



DPC: 25 / 30507485 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: 18 February 2025

Origin: International

Latest date for receipt of comments: 9 April 2025

Project No. 2025/00120

Responsible committee: GEL/65/1 Systems aspects

Interested committees:

Title: BS EN IEC 61508-1 Functional safety of electrical/electronic/programmable electronic safety-related systems

Part 1: General requirements

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 9 April 2025**

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

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

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

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

Responsible Committee Secretary: Ms Charmaine Mukherjee (BSI)

Direct tel:

E-mail: charmaine.mukherjee@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.	



65A/1164/CDV

COMMITTEE DRAFT FOR VOTE (CDV)

PROJECT NUMBER: IEC 61508-1 ED3	
DATE OF CIRCULATION: 2025-02-14	CLOSING DATE FOR VOTING: 2025-05-09
SUPERSEDES DOCUMENTS: 65A/1056A/CD, 65A/1075A/CC	

IEC SC 65A : SYSTEM ASPECTS	
SECRETARIAT: United Kingdom	SECRETARY: Ms Stephanie Lavy
OF INTEREST TO THE FOLLOWING COMMITTEES: TC 8,TC 9,TC 22,TC 31,TC 44,TC 45,TC 56,TC 61,TC 62,TC 65,SC 65B,SC 65C,SC 65E,TC 66,TC 77,TC 80,TC 108,SyC AAL,SyC SM,SC 41	HORIZONTAL FUNCTION(S):
ASPECTS CONCERNED: Safety	
☒ SUBMITTED FOR CENELEC PARALLEL VOTING Attention IEC-CENELEC parallel voting The attention of IEC National Committees, members of CENELEC, is drawn to the fact that this Committee Draft for Vote (CDV) is submitted for parallel voting. The CENELEC members are invited to vote through the CENELEC online voting system.	☐ NOT SUBMITTED FOR CENELEC PARALLEL VOTING

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 relevant "In Some Countries" clauses to be included should this proposal proceed. Recipients are reminded that the CDV stage is the final stage for submitting ISC clauses. (SEE [AC/22/2007](#) OR [NEW GUIDANCE DOC](#)).

TITLE: Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 1: General requirements

PROPOSED STABILITY DATE: 2028

NOTE FROM TC/SC OFFICERS:

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

CONTENTS

1		
2		
3	FOREWORD.....	5
4	INTRODUCTION.....	7
5	1 Scope.....	9
6	2 Normative references	13
7	3 Definitions and abbreviations.....	13
8	4 Conformance to this document	13
9	5 Documentation	14
10	5.1 Objectives.....	14
11	5.2 Requirements	14
12	6 Management of functional safety	15
13	6.1 Objectives.....	15
14	6.2 Requirements	15
15	7 Overall safety lifecycle requirements	19
16	7.1 General.....	19
17	7.1.1 Introduction	19
18	7.1.2 Objectives and requirements – general.....	22
19	7.1.3 Objectives	30
20	7.1.4 Requirements	30
21	7.2 Concept.....	30
22	7.2.1 Objective	30
23	7.2.2 Requirements	30
24	7.3 Overall scope definition.....	31
25	7.3.1 Objectives	31
26	7.3.2 Requirements	31
27	7.4 Hazard and risk analysis	31
28	7.4.1 Objectives	32
29	7.4.2 Requirements	32
30	7.5 Overall safety requirements	33
31	7.5.1 Objective	33
32	7.5.2 Requirements	34
33	7.6 Overall safety requirements allocation	35
34	7.6.1 Objectives	35
35	7.6.2 Requirements	35
36	7.7 Overall operation and maintenance planning.....	40
37	7.7.1 Objective	40
38	7.7.2 Requirements	40
39	7.8 Overall safety validation planning	41
40	7.8.1 Objective	42
41	7.8.2 Requirements	42
42	7.9 Overall installation and commissioning planning	43
43	7.9.1 Objectives	43
44	7.9.2 Requirements	43
45	7.10 E/E/PE system safety requirements specification.....	44
46	7.10.1 Objective	44

47	7.10.2	Requirements	44
48	7.11	E/E/PE safety-related systems – realisation	46
49	7.11.1	Objective	46
50	7.11.2	Requirements	46
51	7.12	Other risk reduction measures – specification and realisation	46
52	7.12.1	Objective	46
53	7.12.2	Requirements	46
54	7.13	Overall installation and commissioning.....	46
55	7.13.1	Objectives	47
56	7.13.2	Requirements	47
57	7.14	Overall safety validation.....	47
58	7.14.1	Objective	47
59	7.14.2	Requirements	47
60	7.15	Overall operation, maintenance and repair.....	48
61	7.15.1	Objective	48
62	7.15.2	Requirements	48
63	7.16	Overall modification and retrofit	51
64	7.16.1	Objective	51
65	7.16.2	Requirements	52
66	7.17	Decommissioning or disposal.....	53
67	7.17.1	Objective	53
68	7.17.2	Requirements	54
69	7.18	Verification.....	54
70	7.18.1	Objective	54
71	7.18.2	Requirements	54
72	8	Functional safety assessment.....	55
73	8.1	Objective	55
74	8.2	Requirements	55
75	9	Functional safety audit.....	58
76	9.1	Objective	58
77	9.2	Requirements	58
78	Annex A (informative)	Example of a documentation structure.....	60
79	A.1	General.....	60
80	A.2	Safety lifecycle document structure.....	61
81	A.3	Physical document structure	64
82	Annex B (normative)	Levels of independence for functional safety assurance activities	66
83	B.1	General.....	66
84	Bibliography.....		68
85			
86	Figure 1 – Overall framework of the IEC 61508 series		12
87	Figure 2 – Overall safety lifecycle		20
88	Figure 3 – E/E/PE system safety lifecycle (in realisation phase).....		21
89	Figure 4 – Software safety lifecycle (in realisation phase).....		21
90	Figure 5 – Relationship of the overall safety lifecycle to the E/E/PE system and		
91	software safety lifecycles		22
92	Figure 6 – Allocation of overall safety requirements to E/E/PE safety-related systems		
93	and other risk reduction measures		37
94	Figure 7 – Example of operations and maintenance activities model		50

95	Figure 8 – Example of operation and maintenance management model	51
96	Figure 9 – Example of modification procedure model	53
97	Figure A.1 – Structuring information into document sets for user groups	65
98		
99	Table 1 – Overall safety lifecycle – overview	24
100	Table 2 – Safety integrity levels – target failure measures for a safety function	
101	operating in low demand mode of operation	38
102	Table 3 – Safety integrity levels – target failure measures for a safety function	
103	operating in high demand mode of operation or continuous mode of operation.....	38
104	Table A.1 – Example of a documentation structure for information related to the	
105	overall safety lifecycle.....	62
106	Table A.2 – Example of a documentation structure for information related to the E/E/PE	
107	system safety lifecycle	63
108	Table A.3 – Example of a documentation structure for information related to the	
109	software safety lifecycle	64
110	Table B.1 – Minimum levels of independence – Verification	67
111	Table B.2 – Minimum levels of independence - Validation	67
112	Table B.3 – Minimum levels of independence – Audit & Assessment.....	67
113		
114		

INTERNATIONAL ELECTROTECHNICAL COMMISSION

**FUNCTIONAL SAFETY OF ELECTRICAL/ELECTRONIC/
PROGRAMMABLE ELECTRONIC SAFETY-RELATED SYSTEMS –****Part 1: General requirements****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) IEC draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). IEC takes no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, IEC had not received notice of (a) patent(s), which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at <https://patents.iec.ch>. IEC shall not be held responsible for identifying any or all such patent rights.

IEC 61508-1 has been prepared by subcommittee 65A: System aspects, of IEC technical committee 65: Industrial-process measurement, control and automation. It is an International Standard.

This third edition cancels and replaces the second edition published in 2010. This edition constitutes a technical revision.

This edition includes the following significant technical changes with respect to the previous edition (the following list does refer to this document; other parts do mention specific further details):

- a) Document was upgraded to the 2024 version of the ISO/IEC Directives; this does introduce a significant number of editorial changes, clause renumbering and rewording of the information provided in Notes;

- b) The scope includes clarification on 'artificial Intelligence' (software technology class), human factors and security. The related requirements are limited to the hazard and risk analysis (refer to 7.1.2.3 on human factors and 7.4.2.3 for security) and further references to external guidance;
- c) The interfaces to other parts of IEC 61508 have been clarified and duplication of requirements in other Parts has been removed;
- d) The differentiation between the required Safety Integrity Level (SIL) and the achieved Systematic Capability (SC) has been clarified;
- e) Requirements on levels of independence for functional safety assurance activities (Annex B) have been introduced;
- f) Various minor editorial errors have been corrected, the normative references and the bibliography has been updated.

It has the status of a basic safety publication according to IEC Guide 104.

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

Draft	Report on voting
65A/XX/FDIS	65A/XX/RVD

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

The language used for the development of this document is English.

This document was drafted in accordance with ISO/IEC Directives, Part 2, and developed in accordance with ISO/IEC Directives, Part 1 and ISO/IEC Directives, IEC Supplement, available at www.iec.ch/members_experts/refdocs. The main document types developed by IEC are described in greater detail at www.iec.ch/publications.

A list of all parts of the IEC 61508 series, published under the general title *Functional safety of electrical / electronic / programmable electronic safety-related systems*, can be found on the IEC website.

The committee has decided that the contents of this document will remain unchanged until the stability date indicated on the IEC website under webstore.iec.ch in the data related to the specific document. At this date, the document will be

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

206

INTRODUCTION

207 Systems comprised of electrical and/or electronic elements have been used for many years to
208 perform safety functions in most application sectors. Computer-based systems (generically
209 referred to as programmable electronic systems) are being used in all application sectors to
210 perform non-safety functions and, increasingly, to perform safety functions. If computer system
211 technology is to be effectively and safely exploited, it is essential that those responsible for
212 making decisions have sufficient guidance on the safety aspects on which to make these
213 decisions.

214 This document sets out a generic approach for all safety lifecycle activities for systems
215 comprised of electrical and/or electronic and/or programmable electronic (E/E/PE) elements
216 that are used to perform safety functions. This unified approach has been adopted in order that
217 a rational and consistent technical policy be developed for all electrically-based safety-related
218 systems. A major objective is to facilitate the development of product and application sector
219 international standards based on the IEC 61508 series.

220 NOTE 1 Examples of product and application sector international standards based on the IEC 61508 series are
221 given in the Bibliography (see references [1], [2] and [3]).

222 In most situations, safety is achieved by a number of systems which rely on many technologies
223 (for example mechanical, hydraulic, pneumatic, electrical, electronic, programmable electronic).
224 Any safety strategy shall therefore consider not only all the elements within an individual system
225 (for example sensors, controlling devices and actuators) but also all the safety-related systems
226 making up the total combination of safety-related systems. The safety strategy shall also
227 consider the influence of humans on the achievement of functional safety. Therefore, while this
228 document is concerned with E/E/PE safety-related systems, it may also provide a framework
229 within which safety-related systems based on other technologies may be considered.

230 It is recognized that there is a great variety of applications using E/E/PE safety-related systems
231 in a variety of application sectors and covering a wide range of complexity, hazard and risk
232 potentials. In any particular application, the required safety measures will be dependent on
233 many factors specific to the application. This document, by being generic, will enable such
234 measures to be formulated in future product and application sector international standards and
235 in revisions of those that already exist.

236 This document

- 237 – considers all relevant overall, E/E/PE system and software safety lifecycle phases (for
238 example, from initial concept, through design, implementation, operation and maintenance
239 to decommissioning) when E/E/PE systems are used to perform safety functions;
- 240 – has been conceived with a rapidly developing technology in mind; the framework is
241 sufficiently robust and comprehensive to cater for future developments;
- 242 – enables product and application sector international standards, dealing with E/E/PE safety-
243 related systems, to be developed; the development of product and application sector
244 international standards, within the framework of this document, should lead to a high level
245 of consistency (for example, of underlying principles, terminology etc.) both within
246 application sectors and across application sectors; this will have both safety and economic
247 benefits;
- 248 – provides a method for the development of the safety requirements specification necessary
249 to achieve the required functional safety for E/E/PE safety-related systems;
- 250 – adopts a risk-based approach by which the safety integrity requirements can be determined;
- 251 – introduces safety integrity levels for specifying the target level of safety integrity for the
252 safety functions to be implemented by the E/E/PE safety-related systems;

253 NOTE 2 This document does not specify the safety integrity level requirements for any safety function, nor does it
254 mandate how the safety integrity level is determined. Instead, it provides a risk-based conceptual framework and
255 example techniques.

- sets target failure measures for safety functions carried out by E/E/PE safety-related systems, which are linked to the safety integrity levels;
- sets a lower limit on the target failure measures for a safety function carried out by a single E/E/PE safety-related system. For E/E/PE safety-related systems operating in
 - a low demand mode of operation, the lower limit is set at an average probability of a dangerous failure on demand of 10^{-5} ;
 - a high demand or a continuous mode of operation, the lower limit is set at an average frequency of a dangerous failure of 10^{-9} [h⁻¹];

NOTE 3 A single E/E/PE safety-related system does not necessarily mean a single-channel architecture.

NOTE 4 It can be possible to achieve designs of safety-related systems with lower values for the target safety integrity for non-complex systems, but these limits are considered to represent what can be achieved for relatively complex systems (for example programmable electronic safety-related systems) at the present time.

- sets requirements for the avoidance and control of systematic faults, which are based on experience and judgement from practical experience gained in industry. Even though the probability of occurrence of systematic failures cannot in general be quantified this document does, however, allow a claim to be made, for a specified safety function, that the target failure measure associated with the safety function can be considered to be achieved if all the requirements in this document have been met;
- adopts a broad range of principles, techniques and measures to achieve functional safety for E/E/PE safety-related systems, but does not explicitly use the concept of fail safe. However, the concept of “fail safe” and “inherently safe” principles may be applicable and adoption of such concepts is acceptable providing the requirements of the relevant clauses in this document are met.

FUNCTIONAL SAFETY OF ELECTRICAL/ELECTRONIC/ PROGRAMMABLE ELECTRONIC SAFETY-RELATED SYSTEMS –

Part 1: General requirements

1 Scope

1.1 This document covers those aspects to be considered when electrical/electronic/programmable electronic (E/E/PE) systems are used to carry out safety functions. A major objective of it

The goal of this document is to facilitate the development of product and application sector international standards by the technical committees responsible for the product or application sector. This will allow all the relevant factors, associated with the product or application, to be fully taken into account and thereby meet the specific needs of users of the product and the application sector. A second objective of this document is to enable the development of E/E/PE safety-related systems where product or application sector international standards do not exist.

The scope of this document is functional safety for E/E/PE safety-related systems but, apart from normative requirements in the hazard and risk analysis phase, does not itself provide normative requirements for malevolent action arising from a cybersecurity risk. However, if a cybersecurity assessment has identified that a reasonably foreseeable cyber security risk will arise, it is essential that measures be taken for all relevant phases of the overall, E/E/PE and software safety lifecycles in order to protect against such threats to ensure that functional safety is achieved.

NOTE 1 For requirements and/or guidance on cybersecurity see IEC 62443 series and ISO/IEC 27000 series.

NOTE 2 For guidance on the coordination between safety and security refer to IEC TR 63069.

1.2 In particular, this document

a) applies to safety-related systems when one or more of such systems incorporates electrical/electronic/programmable electronic elements;

NOTE 1 In the context of low complexity E/E/PE safety-related systems, certain requirements specified in this document can be unnecessary, and exemption from compliance with such requirements is possible (see 4.2, and the definition of a low complexity E/E/PE safety-related system in 3.4.3 of IEC 61508-4).

NOTE 2 Although a person can form part of a safety-related system (see 3.4.1 of IEC 61508-4), human factor requirements related to those aspects of the design of E/E/PE safety-related systems are not considered in detail in this document.

NOTE 3 This document can be applied to custom, low-volume and high volume production safety-related systems, subsystems, elements and compliant items.

NOTE 4 This document can be applied to parts of the safety function (e.g., compliant item or tool) but it does not provide a final SIL statement to a part of the safety function.

b) is generically based and applicable to all E/E/PE safety-related systems irrespective of the application;

c) covers the achievement of a tolerable risk through the application of E/E/PE safety-related systems, but does not cover hazards arising from the E/E/PE equipment itself (for example electric shock);

d) applies to all types of E/E/PE safety-related systems, including protection systems and control systems;

e) does not cover E/E/PE systems where

- a single E/E/PE system is capable on its own of meeting the tolerable risk, and
- the required quantitative performance and integrity of the safety functions of the single E/E/PE system is less than that specified for safety integrity level 1 (the lowest safety integrity level in this document).

f) is mainly concerned with the E/E/PE safety-related systems whose failure could have an impact on the safety of persons and/or the environment; however, it is recognized that the consequences of failure could also have serious economic implications and in such cases this document could be used to specify any E/E/PE system used for the protection of equipment or product;

NOTE 7 See 3.1.1 of IEC 61508-4.

g) considers E/E/PE safety-related systems and other risk reduction measures, in order that the safety requirements specification for the E/E/PE safety-related systems can be determined in a systematic, risk-based manner;

h) uses an overall safety lifecycle model as the organisational framework for dealing systematically with the processes and activities necessary for ensuring the functional safety of the E/E/PE safety-related systems;

NOTE 8 Although the overall safety lifecycle is primarily concerned with E/E/PE safety-related systems, it might also provide a technical framework for considering any safety-related system irrespective of the technology of that system (for example mechanical, hydraulic or pneumatic).

i) specifies the essential concept of safety integrity levels applicable to any sector application;

j) does not specify the selection of safety integrity levels required to address risks specific to sector applications (which must be based on detailed information and knowledge of the sector application).

k) provides general requirements for E/E/PE safety-related systems where no product or application sector international standards exist;

l) requires malevolent and unauthorised actions to be considered during hazard and risk analysis. The scope of the analysis includes all relevant safety lifecycle phases;

NOTE 9 For further details refer to ISO/IEC TR 19791 and IEC 62443 series.

m) does not cover the precautions that may be necessary to prevent unauthorized persons damaging, and/or otherwise adversely affecting, the functional safety of E/E/PE safety-related systems (see k) above);

n) does not specify the requirements for the development, implementation, maintenance and/or operation of security policies or security services needed to meet a security policy that may be required by the E/E/PE safety-related system;

o) does apply to software algorithms of software technology class I;

does apply to software algorithms of software technology class II and in combination with the additional requirements provided in ISO/IEC TS 22440.

NOTE 1 The software technology classes relate to the generically used term “artificial intelligence” as defined in ISO/IEC 22989; for definitions refer to 61508-4, Clauses 3.2.15, 3.2.16 and 3.2.17.

NOTE 2 Refer to ISO/IEC TR 5469:2024 and to ISO/IEC TS 22440-1 for further details.

NOTE 3 The concept of safety integrity level as described in this document can be applied to the hardware used to execute or implement software algorithms of software technology class I, II or III

1.3 This part of the IEC 61508 series of standards includes general requirements that are applicable to all parts. Other parts of the IEC 61508 series concentrate on topics that are more specific:

- parts 2 and 3 provide additional and specific requirements for E/E/PE safety-related systems (part 2 for hardware and part 3 for software);
- part 4 gives definitions and abbreviations that are used throughout all parts of this document

- 379 – part 5 provides guidelines on the application of part 1 in determining safety integrity levels,
380 by showing example methods;
- 381 – part 6 provides guidelines on the application of parts 2 and 3;
- 382 – part 7 contains an overview of techniques and measures.

383 **1.4** This document is a basic safety publication to be used in conjunction with the other parts
384 of IEC 61508 for use by end users to evaluate functional safety applications, or by technical
385 committees in the preparation of standards in accordance with the principles contained in IEC
386 Guide 104 and ISO/IEC Guide 51. This document does not apply in the context of low complexity
387 E/E/PE safety-related systems (see IEC 61508-4 3.4.3).

388 **1.5** Figure 1 shows the overall framework of the IEC 61508 series and indicates the role that
389 IEC 61508-1 plays in the achievement of functional safety for E/E/PE safety-related systems.

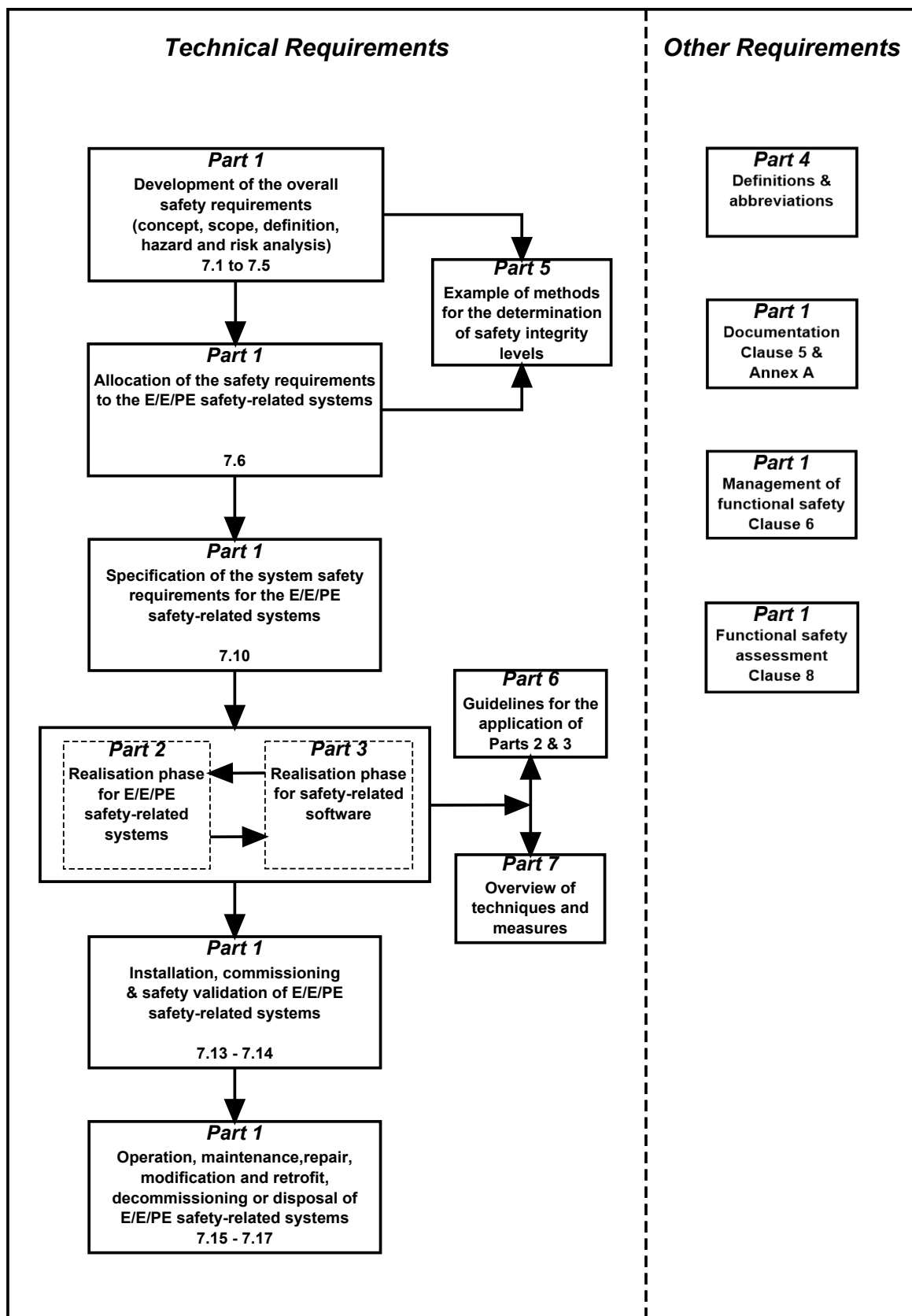


Figure 1 – Overall framework of the IEC 61508 series

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements 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 61508-2:202X, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems*

IEC 61508-3:202X, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 3: Software requirements*

IEC 61508-4:202X, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 4: Definitions and abbreviations*

IEC Guide 104:2019, *The preparation of safety publications and the use of basic safety publications and group safety publications*

ISO/IEC Guide 51:2014, *Safety aspects – Guidelines for their inclusion in standards*

3 Definitions and abbreviations

For the purposes of this document, the definitions and abbreviations given in IEC 61508-4 apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

- IEC Electropedia: available at <https://www.electropedia.org/>
- ISO Online browsing platform: available at <https://www.iso.org/obp>

4 Conformance to this document

4.1 To conform to this document it shall be demonstrated that all the relevant requirements have been satisfied to the required criteria specified (for example safety integrity level) and therefore, for each clause or subclause, all the objectives have been met.

NOTE This can be done in the form of a safety case (justification) which provides clear, comprehensive and defensible arguments, supported by evidence, that all relevant normative requirements in this document are met when operated in the intended operational environment.

4.2 This document specifies the requirements for E/E/PE safety-related systems and has been developed to meet the full range of complexity associated with such systems. However, for low complexity E/E/PE safety-related systems (see 3.4.3 of IEC 61508-4), where dependable field experience exists which provides the necessary confidence that the required safety integrity can be achieved, the following options are available:

- a) in product and application sector international standards implementing the requirements of IEC 61508-1 to IEC 61508-7, certain requirements may be unnecessary and exemption from compliance with such requirements is acceptable;
- a) if this document is used directly for those situations where no product or application sector international standard exists, certain of the requirements specified in this document may be unnecessary and exemption from compliance with such requirements is acceptable providing this is justified.

4.3 Product or application sector international standards for E/E/PE safety-related systems developed within the framework of this document shall take into account the requirements of ISO/IEC Guide 51 and IEC Guide 104.

5 Documentation

5.1 Objectives

5.1.1 The first objective of the requirements of this clause is to specify the necessary information to be documented in order that all phases of the overall, E/E/PE system and software safety lifecycles can be effectively performed.

5.1.2 The second objective of the requirements of this clause is to specify the necessary information to be documented in order that the management of functional safety (see Clause 6), verification (see 7.18) and the functional safety assessment (see Clause 8) activities can be effectively performed.

NOTE 1 The information can be contained in physical documents ,if this is explicitly declared in the relevant subclause.

NOTE 2 Documentation can be available in different forms (for example on paper, film, or any data medium to be presented on screens or displays).

NOTE 3 See Annex A concerning example documentation structures.

NOTE 4 See reference [7] in the Bibliography.

5.2 Requirements

5.2.1 The documentation shall contain sufficient information, for each phase of the overall, E/E/PE system and software safety lifecycles completed, necessary for effective performance of subsequent phases and verification activities.

NOTE What constitutes sufficient information will be dependent upon a number of factors, including the complexity and size of the E/E/PE safety-related systems and the requirements relating to the specific application.

5.2.2 The documentation shall contain sufficient information required for the management of functional safety (Clause 6).

NOTE See notes to 5.1.2.

5.2.3 The documentation shall contain sufficient information required for the implementation of a functional safety assessment, together with the information and results derived from any functional safety assessment.

Note 1 to entry: See notes to 5.1.2.

5.2.4 The information to be documented shall be as stated in the various clauses of this document.

5.2.5 The availability of documentation shall be sufficient for the duties to be performed in respect of the clauses of this document.

NOTE Only the information necessary to undertake a particular activity, required by this document, can be held by each relevant party.

5.2.6 The documentation shall:

- a) be accurate and concise;
- b) be easy to understand by those persons having to make use of it;
- c) suit the purpose for which it is intended;

d) be accessible and maintainable.

5.2.7 The documentation or set of information shall have titles or names indicating the scope of the contents, and some form of index arrangement so as to allow ready access to the information required in this document.

5.2.8 The documentation structure may take account of company procedures and the working practices of specific product or application sectors.

5.2.9 The documents or set of information shall have a revision index (version numbers) to make it possible to identify different versions of the document.

5.2.10 The documents or set of information shall be so structured as to make it possible to search for relevant information. It shall be possible to identify the latest revision (version) of a document or set of information.

NOTE The physical structure of the documentation can vary depending upon a number of factors such as the size of the system, its complexity and organizational requirements.

5.2.11 All relevant documents shall be revised, amended, reviewed and approved under an appropriate document control scheme.

NOTE Where automatic or semi-automatic tools are used for the production of documentation, specific procedures can be necessary to ensure effective measures are in place for the management of versions or other control aspects of the documents.

6 Management of functional safety

6.1 Objectives

6.1.1 The first objective of the requirements of this clause is to specify the responsibilities in the management of functional safety of those who have responsibility for an E/E/PE safety-related system, or for one or more phases of the overall E/E/PE system and software safety lifecycles.

6.1.2 The second objective of the requirements of this clause is to specify the activities to be carried out by those with responsibilities in the management of functional safety.

NOTE The organizational measures dealt with in this clause provide for the effective implementation of the technical requirements and are solely aimed at the achievement and maintenance of functional safety of the E/E/PE safety-related systems.

6.2 Requirements

6.2.1 An organisation with responsibility for an E/E/PE safety-related system, or for one or more phases of the overall, E/E/PE system or software safety lifecycle, shall appoint one or more persons to take overall responsibility for:

- a) the system and for all safety lifecycle phases;
- b) coordinating the safety-related activities carried out in those phases;
- c) the interfaces between those phases and other phases carried out by other organisations;
- d) carrying out the requirements of 6.2.2 to 6.2.11 and 6.2.13;
- e)

coordinating functional safety assessments (see 6.2.12 b) and Clause 8) – particularly where those carrying out the functional safety assessment differ between phases – including communication, planning, and integrating the documentation, judgements and recommendations;

- f) coordinating functional safety audits (clause 9);

g) ensuring that functional safety is achieved and demonstrated in accordance with the objectives and requirements of this document.

NOTE

The activities specified shall form the basis of a safety plan.

NOTE 1 The safety plan(s), relevant to the activities to be undertaken to achieve functional safety conform an integral part of the policy and strategy for the achievement of functional safety.

NOTE 2 Refer to Part 2 Clause 6.2.2 and Part 3 Clause 6.2.2 for additional requirements on safety planning.

6.2.2 The minimum safety lifecycle activities to be performed in each safety lifecycle phase shall be specified. The activities specified shall be the basis for the safety planning.

6.2.3 All persons, departments and organizations responsible for carrying out activities in the applicable overall, E/E/PE system or software safety lifecycle shall be identified, and their responsibilities shall be fully and clearly communicated to them.

Responsibility for safety-related activities, or for safety lifecycle phases, may be delegated to other persons, particularly those with relevant expertise, and different persons could be responsible for different activities and requirements. However, the responsibility for coordination, and for overall functional safety, should reside in one or a small number of persons with sufficient management authority.

EXAMPLE Including persons responsible for verification and functional safety assessment and, where relevant, licensing authorities or safety regulatory bodies.

6.2.4 Procedures shall be developed for defining what information is to be communicated, between relevant parties, and how that communication will take place.

NOTE See Clause 5 for documentation requirements.

6.2.5 Procedures shall be developed for ensuring prompt follow-up and satisfactory resolution of recommendations relating to E/E/PE safety-related systems, including those arising from:

- a) hazard and risk analysis (see 7.4);
- b) functional safety assessment (see Clause 8);
- c) verification activities (see 7.18);
- d) validation activities (see 7.8 and 7.14);
- e) modification and retrofit (see 7.16);
- f) configuration management (see 6.2.10, 6.2.3 of IEC 61508-2, and 6.2.3 of IEC 61508-3);
- g) incident reporting and analysis (see 6.2.6);
- h) requirements management (see 6.2.21).

6.2.6 Procedures shall be developed for ensuring that all detected hazardous events are analysed, and that recommendations are made to minimise the probability of a repeat occurrence.

6.2.7 Requirements for periodic functional safety audits shall be specified, including:

- a) the frequency of the functional safety audits (see Clause 9);
- b) the level of independence of those carrying out the audits (see Annex B);

NOTE See Annex B, B.1.4 of IEC 61508-7 for further guidance on independence of functional safety assurance.

- c) the necessary documentation and follow-up activities (see Clause 9).

NOTE Refer to the ISO 19011 or ISO/IEC 17021 standards for general guidelines for auditing of management systems.

6.2.8 Procedures shall be developed for:

- a) initiating modifications to the E/E/PE safety-related systems (see 7.16.2.2);
- b) obtaining approval and authority for modifications.

6.2.9 Procedures shall be developed for maintaining accurate information on hazards and hazardous events, safety functions and E/E/PE safety-related systems.

6.2.10 Procedures shall be developed for configuration management of the E/E/PE safety-related systems during the overall, E/E/PE system and software safety lifecycle phases, including in particular:

- a) the point, in respect of specific phases, at which formal configuration control is to be implemented;
- b) the procedures to be used for uniquely identifying all constituent parts of the E/E/PE system (hardware and software);
- c) the procedures for preventing unauthorized elements from entering service.

6.2.11 Training and guidelines for emergency services may be provided to address incidents or major hazards, depending on the final application.

NOTE Emergency services which are applicable to the end user can be needed in case of reasonably foreseeable incidents or major hazards.

6.2.12 Those individuals who have responsibility for one or more phases of the overall, E/E/PE system or software safety lifecycles shall, in respect of those phases for which they have responsibility and in accordance with the procedures defined in 6.2.1 to 6.2.11, specify all management and technical activities that are necessary to ensure the achievement, demonstration and maintenance of functional safety of the E/E/PE safety-related systems, including:

- a) the selected measures and techniques used to meet the requirements of a specified clause or subclause (see IEC 61508-2, IEC 61508-3 and IEC 61508-6);
- b) the functional safety assessment activities, and the way in which the achievement of functional safety will be demonstrated to those carrying out the functional safety assessment (see Clause 8);

NOTE Appropriate procedures for functional safety assessment can be used to define

- the selection of an appropriate organisation, person or persons, at the appropriate level of independence;
 - the selection of an appropriate organisation, person or persons, at the appropriate level of technical, procedural and human factors expertise;
 - the drawing up, and making changes to, terms of reference for functional safety assessments;
 - the change of those carrying out the functional safety assessment at any point during the lifecycle of a system;
 - the resolution of disputes involving those carrying out functional safety assessments.
- c) the procedures for analysing operations and maintenance performance, in particular for
- recognising systematic faults that could jeopardise functional safety, including procedures used during routine maintenance that detect recurring faults;
 - assessing whether the demand rates and failure rates during operation and maintenance are in accordance with assumptions made during the design of the system.

6.2.13 Procedures shall be developed to ensure that all persons with responsibilities defined in accordance with 6.2.1 and 6.2.3 (i.e. including all persons involved in any overall, E/E/PE system or software lifecycle activity, including activities for verification, management of functional safety and functional safety assessment), shall have the appropriate competence (i.e. training, technical knowledge, experience and qualifications) relevant to the specific duties that they have to perform. Such procedures shall include requirements for the refreshing, updating and continued assessment of competence.

6.2.14 The appropriateness of competence shall be considered in relation to the particular application, taking into account all relevant factors including:

- a) the responsibilities of the person;
- b) the level of supervision required;
- c) the potential consequences in the event of failure of the E/E/PE safety-related systems – the greater the consequences, the more rigorous shall be the specification of competence;
- d) the safety integrity levels of the E/E/PE safety-related systems – the higher the safety integrity levels, the more rigorous shall be the specification of competence;
- e) the novelty of the design, design procedures or application – the newer or more untried these are, the more rigorous shall be the specification of competence;
- f) previous experience and its relevance to the specific duties to be performed and the technology being employed – the greater the required competence, the closer the fit shall be between the competences developed from previous experience and those required for the specific activities to be undertaken;
- g) the type of competence appropriate to the circumstances (for example qualifications, experience, relevant training and subsequent practice, and leadership and decision-making abilities);
- h) engineering knowledge appropriate to the application area and to the technology;
- i) safety engineering knowledge appropriate to the technology;
- j) knowledge of the legal and safety regulatory framework;
- k) relevance of qualifications to specific activities to be performed;

NOTE Reference [8] in the Bibliography contains an example method for managing competence for E/E/PE safety-related systems.

- l) human factors knowledge concerning the technology and application.

6.2.15 The competence of all persons with responsibilities defined in accordance with 6.2.1 and 6.2.3 shall be documented.

6.2.16 The evidence of competence of all persons with responsibility defined in accordance with 6.2.1 and 6.2.3 shall include:

- a) The competencies required for each of the specific duties to be performed.
- b) Assessment of the competencies of the person who is to undertake the specified duties against the competencies defined in (a) above.
- c) Undertake a comparison of the specified competence profile for the duties to be performed with the competence profile of the person.

NOTE See references [25, 26, 27] in the Bibliography for further guidance..

6.2.17 The activities specified as a result of 6.2.2 to 6.2.15 shall be implemented and monitored.

6.2.18 Procedures shall be developed to ensure that compliant items conform to their design specification, **Such procedures shall be developed for all relevant safety lifecycle phases.**

6.2.19 Suppliers providing products or services to an organization having overall responsibility for one or more phases of the overall, E/E/PE system or software safety lifecycles (see 6.2.1), shall deliver products or services as specified by that organization and shall have an appropriate quality management system.

Traceability shall be provided between inputs and outputs of subsequent and previous safety lifecycle phases and where necessary within phases.

NOTE The concept of traceability is explained in IEC 61508-7 cl. B.1.5. Inputs and outputs of safety lifecycle phases are displayed in Table 1. An example where traceability within a phase can be required is the hazard and risk analysis phase clause 7.4 where traceability between hazard analysis and risk assessment is necessary.

6.2.20 Activities relating to the management of functional safety shall be applied at the relevant phases of the overall, E/E/PE system and software safety lifecycles (see 7.1.1.5).

6.2.21 Procedures shall be developed for requirements management of the E/E/PE safety-related systems during the overall, E/E/PE system and software safety lifecycle phases, including in particular:

- a) the procedures to be used for uniquely identifying all/each requirements;
- b) the procedures to maintain the requirements under configuration management;
- c) the procedures for classifying and allocating the requirements to the constituent parts of the E/E/PE system items (hardware and software).

NOTE Guidance is provided in IEC 61508-6 Annexes H and I on requirements management.

7 Overall safety lifecycle requirements

7.1 General

7.1.1 Introduction

7.1.1.1 In order to deal in a systematic manner with all the activities necessary to achieve the required safety integrity for the safety functions carried out by the E/E/PE safety-related systems, this document adopts an overall safety lifecycle (see Figure 2) as the technical framework.

NOTE The overall safety lifecycle can be used as a basis for claiming conformance to this document, but a different overall safety lifecycle can be used to that given in Figure 2, providing the objectives and requirements of each clause of this document are met.

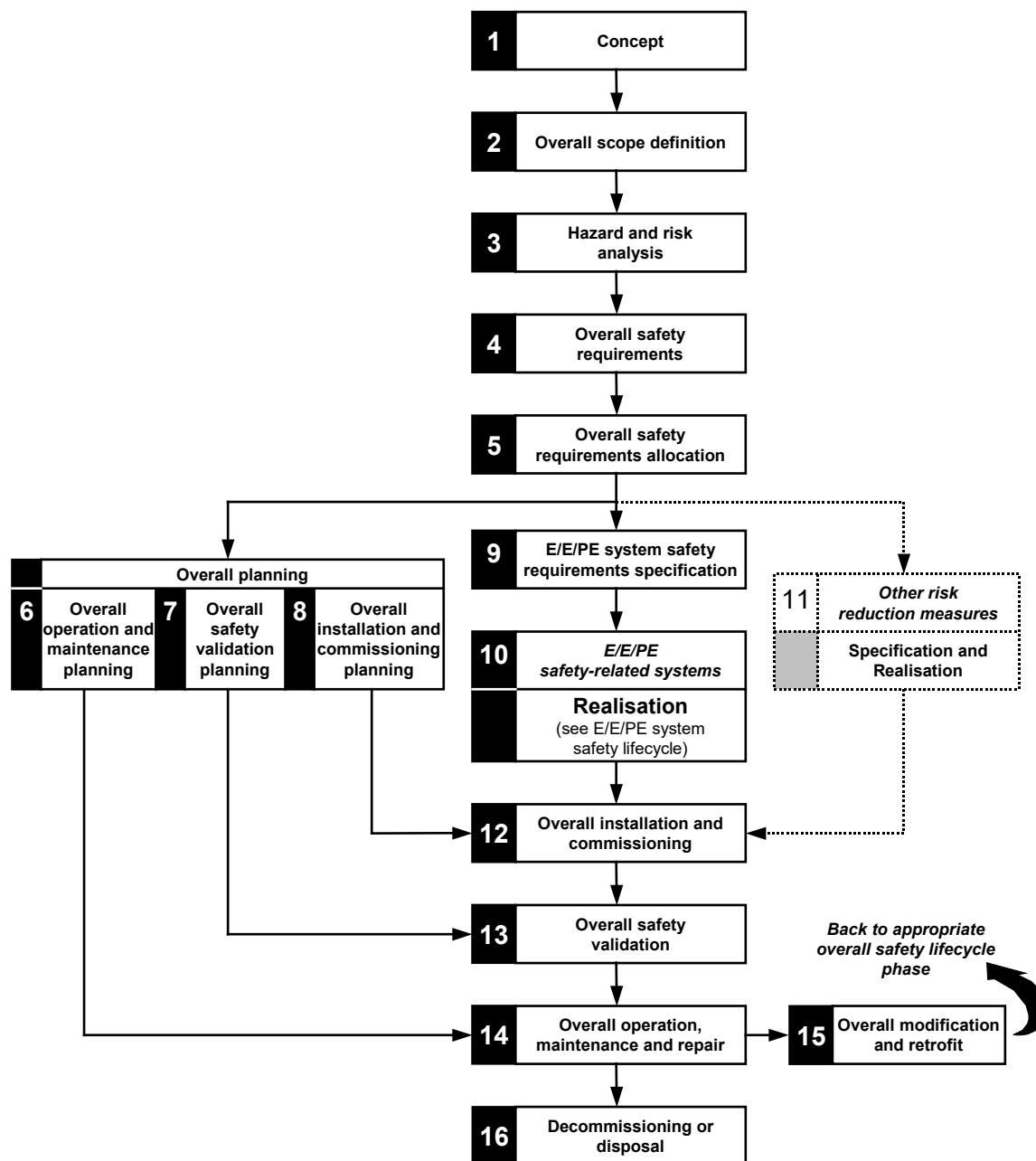
7.1.1.2 The overall safety lifecycle encompasses the following means for meeting the tolerable risk:

- a) E/E/PE safety-related systems;
- b) other risk reduction measures.

7.1.1.3 The E/E/PE safety-related systems realisation phase from the overall safety lifecycle is expanded and shown in Figure 3. This part of the E/E/PE system safety lifecycle forms the technical framework for IEC 61508-2. The part of the software safety lifecycle shown in Figure 4 forms the technical framework for IEC 61508-3. The relationship of the overall safety lifecycle to the E/E/PE system and software safety lifecycles for safety-related systems is shown in Figure 5.

7.1.1.4 The overall, E/E/PE system and software safety lifecycle figures (Figures 2 to 4) are simplified views of reality and as such do not show all the iterations relating to specific phases or between phases. Iteration, however, is an essential and vital part of development through the overall, E/E/PE system and software safety lifecycles.

7.1.1.5 Activities relating to the management of functional safety (Clause 6), verification (7.18) and functional safety assessment (Clause 8) are not shown on the overall, E/E/PE system or software safety lifecycles. This has been done in order to reduce the complexity of the lifecycle figures. These activities, where required, will need to be applied at the relevant phases of the overall, E/E/PE system and software safety lifecycles.



NOTE 1 Activities relating to **verification**, **management of functional safety** and **functional safety assessment** are not shown for reasons of clarity but are relevant to all overall, E/E/PE system and software safety lifecycle phases.

NOTE 2 The phase represented by Box 11 can be outside the scope of this document.

NOTE 3 IEC 61508-2 and IEC 61508-3 can deal with Box 10 (realisation) but they can also deal, where relevant, with the programmable electronic (hardware and software) aspects of Boxes 13, 14 and 15.

NOTE 4 See Table 1 for a description of the objectives and scope of the phases represented by each box.

NOTE 5 The technical requirements can be necessary for overall operation, maintenance, repair, modification, retrofit and decommissioning or disposal can be specified as part of the information provided by the supplier of the E/E/PE safety-related system, subsystems and/or elements that are used to perform the safety functions or safety functions.

Figure 2 – Overall safety lifecycle