



DPC: 24 / 30486630 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: 01 February 2024

Origin: International

Latest date for receipt of comments: 20 March 2024

Project No. 2024/00247

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

Interested committees:

Title: BS EN IEC 61513 Nuclear power plants - Instrumentation and control important to safety -General requirements for systems

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 20 March 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.	

PROJECT NUMBER: IEC 61513 ED3	
DATE OF CIRCULATION: 2024-01-26	CLOSING DATE FOR COMMENTS: 2024-04-19
SUPERSEDES DOCUMENTS: 45A/1430/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: SC 65A	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 – General requirements for systems
--

NOTE FROM TC/SC OFFICERS: CD1 prepared and circulated in accordance with WGA3 recommendations and decision 45A/2023-11 from October 2023 SC45A Plenary meeting, see 45A/1509/RM.

CONTENTS

1	Scope	7
2	Normative references	10
3	Terms and definitions	11
4	Symbols and abbreviations	26
5	Overall I&C safety lifecycle	26
6	System safety lifecycle	52
7	Overall integration and commissioning	95
8	Overall operation and maintenance	95
	Annex A (informative) Fundamental Safety Principles in the NPP	97
	A.1 General	97
	A.2 Fundamental safety functions, safety analysis and safety assessment	97
	A.2.1 Safety assessment	98
	A.2.2 Safety analysis	99
	A.3 Defence in depth	100
	A.3.1 Independence	101
	A.3.2 Common cause failures	101
	A.4 Interfaces of safety with nuclear security	102
	Annex B (informative) Relations of IEC 61508 with IEC 61513 and standards of the nuclear application sector	103
	B.1 General	103
	B.2 Comparison of scopes and concepts	103
	B.3 Correspondence between IEC 61508-1 and this standard	105
	B.4 Correspondence between IEC 61508-2 and this standard	107
	B.5 Correspondence between some important terms of IEC 61508-4 and the definitions of this standard and of the nuclear application sector	109
	Annex C (informative) Typical document structure for overall I&C, I&C architecture and I&C system design	111
	Annex D (informative) Changes in later revisions of SC 45A standards to adapt to this version of IEC 61513	115

INTERNATIONAL ELECTROTECHNICAL COMMISSION

**NUCLEAR POWER PLANTS –
INSTRUMENTATION AND CONTROL IMPORTANT TO SAFETY –
GENERAL REQUIREMENTS FOR SYSTEMS**

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 61513 has been prepared by subcommittee 45A: Instrumentation and control of nuclear facilities, of IEC technical committee 45: Nuclear instrumentation.

This third edition cancels and replaces the second edition, published in 2011, and constitutes a technical revision.

The main technical changes with regard to the previous edition are as follows:

- to align the standard with the recent IAEA documents SSR-2.1 and SSG-39, to review the existing requirements and to update the terminology and definitions;
- to take account of, as far as possible, requirements associated with standards published or thoroughly revised since the second edition, IEC 62566, IEC 61226, IEC 62138, IEC 60987, IEC 63046 and IEC 63351;

- to integrate experience from use of the earlier revisions of the standard.

FDIS	Report on voting
45A/xxx/FDIS	45A/yyy/RVD

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

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

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

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

INTRODUCTION

a) Technical background, main issues and organisation of the standard

This International Standard sets out requirements applicable to instrumentation and control systems and equipment (I&C systems) that are used to perform functions important to safety in nuclear power plants (NPPs).

This standard highlights the relations between

- the safety objectives of the NPP and the requirements for the overall architecture of the I&C systems important to safety;
- the overall architecture of the I&C systems and the requirements of the individual systems important to safety.

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

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

IEC 61513 is the first level IEC SC 45A document tackling the issue of general requirements for systems. It is the entry point of the IEC SC 45A standard series.

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

c) Recommendations and limitations regarding the application of this standard

It is important to note that this standard establishes no additional functional requirements for safety 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.

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

The top-level documents of the IEC SC 45A standard series are IEC 61513 and IEC 63046. IEC 61513 provides general requirements for I&C systems and equipment that are used to perform functions important to safety in NPPs. IEC 63046 provides general requirements for electrical power systems of NPPs; it covers power supply systems including the supply systems of the I&C systems. IEC 61513 and IEC 63046 are to be considered in conjunction and at the same level. IEC 61513 and IEC 63046 structure the IEC SC 45A standard series and shape a complete framework establishing general requirements for instrumentation, control and electrical systems for nuclear power plants.

IEC 61513 and IEC 63046 refer directly to other IEC SC 45A standards for general topics related to categorization of functions and classification of systems, qualification, separation, defence against common cause failure, control room design, electromagnetic compatibility, cybersecurity, software and hardware aspects for programmable digital systems, coordination of safety and security requirements and management of ageing. The standards referenced directly at this second level should be considered together with IEC 61513 and IEC 63046 as a consistent document set.

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

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

The IEC SC 45A standards series consistently implement and detail the safety and security principles and basic aspects provided in the relevant IAEA safety standards and in the relevant documents of the IAEA nuclear security series (NSS). In particular this includes the IAEA requirements SSR-2/1, establishing safety requirements related to the design of nuclear power plants (NPPs), the IAEA safety guide SSG-30 dealing with the safety classification of structures, systems and components in NPPs, the IAEA safety guide SSG-39 dealing with the design of instrumentation and control systems for NPPs, the IAEA safety guide SSG-34 dealing with the design of electrical power systems for NPPs and the implementing guide NSS17 for computer security at nuclear facilities. The safety and security terminology and definitions used by SC 45A standards are consistent with those used by the IAEA.

IEC 61513 and IEC 63046 have adopted a presentation format similar to the basic safety publication IEC 61508 with an overall life-cycle framework and a system life-cycle framework. Regarding nuclear safety, IEC 61513 and IEC 63046 provide the interpretation of the general requirements of IEC 61508-1, IEC 61508-2 and IEC 61508-4, for the nuclear application sector. In this framework IEC 60880, IEC 62138, IEC 62566 and IEC 62566-2 correspond to IEC 61508-3 for the nuclear application sector. IEC 61513 and IEC 63046 refer to ISO as well as to IAEA GS-R part 2 and IAEA GS-G-3.1 and IAEA GS-G-3.5 for topics related to quality assurance (QA). At level 2, regarding nuclear security, IEC 62645 is the entry document for the IEC/SC 45A security standards. It builds upon the valid high level principles and main concepts of the generic security standards, in particular ISO/IEC 27001 and ISO/IEC 27002; it adapts them and completes them to fit the nuclear context and coordinates with the IEC 62443 series. At level 2, IEC 60964 is the entry document for the IEC/SC 45A control rooms standards, IEC 63351 is the entry document for the human factors engineering standards, and IEC 62342 is the entry document for the ageing management standards.

NOTE 1 It is assumed that for the design of I&C systems in NPPs that implement conventional safety functions (e.g. to address worker safety, asset protection, protection from chemical hazards and process energy hazards), international or national standards would be applied, that are based on the requirements of such a standard as the IEC 61508 series.

NOTE 2 IEC TR 63400 provides a more comprehensive description of the overall structure of the IEC SC 45A standards series and of its relationship with other standards bodies and standards.

NUCLEAR POWER PLANTS – INSTRUMENTATION AND CONTROL IMPORTANT TO SAFETY – GENERAL REQUIREMENTS FOR SYSTEMS

1 Scope

1.1 General

I&C systems important to safety may be implemented using hardwired equipment, programmable digital equipment such as processor-based or HDL-programmed devices, or by using a combination of several types of technologies. This International Standard provides requirements and recommendations for the overall I&C which may contain any combination of these technologies.

This standard highlights also the need for complete and precise requirements, derived from the plant safety goals, as a pre-requisite for generating the comprehensive requirements for the overall I&C, and hence for the individual I&C systems important to safety.

This standard introduces the concept of a safety lifecycle for the overall I&C including the I&C architecture, and a safety lifecycle for the individual systems. By this, it highlights the relations between the safety objectives of the NPP and the requirements for the architecture of the I&C systems important to safety, and the relations between the I&C architecture and the requirements of the individual systems important to safety.

Standards such as ISO/IEC/IEEE 15288 [24] provide an overarching concept of life cycle provisions covering product-related processes as well business development. The scope of IEC 61513 refers to safety aspects and their demonstration, and significantly deepens the considerations of ISO 15288 in this field.

The lifecycles illustrated in, and followed by, this standard are not the only ones possible; other lifecycles may be followed, provided that the objectives stated in this standard are satisfied.

NOTE The standard addresses the safety lifecycle of the overall I&C and of the individual systems. Although systems not important to safety are not in the scope of the standard, they have to be considered in the overall I&C safety lifecycle, as they may constitute constraints for the safety system design and qualification (e.g. installation in common rooms, interfaces, sizing of support systems, coordination of installation and commissioning works).

Furthermore, the standard does not describe the handling of interfaces between organizations (owner, architect engineer, engineering organizations, commissioning organizations). In practice, responsibilities for plans, activities and documents will be allocated according to the contractual arrangements.

1.2 Application: new and pre-existing plants

This standard applies to the I&C of new nuclear power plants as well as to I&C upgrading or back-fitting of existing plants.

For existing plants, only a subset of requirements is applicable depending on the scope of the project, and this subset should be identified at the beginning of any project.

1.3 Framework

The standard comprises four normative clauses (an overview is provided in Figure 1):

- Clause 5 addresses the overall I&C safety lifecycle:

- defining requirements for the I&C functions, and associated systems and equipment derived from the safety analysis of the NPP, the defence-in-depth and diversity concept of the NPP, the categorisation of I&C functions, and the plant lay-out and operational context;
- structuring the I&C architecture, dividing it into a number of systems and assigning the I&C functions to systems. Design criteria are identified, including those to give defence in depth and to minimize the potential for common cause failure (CCF);
- planning the I&C architecture.
- Clause 6 addresses the requirements for the individual I&C systems important to safety, particularly the requirements for systems built from programmable digital equipment. This includes differentiation of requirements according to the safety category of the I&C functions which are implemented (systems of class 1, 2 and 3);
- Clauses 7 and 8 address the overall integration, commissioning, operation and maintenance of the I&C systems.

NOTE Figure 1 outlines the structure of the standard. It does not necessarily present the timely order of activities which may be in reality partially executed in parallel, or include iterations.

Additionally, the standard provides informative annexes:

- Annex A highlights the relations between IAEA and basic safety concepts that are used throughout this standard;
- Annex B provides guidance to support comparison of this standard with parts 1, 2 and 4 of IEC 61508. This annex surveys the main requirements of IEC 61508 to verify that the issues relevant to safety are adequately addressed, considers the use of common terms and explains the reason for adopting different or complementary techniques or terms;
- Annex C provides a proposal for the documentation structure for overall I&C planning and I&C system design;
- Annex D indicates the main changes to be considered during the next update cycles of several SC45A standards to align them to this revision of IEC 61513.

149

5 Overall safety lifecycle: Requirements specification for the overall I&C	
5.2 Deriving the I&C requirements from the plant safety design base	5.3 Requirements on output documentation
5.2.2 Functional, performance and independence requirements 5.2.3 Categorisation requirements 5.2.4 Plant constraints	Overall requirements specification for the I&C systems important to safety

150

5 Overall safety lifecycle: Design and planning of the I&C architecture and assignment of the I&C functions to the individual I&C systems		
5.4 Requirements on the objectives	5.5 Requirements on the overall planning	5.6 Requirements on the documentation
5.4.2 Design of the I&C architecture 5.4.3 Assignment of the functions to the individual systems 5.4.4 Required analysis	5.5.2 O QA programs 5.5.3 O security planning 5.5.4..O I&C configuration management 5.5.5..Requirements management plan 5.5.6 O integration and commissioning plan 5.5.7 O operation plan 5.5.8 O maintenance plan	5.6.2 Architectural design 5.6.3 Functional assignment

151

6 System safety lifecycle: Realisation and planning of the individual I&C systems		
6.2 Requirements on the objectives of the system lifecycle phases	6.3 Requirements on the system planning	6.4 Requirements on output documentation
6.2.2 Requirements specification 6.2.3 Equipment selection & system specification 6.2.4 Detailed design & implementation 6.2.5 Integration 6.2.6 Validation 6.2.7 Installation 6.2.8 Modifications	6.3.2 S quality plan 6.3.3 S integration plan 6.3.4 S validation plan 6.3.5 S installation plan 6.3.6 S operation plan 6.3.7 S maintenance plan	6.4.2 Requirements specification 6.4.3 Specification 6.4.4 Detailed design 6.4.5 Integration 6.4.6 Validation 6.4.7 Modification
6.5.2 Requirements on system qualification	6.5 Qualification 6.5.3, 6.5.4 S Qualification plan	6.5.5 Requirements on qualification documents

152

7 Overall integration and commissioning	
7.2 Requirements on the objectives	7.3 Requirements on output documentation

153

8 Overall operation and maintenance	
8.2 Requirements on the objectives	8.3 Requirements on output documentation

154 **Key** QA: Quality Assurance; O: Overall; S: System

IEC 1895/11

Figure 1 – Overall framework of this standard**2 Normative references**

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

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

IEC 60709, *Nuclear power plants – Instrumentation, control and electrical power systems – Separation*

IEC/IEEE 60780-323, *Nuclear power plants – Electrical equipment important to safety – Qualification*

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

IEC 60964, *Nuclear power plants – Control rooms – Design*

IEC 60965, *Nuclear power plants – Control rooms – Supplementary control points for reactor shutdown without access to the main control room*

IEC/IEEE 60980-344, *Nuclear facilities - Equipment important to safety - Seismic qualification*

IEC 60987, *Nuclear power plants – Instrumentation and control important to safety – Hardware requirements*

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

IEC 61500, *Nuclear power plants – Instrumentation and control important to safety – Data communication in systems performing category A functions*

IEC 62003, *Nuclear power plants - Instrumentation, control and electrical power systems - Requirements for electromagnetic compatibility testing*

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

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

IEC 62566, *Nuclear power plants - Instrumentation and control important to safety - Development of HDL-programmed integrated circuits for systems performing category A functions*

IEC 62566-2, *Nuclear power plants - Instrumentation and control systems important to safety - Development of HDL-programmed integrated circuits - Part 2: HDL-programmed integrated circuits for systems performing category B or C functions*

190 IEC 62645, *Nuclear power plants - Instrumentation, control and electrical power systems -*
191 *Cybersecurity requirements*

192 IEC 62671, *Nuclear power plants - Instrumentation and control important to safety - Selection*
193 *and use of industrial digital devices of limited functionality*

194 IEC 62859, *Nuclear power plants - Instrumentation and control systems - Requirements for*
195 *coordinating safety and cybersecurity*

196 IEC 62988, *Nuclear power plants - Instrumentation and control systems important to safety -*
197 *Selection and use of wireless devices*

198 IEC 63351(FDIS), *Nuclear Facilities - Human Factors Engineering - Application to the Design*
199 *of Human Machine Interfaces*

200 IAEA *Fundamental Safety Principles – Safety Fundamentals No. SF-1*

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

202 IAEA GS-G-3.5, *The Management System for Nuclear Installations*

203 IAEA GSR Part 2, *Leadership and Management for Safety – General Safety Requirements*

204 IAEA GS-G-3.1, *Application of the Management System for Facilities and Activities – Safety*
205 *Guide*

206 IAEA SSG-39, *Design of Instrumentation and Control Systems for Nuclear Power Plants –*
207 *Specific Safety Guide*

208 **3 Terms and definitions**

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

210 **3.1**

211 **application function**

212 function of an I&C system that performs a task related to the process being controlled rather
213 than to the functioning of the system itself

214 NOTE 1 See also “I&C function”, “I&C system”, “application software”, “service function”.

215 NOTE 2 An application function is normally a subfunction of an I&C function.

216 **3.2**

217 **application software**

218 software complementing the system software of a system, as needed to implement its
219 application and service functions.

220 NOTE 1 The distinction between system software (generic, re-usable) and application software (typically plant-
221 specific) is generally made to minimize duplication of code and to optimize the allocation of the qualification
222 activities. It is an especially useful distinction when using an I&C platform.

223 NOTE 2 See also “system software”, “application function”, “service function”.

224 **3.3**

225 **application software library**

226 collection of software modules with typical functionality suitable to create application software

227 NOTE 1 When using pre-existing equipment, such a library is considered to be part of the system software and
228 qualified as such.

229 NOTE 2 See also Figure 2.

230 3.4

231 category of an I&C function

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

235 NOTE 1 See also “class of an I&C system”, “I&C function”.

236 NOTE 2 IEC 61226 defines categories of I&C functions. To each category there corresponds a set of
237 requirements applicable on both the I&C function (concerning its specification, design, implementation, verification
238 and validation) and the whole the I&C chain (concerning the properties and the related qualification). The
239 requirements are regardless of how the items of the I&C chain are distributed in a number of interconnected I&C
240 systems. For more clarity, this standard defines categories of I&C functions and classes of I&C systems and
241 establishes a relation between the category of the function and the minimal required class for the associated
242 systems and equipment.

243 3.5

244 channel

245 an arrangement of interconnected components within a system that initiates a single output.

246 NOTE A channel loses its identity where the single-output signals are combined with signals from another channel
247 (e.g., from a monitoring channel or a safety actuation channel).

248 [IAEA Safety Glossary, 2022 Edition]

249 3.6

250 class of an I&C system

251 one of three possible assignments (1, 2, 3) of I&C systems important to safety resulting from
252 consideration of their requirement to implement I&C functions of different safety importance.
253 An unclassified assignment is made if the I&C system does not implement functions important
254 to safety

255 NOTE See also “category of an I&C function”, “items important to safety”, “safety systems”.

256 3.7

257 commissioning

258 the process by means of which systems and components of facilities and activities, having
259 been constructed, are made operational and verified to be in accordance with the design and
260 to have met the required performance criteria

261 [IAEA Safety Glossary, 2022 Edition]

262 NOTE Commissioning is typically structured in subsequent steps and according to disciplines: commissioning of
263 I&C systems and of electrical systems, non-nuclear commissioning of process systems, commissioning of
264 interconnected plant systems, nuclear commissioning. All steps contribute to the qualification of the I&C systems.

265 3.8

266 common cause failure

267 CCF

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

270 [IAEA Safety Glossary 2022 Edition]

271 NOTE 1 Common causes can be internal or external to an I&C system.

272 NOTE 2 The IEC definition differs from the IAEA definition: The term “specific” was deleted because otherwise the
273 definition of CCF is not consistent with the definition of CMF “Common mode failure”. Furthermore, this additional
274 word is not necessary in order to understand the definition.

275 **3.9**
276 **complexity**
277 degree to which a system or component has a design, implementation or behaviour that is
278 difficult to understand and verify

279 [ISO/IEC/IEEE 24765, modified]

280 **3.10**
281 **component**
282 one of the parts that make up a system. A component can be hardware, computer programs
283 and configuration data, and may be subdivided into other components

284 [ISO/IEC/IEEE 24765, modified]

285 NOTE 1 See also “I&C system”, “equipment”.

286 NOTE 2 The terms “equipment”, “component”, and “module” are often used interchangeably. The relationship of
287 these terms is not yet standardised.

288 NOTE 3 This IEC/SC 45A definition is in principle compatible with the sub-definition of “Component” given in the
289 frame of the 2022 edition of the IAEA Safety Glossary definition of “Structures Systems and Components (SCC)”.
290 Nevertheless, as only examples of hardware components are given, this can mislead the reader and IEC/SC 45A
291 prefer to use a definition which explicitly covers software components.

292 **3.11**
293 **configuration management**
294 the process of identifying and documenting the characteristics of a facility’s structures,
295 systems and components (including programmable digital items, software and configuration
296 data), and of ensuring that changes to these characteristics are properly developed,
297 assessed, approved, issued, implemented, verified, recorded and incorporated into the facility
298 documentation

299 [IAEA Safety Glossary, 2022 Edition]

300 **3.12**
301 **constraint**
302 externally imposed limitation on the system, its design, or implementation or on the process
303 used to develop or modify a system

304 NOTE 1 A constraint is a factor that is imposed on the solution by force or compulsion and may limit or modify the
305 design.

306 [ISO/IEC/IEEE 29148:2018]

307 **3.13**
308 **data**
309 representation of information or instructions in a manner suitable for communication,
310 interpretation, or processing by computers

311 [ISO/IEC/IEEE 24765, modified]

312 **3.14**
313 **defence-in-depth**
314 a hierarchical deployment of different levels of diverse equipment and procedures to prevent
315 the escalation of anticipated operational occurrences and to maintain the effectiveness of
316 physical barriers placed between a radiation source or radioactive material and workers,
317 members of the public or the environment, in operational states and, for some barriers, in
318 accident conditions

319 [IAEA Safety Glossary, 2022 Edition]

320 NOTE See also Clause A.3.

321 3.15

322 dependability

323 a general term describing the overall trustworthiness of a system; that is, the extent to which
324 reliance can justifiably be placed on this system. Reliability, availability and safety are
325 attributes of dependability

326 [IAEA Safety Glossary, 2022 Edition]

327 3.16

328 design basis

329 The range of conditions and events taken explicitly into account in the design of structures,
330 systems and components and equipment of a facility, according to established criteria, such
331 that the facility can withstand them without exceeding authorized limits.

332 [IAEA Safety Glossary, 2022 Edition]

333 3.17

334 diversity

335 presence of two or more independent (redundant) systems or components to perform an
336 identified function, where the different systems or components have different attributes so as
337 to reduce the possibility of common cause failure, including common mode failure

338 [IAEA Safety Glossary, 2022 Edition]

339 NOTE 1 When “Diversity” is used with an additional attribute, the term diversity indicates the general meaning
340 “Existence of two or more different ways or means of achieving a specified objective”, where the attribute indicates
341 the characteristics of the different ways applied, e.g. functional diversity, equipment diversity, signal diversity. The
342 most common terms describing diversity approaches are listed below (based on IAEA SSG-39 §6.60). The terms
343 are not perfectly homogeneous; for example, “Signal diversity” and “Logic diversity” are typical attributes of “design
344 diversity”:

- 345 • “Design diversity” refers to using different design approaches to solve the same problem or a similar
346 problem;
- 347 • “Equipment diversity” refers to using hardware with significantly different characteristics (e.g. analogue
348 equipment versus digital equipment);
- 349 • “Functional diversity” refers to using systems that take different actions to reach the same outcome;
- 350 • “Signal diversity” refers to initiating an action by different plant parameters;
- 351 • “Logic diversity” refers to the use of different software or hardware description languages, different
352 algorithms, different timings of logical functions, or different sequencing of logical functions.
- 353 • “Diversity in the development process” refers to crediting differences in the structure and subdivision of
354 activities, including differences in the organization, such as the use of different design and development
355 teams and different implementation and testing teams

356 NOTE 2 Currently, the definition of “functional diversity” given in IEC 60880 and IEC 62340 corresponds to “signal
357 diversity”; the definition of functional diversity in the IAEA glossary 2022 provides examples of signal diversity. This
358 inconsistency needs to be corrected.

359 3.18

360 equipment

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

363 NOTE 1 See also “component”, “I&C system”.

364 NOTE 2 Equipment can be a programmable digital item and include software and configuration data.

365 NOTE 3 The terms “equipment”, “component”, and “module” are often used interchangeably. The relationship of
366 these terms is not yet standardised.

NOTE 4 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.

3.19

equipment family (equipment platform, I&C platform)

set of programmable digital components that may work co-operatively in one or more defined architectures (configurations). The development of plant specific configurations and of the related application software and configuration data may be supported by software tools. An equipment family usually provides a number of standard functionalities (e.g. application functions library) that may be combined to generate specific application software and configuration data

NOTE 1 See also "functionality", "application software", "application software library".

NOTE 2 An equipment family can be a product of a defined manufacturer or a set of products interconnected and adapted by a supplier.

NOTE 3 The terms "equipment platform" and "I&C platform" is sometimes used as a synonym of "equipment family".

3.20

equipment qualification

generation and maintenance of evidence to ensure that equipment will operate on demand, under specified service conditions, to meet system performance requirements

[IAEA Safety Glossary, 2022 Edition]

NOTE The definition is wider than that in IEC/IEEE 60780-323:2016 which has been taken from the IAEA safety glossary 2007 and which refers to "specific" service conditions.

3.21

error

discrepancy between a computed, observed or measured value or condition and the true, specified or theoretical value or condition

NOTE See Figure 3.

3.22

failure

loss of the ability of a structure, system or component to function within acceptance criteria

[IAEA Safety Glossary edition 2022]

NOTE 1 Equipment is considered to fail when it becomes incapable of functioning, whether or not it is needed at that time. A failure in, for example, a backup system may not be manifest until the system is called upon to function, either during testing or on failure of the system it is backing up.

NOTE 2 A failure is the result of a hardware fault, systematic fault, system fault, operator or maintenance error, and the associated signal trajectory which results in the failure.

NOTE 3 See also "fault", "systematic failure".

3.23

fault

defect in a hardware, software or system component

NOTE 1 See also Figure 3.

NOTE 2 A fault in a system can be due to a random failure of a system component, that results e.g. from hardware degradation due to ageing. It can also be a systematic fault, e.g. a software fault, which results from design errors.

NOTE 3 A fault (notably a design fault) can remain undetected in a system until specific conditions are such that the result produced does not conform to the intended function, i.e. a failure of the system occurs.

414 **3.24**
415 **functional verification**
416 check of the correctness of the application functions specifications against the top level plant
417 functional and performance requirements.

418 NOTE It is complementary to the validation testing that verifies the compliance of the system with the functions
419 specification.

420 **3.25**
421 **functionality**
422 attribute of a function which defines the operations which transform input information into
423 output information

424 NOTE Functionality of application functions generally affect the plant operation. Input can be obtained from
425 sensors, operators, other equipment, or from other software. Outputs can be directed to actuators, operators, other
426 equipment, or other software (see IEC 61508-2).

427 **3.26**
428 **hardware description language, HDL**
429 language used to formally describe the functions and/or the structure of an electronic
430 component for documentation, simulation or synthesis

431 [IEC 62566:2012, 3.6]

432 **3.27**
433 **hardwired item (device, equipment, system)**
434 item that relies on relays, on analogue electronic or on discrete digital logic

435 [IEC 60987:2021, 3.10]

436 **3.28**
437 **HDL-programmed device, HPD**
438 integrated circuit configured specifically for NPP I&C systems using Hardware Description
439 Languages and related software tools

440 [IEC 62566:2012, 3.6, modified]

441 **3.29**
442 **hazard**
443 event having the potential to cause injury to plant personnel or damage to components,
444 equipment or structures. Hazards are divided into internal hazards and external hazards

445 NOTE 1 Internal hazards are, for example, fire and flooding. Internal hazards can be also a consequence of a PIE
446 (for example, loss of coolant accident, steam-line break).

447 NOTE 2 External hazards are, for example, earthquake and lightning.

448 **3.30**
449 **human error**
450 discrepancy between the human action taken or omitted, and that intended or required

451 [IEV 192-03-14; IEC 63351]

452 **3.31**
453 **I&C architecture**
454 organisational structure of the I&C systems of the plant which are important to safety

455 NOTE 1 The organisational structure defines notably the main functions, class and boundaries of each system,
456 the interconnections and independence between systems, the priority and voting between concurrently acting
457 signals, the HMI.

458 NOTE 2 In this standard the term designates only a subset of the whole I&C architecture of the plant. The latter
459 includes also the unclassified systems and equipment.

460 NOTE 3 The terms “I&C architecture” and “overall architecture of the I&C systems important to safety” are
461 equivalent.

462 NOTE 4 For the individual I&C system, the term “system architecture” is used.

463 3.32

464 I&C chain

465 Set of elements involved in an I&C function, from sensors or manual commands to the
466 generation of the actuation signal or to displays in human machine interfaces.

467 NOTE 1 I&C chains can be assigned to layers, and comprise the following elements which all contribute to the
468 I&C function:

- 469 • Sensor(s): this part includes the probes or probes with transmitters (layer 0);
- 470 • Conditioning of sensor signals as well as their distribution to different I&C systems (layer 1);
- 471 • Actuator control / I&C portion of the actuators (layer 1 as well);
- 472 • Processing of conditioned signals, of manual command signal, generation of orders and transmission to the
473 actuators or indicators (layer 2);
- 474 • Human-machine interface equipment (layer 3);
- 475 • Cables, connectors, penetrations, junction boxes

476 The set of elements depends on project-specific rules which ensure that all parts involved in I&C functions are
477 properly addressed in analysis and qualification, even when they are at the boundaries between disciplines such as
478 “actuators” which have aspects in process, electrical and I&C engineering or sensing lines and thermowells that
479 need to be addressed by I&C and process engineering as well.

480 NOTE 2 Different to a “channel”, an I&C chain does not lose its identity even if it includes processing equipment
481 which accommodates several functions.

482 3.33

483 I&C function

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

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

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

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

492 3.34

493 I&C project organisation

494 organisation(s) or individuals that have responsibility during the phases of the overall I&C
495 safety lifecycle and/or during the phases of the safety lifecycles of the I&C systems, to define
496 and perform all management and technical activities concerning the I&C functions, systems
497 and equipment important to safety

498 NOTE This term is to be contrasted with “operating organisation”.

499 3.35

500 I&C system

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

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

508 NOTE 2 The elements included in a specific I&C system are defined in the specification of the boundaries of the
509 system.

510 NOTE 3 According to their typical functionality, IAEA distinguishes between automation / control systems, HMI
511 systems, interlock systems and protection systems.

512 NOTE 4 See also "system" and "I&C function".

513 3.36

514 independent equipment (independent systems, independent subsystems)

515 equipment that possesses both of the following characteristics:

516 1) the ability to perform its required function is unaffected by the operation or failure of other
517 equipment;

518 2) the ability to perform its function is unaffected by the occurrence of the effects resulting
519 from the postulated initiating event for which it is required to function

520 [IAEA Safety Glossary, 2022 Edition]

521 NOTE Means to achieve independence in the design are actuation priority, electrical isolation (also called
522 functional isolation in IAEA documents), physical separation and communications independence.

523 3.37

524 interrupt

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

526 [ISO/IEC/IEEE 24765]

527 3.38

528 item important to safety

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

531 NOTE 1 Items important to safety include:

532 a) those structures, systems and components whose malfunction or failure could lead to undue radiation
533 exposure of the site personnel or members of the public;

534 b) those structures, systems and components that prevent anticipated operational occurrences from leading to
535 accident conditions;

536 c) safety features for design extension conditions;

537 d) those features that are provided to mitigate the consequences of malfunction or failure of structures,
538 systems or components.

539 [IAEA Safety Glossary, 2022 Edition]

540 NOTE 2 This definition is intended to encompass all aspects of nuclear safety and addresses equipment and
541 systems performing functions of categories A, B and C according to IEC 61226.

542 NOTE 3 In this standard, the items considered will be mainly I&C systems or I&C functions.

543 3.39 operational system software

544 that part of system software which is running on the target processor during operation, such as: input/output
545 drivers and services, interrupt management, scheduler, communication drivers, application oriented libraries, on-
546 line diagnostics, redundancy and graceful degradation management

547 [IEC 62138:2018, 3.30, modified]

3.40**overall I&C**

the set of overarching planning, coordination and design activities for all I&C systems and I&C equipment for a NPP project, including identification of the requirements and constraints from the plant design base, specification of the I&C architecture and of all overarching design principles, engineering, testing and other qualification methods

NOTE "Overall I&C" comprises activities related to I&C systems and equipment important to safety as well as I&C not important to safety. The overall I&C safety life cycle is embedded in the overall I&C activities.

3.41**overall I&C safety lifecycle**

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

[IEC 61508-4:CD 2022-11, 3.7.1, modified]

NOTE 1 The overall safety lifecycle of the I&C induces requirements for the individual system safety lifecycles.

NOTE 2 See also "system safety lifecycle".

3.42**postulated initiating event****PIE**

a postulated event identified in design as capable of leading to anticipated operational occurrences or accident conditions

[IAEA Safety Glossary, 2022 Edition]

3.43**pre-existing items**

hard- or software or programmable digital equipment that already exists, is available as a commercial or proprietary product, and is being considered for use

NOTE This definition includes that of pre-developed software, see IEC 60880

3.44**programmable digital item**

item that relies on software instructions or programmable logic to accomplish a function

NOTE Item" may be taken as system, equipment, device, module.

3.45**provision**

expression in the content of a normative document that takes the form of a statement, an instruction, a recommendation or a requirement

NOTE These types of provision are distinguished by the form of wording they employ; e.g. instructions are expressed in the imperative mood, recommendations by the use of the auxiliary "should" and requirements by the use of the auxiliary "shall".

[ISO/IEC Guide 2:2004, 7.1]

3.46**quality**

degree to which a set of inherent characteristics fulfils requirements

[ISO 9000:2015] [7]

592 **3.47**
593 **quality assurance**
594 the function of a management system that provides confidence that specified requirements
595 will be fulfilled

596 [IAEA Safety Glossary, 2022 Edition]

597 **3.48**
598 **quality plan**
599 specification of the actions and associated resources to be applied to a specific object

600 [ISO 10005:2018]

601 NOTE In some IEC SC45 standards also the term “quality assurance plan” is used as a synonym.

602 **3.49**
603 **redundancy**
604 provision of alternative (identical or diverse) structures, systems and components, so that any
605 single structure, system or component can perform the required function regardless of the
606 state of operation or failure of any other

607 [IAEA Safety Glossary, 2022 Edition]

608 **3.50**
609 **reliability**
610 the probability that a system or component or an item will meet its minimum performance
611 requirements when called upon to do so for a specified period of time and under stated
612 operating conditions

613 [IAEA Safety Glossary, 2022 Edition]

614 **3.51**
615 **requirement**
616 statement which translates or expresses a need and its associated constraints and conditions

617 NOTE 1 Requirements exist at different levels in the system structure.

618 NOTE 2 A requirement is an expression of one or more particular needs in a very specific, precise and
619 unambiguous manner.

620 NOTE 3: A requirement always relates to a system, software or service, or other item of interest.

621 [ISO/IEC/IEEE 29148:2018]

622 NOTE 4 In IEC/SC 45A documents the following types of requirements are distinguished:

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

626 *Functional and performance requirements* – Functional requirements state the actions to be taken by the
627 system in response to specific signals or conditions, and performance requirements define features such as
628 response times and accuracy.

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

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

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

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

637 NOTE 5 The IAEA Safety Glossary, Edition 2022 contains the following definition:

638 *requirement (safety)* – that which is established or required by the Fundamental Safety Principles (IAEA Safety
639 Fundamentals) or IAEA Safety Requirements publications or by (national or international) laws or regulations.

640 This IAEA definition is useful in the framework of IAEA publications, but too narrow for use in a technical standard.
641 It corresponds to the IEC/SC 45A definition “Safety requirement” as provided in Note 4.

642 3.52

643 reusable software

644 software module that can be used in more than one computer program or software system

645 [ISO/IEC/IEEE 24765, modified]

646 3.53

647 safety function

648 a specific purpose that must be accomplished for safety for a facility or activity to prevent or
649 to mitigate radiological consequences of normal operation, anticipated operational
650 occurrences and accident conditions

651 [IAEA Safety Glossary, 2022 Edition]

652 3.54

653 safety group

654 the assembly of equipment designated to perform all actions required for a particular initiating
655 event to ensure that the limits specified in the design basis for anticipated operational
656 occurrences and design basis accidents are not exceeded

657 [IAEA Safety Glossary, 2022 Edition]

658 NOTE One way to manage the relation of several functions to a single PIE (this is a “safety group”) is by having in
659 the functional requirements documents the identification of the events to which the function contributes, without
660 having an additional explicit sorting of functions according to PIEs.

661 3.55

662 safety requirement

663 requirement imposed by authorities (legal, regulatory or standards bodies) and design
664 organizations on the safety of the NPP in terms of impact on individuals, society and
665 environment during the NPP lifecycle

666 NOTE The IAEA Safety Glossary, Edition 2022 contains the following definition:

667 *requirement (safety)* – that which is established or required by the Fundamental Safety Principles (IAEA Safety
668 Fundamentals) or IAEA Safety Requirements publications or by (national or international) laws or regulations.

669 This IAEA definition is useful in the framework of IAEA publications, but too narrow for use in a technical standard.
670 It corresponds to the IEC/SC 45A definition “Safety requirement” as provided in Note 4.

671 3.56

672 safety system

673 a system important to safety, provided to ensure the safe shutdown of the reactor or the
674 residual heat removal from the core, or to limit the consequences of anticipated operational
675 occurrences and design basis accidents

676 [IAEA Safety Glossary, 2022 Edition]

677 NOTE The standard addresses systems performing functions categorized A, B and C according to IEC 61513.

678 **3.57**
679 **security**
680 capability of the programmable digital system to protect information and data so that
681 unauthorized persons or systems cannot read or modify relevant data or perform or inhibit
682 control actions, and authorized persons or systems are not denied access

683 [ISO/IEC 24765:2017, 3.3653 / 5., modified]

684 **3.58**
685 **self-supervision**
686 automatic testing of system hardware and of the integrity of software and configuration data of
687 a programmable digital item

688 [IEC 60671:2007, modified]

689 **3.59**
690 **service function**
691 function of an I&C system related to the functioning of the system itself, such as configuration,
692 commissioning, periodic testing, self-supervision, maintenance, modification and security

693 **3.60**
694 **single failure**
695 loss of capability of a component to perform its intended safety function(s), and any
696 consequential failure(s) which result from it

697 [IAEA Safety Glossary, 2022 Edition, modified]

698 NOTE This definition differs from the 2022 edition of the IAEA Safety Glossary which is "A failure which results in
699 the loss of capability of a system or component to perform its intended safety function(s), and any consequential
700 failure(s) which result from it". The term "system" was suppressed because the original IAEA definition for single
701 failure was deemed inadequate by IEC/SC 45A experts in that it must result in the loss of system function. Systems
702 that meet the single failure criterion would therefore have no single failures. It seems that this could lead to circular
703 arguments regarding compliance with the single failure criteria. The definition is aligned with the definition of
704 "failure".

705 **3.61**
706 **single failure criterion**
707 a criterion (or a requirement) applied to a system such that it must be capable of performing
708 its task in the presence of any single failure

709 [IAEA Safety Glossary, 2022 Edition]

710 NOTE See e.g. requirement 25 of IAEA SSR-2/1, for guidance how the single failure criterion is achieved and how
711 it is applied to a safety group.

712 **3.62**
713 **software**
714 programs (i.e. sets of ordered instructions), data, rules and any associated documentation
715 pertaining to the operation of a computer-based I&C system

716 NOTE The term is reserved for CPU / processor based technology. Interconnection information and other
717 configuration data representing the implementation of an application in HDL-programmed devices are not included.

718 **3.63**
719 **specification**
720 document that specifies, in a complete, precise, verifiable manner, the requirements, design,
721 behaviour or other characteristics of a system or component and, often, the procedures for
722 determining whether these provisions have been satisfied

723 [IEC 60880:202x, 3.39]

724 **3.64**
725 **system**
726 a set of components which interact according to a design so as to perform a specific (active)
727 function, and where an element of a system can be another system, called a subsystem

728 [IAEA Safety Glossary, 2022 Edition, modified]

729 NOTE 1 See also “I&C system”.

730 NOTE 2 I&C systems are distinguished from mechanical systems and electrical systems of the NPP.

731 NOTE 3 The IAEA definition use a subordinate clause with ambiguous relationship to the nouns in the main
732 clause. This grammatical ambiguity is avoided in the proposed definition.

733 **3.65**
734 **system architecture**
735 organisational structure of an I&C system

736 NOTE See also “I&C architecture”.

737 **3.66**
738 **system qualification**
739 process of determining whether a system is suitable for operational use, by examination and
740 provision of other evidence that the system fulfils in its entirety the requirement specification
741 as intended (functionality, response time, fault tolerance, robustness etc.)

742 NOTE 1 The qualification requirements are derived from the specific class of the I&C system and a specific
743 application context.

744 NOTE 2 I&C systems are typically implemented on the basis of interacting sets of equipment. Such equipment
745 may be developed as part of the project, or it may be pre-existing equipment (i.e. developed in the framework of a
746 previous project, being a commercial off-the-shelf product or an equipment family). Typically, qualification of an
747 “I&C system” is accomplished in stages: first by the qualification of individual pre-existing equipment (usually early
748 in the system realization process); in a second step by the qualification of the integrated I&C system (i.e. the final
749 realized design).

750 NOTE 3 Qualification of I&C systems is always a plant- and application-specific activity. However, it may rely to a
751 large degree on qualification activities performed outside the framework of a specific plant design (these are called
752 “generic qualification” or “pre-qualification”). Pre-qualification may reduce the plant-specific qualification effort
753 significantly, however, the application-specific qualification requirements should still be shown to be met.

754 NOTE 4 The definition is consistent with the definition of “qualification” and “system validation” given in IAEA
755 safety glossary 2022, restricted to the case of an I&C system.

756 **3.67**
757 **system safety lifecycle**
758 necessary activities involved in the implementation of an I&C system important to safety
759 occurring during a period of time that starts at a concept phase with the system requirements
760 specification and finishes when the I&C system is no longer available for use

761 NOTE 1 The system safety lifecycle refers to the activities of the overall I&C safety lifecycle.

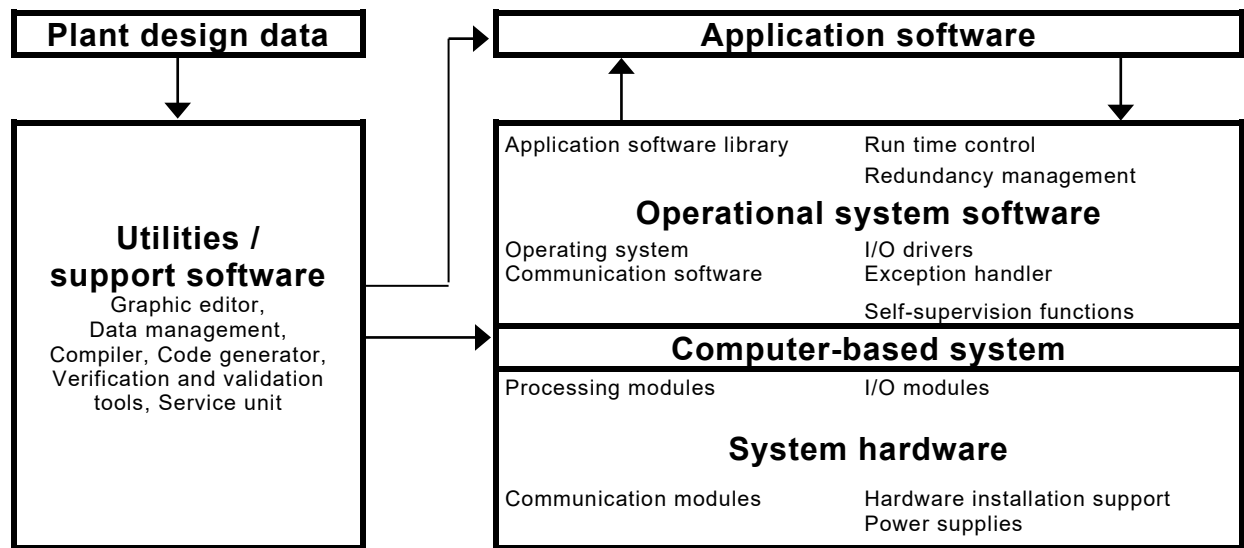
762 NOTE 2 See also “overall I&C safety lifecycle”.

763 **3.68**
764 **system software**
765 software designed for a specific computer system or family of computer systems to facilitate
766 the operation and maintenance of the computer system and associated programs, for
767 example, operational system software and utilities.

768 NOTE 1 Utilities, also called support software, comprise software that aids in the development, test, or
769 maintenance of other software and of the system such as translators, graphic editors, diagnostics tools, test and
770 simulation tools,

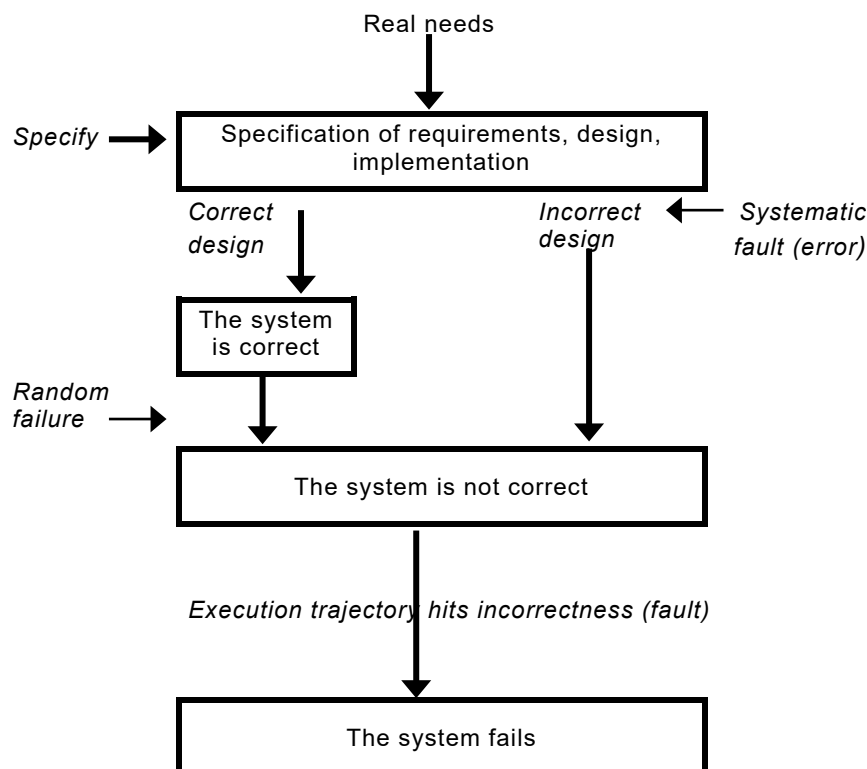
771 NOTE 2 See also “operational system software”, “application software”.

- 772 **3.69**
773 **systematic fault**
774 fault related in a deterministic way to a certain cause, which can only be eliminated by a
775 modification of the design or of the manufacturing process, operational procedures, documen-
776 tation or other relevant factors
- 777 [IEC 61508-4 (CD 2022-11), 3.6.6, modified]
- 778 **3.70**
779 **systematic failure**
780 system failure due to the activation of a systematic fault
- 781 NOTE 1 Software failures are typical examples of systematic failures, since software consists solely of design and
782 does not wear out or suffer from physical failure. Since the triggers which activate software faults are encountered
783 at random during system operation, software failures also occur randomly.
- 784 NOTE 2 See also “failure”, “fault”.
- 785 **3.71**
786 **type test(s)**
787 conformity test subjecting one or more items representative of the production to a series of
788 tests with the equipment functioning in a state and mounting representative of its intended
789 use in actual operation (including any software and representative configuration data)
- 790 [IAEA Safety Glossary, 2022 Edition, modified considering Clause 6.1.1 of IEC/ IEEE 60780-
791 323:2016]
- 792 **3.72**
793 **verification**
794 confirmation by examination and by means of objective evidence that specified objectives
795 have been met and specified requirements for specific results have been fulfilled
- 796 NOTE 1 Verification indicates the assessment of the results of an individual activity against its inputs.
- 797 NOTE 2 Verification may comprise activities such as: performing alternative calculations; comparing a new design
798 specification with a similar proven specification; undertaking tests and demonstrations; and reviewing documents
799 prior to issue.
- 800 NOTE 3 The corresponding status is termed ‘verified’.
- 801 [IAEA Safety Glossary, 2022 Edition, definition 2]
- 802 **3.73**
803 **validation testing**
804 testing of an integrated I&C system to demonstrate its compliance with the functional,
805 performance and interface requirements
- 806 NOTE In the versions of IEC 60880, 62138, 62566 published before IEC 61513 Ed3, “system validation” is used
807 instead of “validation testing”.
- 808



IEC 1896/11

Figure 2 – Typical relations of hardware and software in a computer-based system



IEC 1897/11

Figure 3 – Relations between system failure, random failure and systematic fault

4 Symbols and abbreviations

ASIC	Application-specific integrated circuit
CB	Computer-based
CCF	Common-cause failure
CM	Configuration management
COTS	Commercial off-the-shelf
DiD	Defence in Depth
EMI	Electromagnetic interference
FPGA	Field-programmable gate array
HDL	Hardware description language
HMI	Human machine interface
HPD	HDL-programmed device
HVAC	Heating, Ventilation and Air Conditioning
I&C	Instrumentation and control
I/O	Input/output
NPP	Nuclear power plant
PDIP	Pre-developed I&C package
PIE	Postulated initiating events
PSA	Probabilistic Safety Assessment
QA	Quality assurance

5 Overall I&C safety lifecycle

5.1 General

The objective of this clause is to define how to

- derive the requirements for the overall I&C from the safety design base of the NPP (see Clauses A.1 and A.2), and
- derive the requirements for the individual I&C systems important to safety from these overall requirements.

To ensure that all the plant safety requirements to be met by the I&C are captured, implemented, and maintained, a systematic approach is required. This is achieved by placing the activities associated with development, implementation and operation of I&C in the framework of a safety lifecycle of the overall I&C. This lifecycle refers in turn to the safety lifecycles of the individual I&C systems (see Clause 6).

NOTE Different lifecycles than the presented one may be followed, provided that the objectives of the standard are satisfied, see Clause 1.1.

5.1.1 Starting point

The overall I&C safety lifecycle starts with deriving I&C requirements from the plant safety design base. Some of the requirements, such as the collection of the functional requirements, can only be prepared if a minimum of boundary conditions and constraints have been defined already as part of the safety design base of the plant, especially (see Clause 5.2.4):

- a preliminary I&C architecture, with an anticipated number of defence levels envisaged in the overall I&C, including the safety class defined for every system;

- the technological choices for the human-machine interface systems (technology of the main HMI equipment in the main control room, in the remote shut down station, extent of local control stations...). This could be e.g. fully computerized main and backup HMI, a mix of computerized and analog technology.
- role of main control room and supplementary control room including their locations and classification principles;
- a preliminary building layout, with allocated space in building and an initial power supply and HVAC system capacities;
- preliminary provisions for cable ways.

The safety lifecycle is presented without making these preliminary design activities explicit, although they could be the result of design iterations between overall plant design, system design, layout design and I&C taking significant time, especially in a new reactor type development. The lifecycle in this standard is presented assuming that these iterations have converged, and the constraints and requirements of the plant safety design base regarding overall I&C are stable and sufficiently mature. Still, it is assumed that maturity loops for the requirements from the safety design base and the plant constraints are ongoing during the execution of the overall I&C safety lifecycle and the I&C system safety lifecycles.

Starting point for the activities of the overall I&C safety lifecycle and the safety lifecycles of the individual I&C systems is that an overall I&C project organisation has been set up that will be in charge of the I&C project including planning, execution and interfacing to the other disciplines of the NPP project. Requirements on the plans are specified in Clauses 5.5 and 6.3.

5.1.2 Scope of the overall I&C safety lifecycle

The phases of a typical overall I&C safety lifecycle include

- a) review of the plant safety design base including (see 5.2):
 - functional, performance and independence requirements;
 - functional categorisation;
 - constraints from the plant design framework;
- b) definition of the overall requirements specification of the I&C functions, I&C systems and I&C equipment important to safety (see 5.3);
- c) design of the I&C architecture and assignment of the I&C functions to individual systems and equipment (see 5.4);
- d) definition of the overall planning (see 5.5);
- e) realisation of the individual systems (see Clause 6);
- f) overall integration and commissioning of the systems (see Clause 7);
- g) overall operation and maintenance (see Clause 8).

Numbers in brackets identify the clause and subclause of this standard where the relevant phase is addressed, while the objective, inputs to, outputs from, and scope of each phase are developed in Table 1.

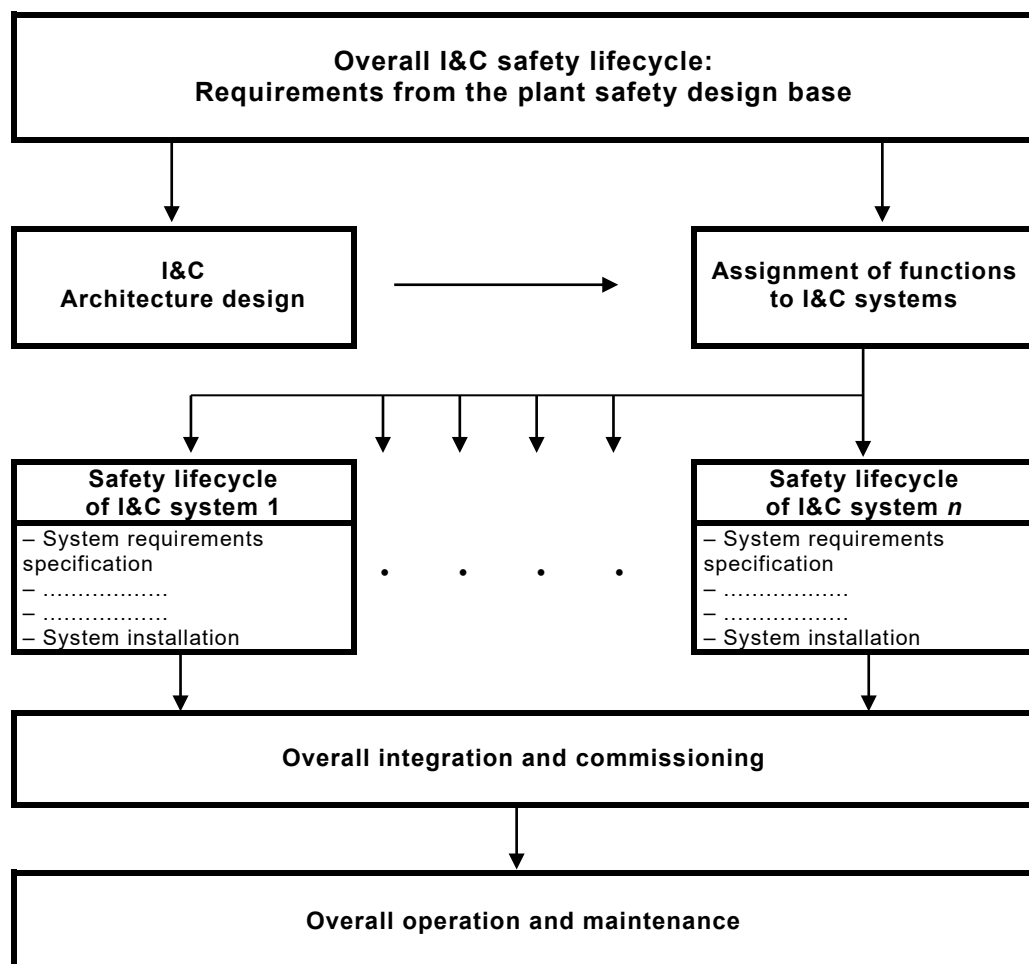
The connections between this lifecycle and the safety lifecycles of the individual I&C systems are shown in simplified form in Figure 4. The following applies:

5.1.2.1 The overall I&C safety lifecycle is an iterative process where the outputs of each phase shall be verified as being consistent with the inputs from the preceding activities. A phase may start even if the activities of the preceding phase are not finished providing that adequate configuration controls have been applied which ensure that the overall consistency of the development process is maintained;

5.1.2.2 A phase shall only be declared finished if the preceding phases have been completed.

NOTE 1 Starting a phase if the preceding phase is not finished implies a trade-off between scheduling constraints and the risk for / need of re-work. Risk for rework depends on the number of decoupling assumptions that may be made regarding plant constraints, functional requirements and maturity of the design of process systems.

NOTE 2 Completion of a phase could be with remaining open points items judged to have no significant impact and scheduled for closure via the overall I&C configuration management processes.



IEC 1898/11

Figure 4 – Connections between the overall I&C safety lifecycle and the safety lifecycles of the individual I&C systems

Table 1 – Overview of the overall I&C safety lifecycle

Clause or subclause	Inputs	Objectives of the activity	Scope	Outputs
5 Requirements placed upon the overall I&C safety lifecycle and its relationship to the systems' lifecycles				
<i>5.2 Deriving the I&C requirements from the plant safety design base</i>				
5.2.2 Review of the functional, performance and independence requirements	Plant safety design base documents Principles of plant operation	To identify – the overall functional and performance requirements of the I&C systems important to safety, – the defence in-depth concept of the plant and the independence requirements placed upon the I&C functions, – the automatic functions and operator task	Plant systems and related I&C systems important to safety	Identification of input requirements for 5.3
5.2.3 Review of the categorisation requirements	Plant safety categorisation	To identify the categorisation of I&C functions To verify for completeness To verify for feasibility of complex requirements	I&C functions important to safety	Identification of input requirements for 5.3
5.2.4 Review of plant constraints	Plant lay-out documents and design data base	To identify – plant/I&C systems boundaries, – constraints from support systems and plant layout, environmental conditions, – sources of potential internal and external hazards, – principles of plant operation and maintenance	Plant layout Plant systems I&C systems	Identification of constraints for the I&C architecture design (see 5.4) and for the requirements specification of the individual I&C systems (see 6.2)
5.3 Output documentation	Outputs of 5.2	To develop the overall requirements specification of the I&C systems important to safety in terms of functional, performance, independence and categorisation requirements	I&C systems	Overall I&C requirements specification for 5.4
<i>5.4 Design of the overall I&C architecture and assignment of the I&C functions</i>				
5.4.2 Design of the I&C architecture	Output of 5.3	To design the I&C architecture suitable to implement the overall requirements specifications of the I&C systems important to safety To provide adequate measures against CCF potential	I&C functions and I&C systems	Detailed design of the I&C architecture in terms of automation systems, HMI and interconnections, tools (see 5.6.2)
5.4.3 Functional assignment	Output of 5.4.2 and 5.5 (Iteration with output of 6.4)	To assign the I&C functions to the individual I&C systems and equipment To provide requirements (boundaries, classification, functionality, reliability and other required properties) for the individual I&C systems	I&C functions and I&C systems	Requirements for the application functions of systems and HMI, the design of the I&C systems and the tools (see 5.6.3)
5.4.4 Required analysis	Outputs of 5.4.2 and 5.4.3	To assess reliability and defence against CCF To assess human factors	I&C functions and I&C systems	Assessment of reliability and defence against CCF (5.4.4.2) Assessment of human factors (5.4.4.3)

Clause or subclause	Inputs	Objectives of the activity	Scope	Outputs
5.5 Overall planning	Output of 5.4	To develop plans for QA, security, integration, commissioning, operation and maintenance of systems	I&C systems working co-operatively	Plans for the designated activities
6 System safety lifecycle	Output of 5.6	To specify and create I&C systems conforming to the I&C architecture specification (see Clause 6)	Individual I&C systems	Outputs are described in Table 3
7 Overall integration and commissioning	Output of 5.5.6 and 6.3.5	To test and commission the interconnected systems of the I&C architecture	I&C systems of the I&C architecture	Fully integrated and commissioned systems Report of the overall commissioning (see 7.3)
8 Overall operation and maintenance	Output of 5.5.7, 5.5.8 and 7.2	To operate maintain and repair the systems in order that the safety is maintained	I&C systems of the I&C architecture	Continuing achievement of functions. Records of operation and maintenance (see 8.3)
NOTE For a comparison of this definition of phases with that of IEC 61508-1 [1], see Annex B.				

919

920 **5.2 Deriving the I&C requirements from the plant safety design base**921 **5.2.1 General**

922 The objective of the requirements of this subclause is to derive input requirements for the
 923 specification of the I&C systems and input constraints for the I&C architectural design,
 924 resulting from the plant safety design base and the plant design framework.

925 IAEA SF-1 establish one fundamental safety objective and ten safety principles that together
 926 make up an “integrated overall safety approach” ensuring the safety of a NPP. These
 927 principles will be used in the design by considering all relevant “postulated initiating events”
 928 (PIEs) and successive physical barriers to keep radiation exposure to workers, public and the
 929 environment within limits. Key elements are (IAEA SSR-2/1)

- 930
- the application of the concept of defence in depth with 5 levels of defence, and
 - an appropriate quality level to maintain the integrity of design throughout the lifetime of the plant.
- 931
932

933 Both together provide sufficient functions and systems necessary to maintain the plant in a
 934 normal operating state, to ensure the correct response to all PIEs, and to facilitate the long-
 935 term management of the plant following an accident (see Clause A.2).

936 **5.2.2 Review of the functional, performance and independence requirements**

937 The functional, performance and independence requirements for the I&C functions important
 938 to safety and the principles of operation of the plant are defined in the plant safety design
 939 base which is an inherent element of the overall I&C design project. The requirements
 940 concerning human-machine interactions consider the principles of operation together with
 941 ergonomic considerations in order to minimize failures due to human factors.

942 The I&C design process requires the following inputs from the plant safety design base:

- the defence in-depth concept of the plant, with
 - the definition of the levels of defence;
 - the assignment of functions to the levels to address PIE sequences, and
 - related constraints, such as independence between individual functions.
- the requirements regarding handling of internal and external hazards, including constraints from building arrangement and related separation constraints;
- overall provisions for a main control room and a remote shut down station should the main control room be unavailable (IEC 60964, IEC 60965);
- constraints from the design of the safety support systems (HVAC, emergency power supply);
- constraints regarding environmental conditions (climatic, EMC, seismic);
- the approach for the categorization of safety functions;
- the failure criteria and redundancy requirements applicable for every category and type of safety function (e.g. single failure criterion combined with maintenance case for category A; redundancy for category B and exceptions);
- requirements on voting between redundant signals;

NOTE 1 In cases where the reliability of a function is required to be very high, the requirements specification for the plant and the I&C stipulate different levels of defence for the same PIE, for example, two or more independent and functionally diverse physical initiation criteria and, if appropriate, a second, functionally diverse, independent, redundant mechanical system for accident control.

NOTE 2 The defence in-depth levels may include functions important to safety and may include other functions. The requirements of this standard address only those functions that are important to safety.

- the role of the operators, of the automation and the set of prescribed operator actions in the management of anticipated operational occurrences and accident conditions; partially, this information may be overlapping with the set of functions for operator information / manual controls within the defence-in-depth concept;
- the function assignment in accordance with IEC 60964 defining which functions have been assigned to operators and which functions have been assigned to machines, i.e. the inventory of manual controls and automatic control functions;
- overall concept for alarm signalization (alarm classes, priorities);
- the variables and alarms to be displayed for the operator to use in taking manual control actions;
- the functional and performance requirements of the functions of the plant important to safety needed to meet the general safety requirements, in terms of
 - process variables,
 - algorithms and setpoints,
 - actuation signals,
 - manual controls, indicators, alarms,
 - performances (accuracy, response time),
 - reliability requirements (e.g. system availability; unavailability targets).

NOTE 3 Where functional verification is required (see 6.2.4.2), the design base provides the initial conditions, allowable limits and allowable rate of change of the plant variables to be controlled by the I&C systems important to safety.

NOTE 4 The compilation of the inventory of automatic control functions, manual controls and variables to be monitored may be iterative, i.e. it may start with a preliminary list of functions, functional and performance requirements which are subsequently refined, as the design of process and electrical systems proceeds. Especially functions for operation and monitoring of process systems may be the result of the design of the individual plant systems and selection of the mechanical / electrical equipment. Therefore, the detailed set of functional and performance requirements for process system related functions is not directly obtained from the plant safety design base but from the designers of the individual process systems.

- the priority principles between automatic and manually initiated actions, taking into account functional categories, main and supplementary control rooms, local control stations.

5.2.3 Review of the categorisation requirements

5.2.3.1 Assumptions of this standard concerning categorisation of functions and classification of systems

Functions, systems and equipment in the NPPs are classified according to their importance to safety. This standard distinguishes between categorisation of I&C functions and classification of I&C systems, in accordance with IEC 61226.

The categorisation process places each I&C function into a category according to its importance to safety.

These categories are characterised by sets of requirements on the specification, design, implementation, verification and validation of the I&C function, as well as by requirements on the properties of the systems suitable for the categories, their qualification, the application functions, the service functions, and the quality aspects for software, programmable logic and hardware, as appropriate. Consistent requirements apply to the whole I&C chain. Therefore, it is practical to define classes of I&C systems which are suitable to implement I&C functions up to a defined category.

The categorisation of the I&C functions is part of the plant safety design base and is outside the scope of this standard. This standard assumes that the plant safety design base has assigned the individual I&C functions important to safety to one of three categories A, B or C of IEC 61226.

NOTE The normative references for categorisation of functions may vary between countries and deviate from the reference of this standard (IEC 61226). A specific situation may also arise when applying this standard to existing plants where new categorization requirements are valid only for the parts in the scope of a modernization project. In such cases, a specific analysis may be required to identify the minimum requirements per system class.

The classification of the I&C systems is defined by the I&C project organisation in the design phase of the I&C architecture before the functional assignment of the I&C functions to the systems (see 5.4.2 and 5.4.3).

5.2.3.2 Requirements

5.2.3.2.1 The categorisation of the I&C functions shall be provided in the plant safety design base and shall constitute a reference input to the overall I&C requirements specification (see 5.3).

5.2.3.2.2 The I&C project organisation shall review the categorisation and verify it for completeness and feasibility. In the case of non-feasibility (for example, assignment of the highest category to a function which cannot meet the single failure criterion due to the plant design), the definition and categorisation of I&C functions shall be reviewed against the plant I&C functional requirements. The functional requirements and their associated categorisation shall be iterated until a feasible solution is achieved.

5.2.4 Review of plant and project constraints

The I&C architectural design (see 5.4) is subject to constraints imposed from the plant design framework.

5.2.4.1 The I&C project organisation shall identify the constraints placed on I&C equipment by the plant layout, the interfaces with plant equipment, and the events outside the I&C, including:

- the boundaries between the I&C systems and equipment and the plant systems, including the interfaces to the electrical/mechanical actuation systems and the auxiliary systems, such as power supplies and air conditioning systems;
- the range of transient and steady-state environmental conditions in normal, abnormal and accident conditions under which the I&C systems are required to operate;

NOTE There could be mismatch between the environmental conditions in rooms and the specifications of the selected I&C equipment. This is a typical case for situations leading to design iterations / maturity loops.

- the range of transient and steady-state conditions of motive and control power in normal, abnormal and accident conditions under which the I&C systems are required to operate;
- the general constraints on installation and cable routing;
- the specific constraints on installation and cable routing to centres of convergence such as the control room and cable spreading rooms;
- the constraints on grounding and power supply distribution;
- the internal and external hazards to be considered according to the plant hazard assumptions. These include fire, flooding, icing, lightning, overvoltage, electromagnetic interference, earthquake, explosion and chemical influences.

5.2.4.2 The I&C project organisation shall identify the constraints placed on I&C equipment by the utility's principles of operation, i.e. constraints from

- security (IEC 62645);
- operation and maintenance (IEC 60964);
- "in-service maintenance" including periodic testing of the process systems and I&C systems.

5.2.4.3 Typically, this will lead to additional requirements guiding the subdivision of the I&C architecture in separate sub-systems. Areas to be considered include:

- the subdivision of the I&C systems should take into account that the plant is typically structured in distinct plant systems, which are grouped in lots so as to organize engineering, installation, start-up and testing activities;
- maintenance work, periodic testing and modification activities shall be possible for selected plant and I&C subsystems whereas other subsystems have to stay fully operational;
- the impact of the distribution and sharing of operating staff responsibilities should be analysed and taken into account in the subdivision of the I&C systems;
- requirements should be identified regarding tools and service work stations for maintenance and diagnostics, including the interface to the engineering systems. This may include requirements concerning the human-machine interfaces to the maintenance staff, interfaces with central plant management facilities etc;
- the impact of staggered security degrees and security zones should be taken into account.

5.2.4.4 The I&C project organisation should identify the constraints resulting from the contractual framework for the NPP construction project. Areas to consider include

- identification of I&C equipment / I&C systems including HMIs that come with procured process system packages (pre-developed I&C packages, PDIP, such as. control equipment for emergency diesel generators or for HVAC packages, for lifting machines / cranes);

- 1084 • I&C equipment types or equipment suppliers imposed by the plant owner;
- 1085 • lifetime support requirements (e.g. constraints for replacement of parts with limited
- 1086 lifetime; long-term vendor support for equipment platforms).

1087 **5.2.4.5** The I&C project organization should develop overarching specifications for the I&C
 1088 system upstream to the I&C system lifecycle and before the procurement stage of process
 1089 system packages. These should include specifications such as

- 1090 • documentation standards;
- 1091 • standard types of interfaces;
- 1092 • preferred types of automation equipment for PDIPs
- 1093 • preferred types of field instrumentation equipment, e.-g. via a harmonized equipment
- 1094 catalogue;
- 1095 • rules for equipment coding and labelling;
- 1096 • HMI guidelines for panels or display units (to address consistency between HMIs
- 1097 coming with process system packages and with the main plant HMI);

1098 **5.3 Requirements specifications for the individual I&C functions**

1099 One key output of the activity described in 5.2 are the requirements specifications for the
 1100 individual I&C functions important to safety.

1101 The requirements specifications encompass the whole of the I&C function from its inputs
 1102 (sensors, operator controls, other equipment) to its outputs (directed to actuators, displays for
 1103 operators or other equipment). Further splitting of these requirements specifications will
 1104 provide the requirements specifications of the subfunctions at the level of the individual I&C
 1105 systems. This will depend upon the selected I&C architecture (see 5.4) and how the functions
 1106 are implemented through distributed equipment (instrumentation, processing and actuators).

1107 **NOTE** The specifications may be allocated to a suitably number and organisation of documents, e.g. dedicated
 1108 documents according to the safety category, defence line or other criteria derived from the design basis. Managing
 1109 the requirements in a data base and generating documentation packages from the data base could be an efficient
 1110 way for handling the data. It is not mandatory to have a single document per I&C function.

1111 **5.3.1** A requirements specification shall be established for each I&C function. It shall include:

- 1112 • a specification of the algorithm defining the way the function transforms input
- 1113 information to output information in order to operate or monitor the plant;
- 1114 • a specification of the performances, defining the range, accuracy and timely response
- 1115 of the function;

1116 **NOTE** Timely response typically implies a maximum response time (e.g. for trip functions), but could also
 1117 be a time constant for closed-loop control functions, or a quality requirement (residual noise). In some
 1118 cases, also a minimum response time could be specified, if race conditions between two functions have to
 1119 be avoided.

- 1120 • a reliability target, if available from the probabilistic safety assessment of the NPP or
- 1121 specified as a decoupling requirement;
- 1122 • specification of the category of the function.

1123 **NOTE** The category implicitly defines the minimal classification requirements of the I&C systems required
 1124 for the implementation of the function (see Table 2).

1125 **5.3.2** The requirements specifications shall define any dependency between functions which
 1126 generate constraints on the assignment of functions to the I&C systems. This includes:

- 1127 • the combinations of functions to be monitored to control protective actions;
- 1128 • the combination of functions ensuring defence in depth;
- 1129 • the combination of functions which constitute a safety group.