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

587 Note 4 to entry: For example, a smart sensor may be capable of outputting a signal representing the flow or level
588 via an analog output ranging from 4 mA to 20 mA or via a HART protocol. If the designer of the nuclear application

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

591 **3.20**

592 **quality**

593 degree to which a set of inherent characteristics of an object fulfils requirements

594 [SOURCE: ISO 9000:2015, 3.6.2]

595 **3.21**

596 **quality assurance**

597 function of a management system that provides confidence that specified requirements will be
598 fulfilled

599 [SOURCE: IAEA Nuclear Safety and Security Glossary, 2022 Edition]

600 **3.22**

601 **requirement**

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

604 [SOURCE: ISO/IEC Directives, Part 2, 2011, 3.3.1]

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

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

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

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

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

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

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

619 Note 2 to entry: The IAEA safety glossary Edition 20022 (Interim) contains the following definition:

620 , *Requirement* - That which is established or required by (national or international) laws or regulations, or by IAEA
621 Safety Fundamentals or IAEA Safety Requirements publications.

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

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

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

628 **3.23**

629 **restricted configurability**

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

632 **3.24**

633 **risk-informed safety classification (RISC)**

634 Using IEEE 1819, electrical and electronic systems and components (EESCs) that are Class
635 1E can be categorized as RISC-1 (safety-significant) or RISC-3 (low safety-significant). EESCs
636 that are non-Class 1E can be categorized as RISC-2 (safety-significant) or RISC-4 (low safety-
637 significant)

638 Note to entry: See IEEE 1819:2016 for additional details.

639 3.25

640 self-supervision

641 automatic testing of system hardware performance and software consistency of a computer
642 based I&C system

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

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

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

649 [SOURCE: IEC 60671:2007, 3.8]

650 3.26

651 software

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

654 Note 1 to entry: The term is reserved for CPU / processor based technology. Interconnection information and other
655 configuration data representing the implementation of an application in HDL-programmed devices are not included.

656 [SOURCE: IEC 61513:20XX, 3.61]

657 3.27

658 software criticality analysis

659 analysis of software to classify each function within the software as to its potential to cause
660 unsafe failures

661 3.28

662 superfluous function

663 all functions performed by a candidate device that are not required functions

664 Note 1 to entry: For example, while a primary function may be the sensing of pressure transmission of a 4 mA to
665 20 mA signal to another device, an ancillary function may be one which supports adjusting the filtering parameters
666 of this output to achieve the desired safety function, while a superfluous function may be a second output such as a
667 voltage signal that is not needed for the safety function.

668 Note 2 to entry: See also "Primary function" and "ancillary function".

669 3.29

670 surveillance test

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

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

680 Note 2 to entry: A synonym is "proof test".

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

682 3.30

683 system qualification

684 process of determining whether a system is suitable for operational use, by examination and
685 provision of other evidence that the system fulfils in its entirety the requirement specification as
686 intended (functionality, response time, tolerance to failure, robustness etc.)

687 [SOURCE: IEC 61513:20XX, 3.65]

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

690 Note 2 to entry: Qualification of I&C systems may rely to a large degree on qualification activities performed outside
691 the framework of a specific plant design ("generic qualification", "pre-qualification"). Pre-qualification can reduce the
692 plant-specific qualification effort significantly, however, the application-specific qualification requirements are still to
693 be met.

694 Note 3 to entry: The definition is consistent with the definition of "qualification" and "system validation" given in IAEA
695 Nuclear Safety and Security Glossary 2022, restricted to the case of an I&C system.

696 3.31

697 **systematic fault**

698 fault related in a deterministic way to a certain cause, which can only be eliminated by a
699 modification of the design or of the manufacturing process, operational procedures, documen-
700 tation or other relevant factors

701 [SOURCE: IEC 61508-4:2010, 3.6.6, modified from "systematic failure"]

702 4 Symbols and abbreviations

703	ASIC	Application specific integrated circuit
704	CM	Compensatory Measure
705	COTS	Commercial off the shelf
706	CPU	Central processing unit
707	CT	Complementary testing
708	DDLFF	Digital Device of Limited Functionality
709	DI	Documentation Improvement
710	EAP	Evaluation and Application Plan
711	EAR	Evaluation and Application Report
712	EMC	Electromagnetic compatibility
713	EMI	Electromagnetic interference
714	FMEA	Failure modes effects analysis
715	FMECA	Failure modes effects and criticality analysis
716	FMEDA	Failure modes effects and diagnostic analysis
717	FPGA	Field programmable gate array
718	FTA	Fault tree analysis
719	HART	Highway addressable remote transducer (protocol)
720	HDL	Hardware description language
721	HMI	Human machine interface
722	HPD	HDL programmed device
723	I&C	Instrumentation and control
724	NPP	Nuclear power plant
725	OE	Operating experience
726	PLC	Programmable logic controller
727	PS	Product stability
728	PROM	Programmable read only memory
729	QA	Quality assurance
730	RISC	Risk-informed safety classification
731	SIL	Safety Integrity Level
732	VHDL	Very high speed integrated circuit hardware description language