



DPC: 25 / 30507489 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. 2025/00121

Responsible committee: GEL/65/1 Systems aspects

Interested committees:

Title: BS EN IEC 61508-2 Functional safety of electrical/electronic/programmable electronic safety-related systems

Part 2: Requirements for electrical/electronic/programmable electronic safety-related 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 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/1165/CDV

COMMITTEE DRAFT FOR VOTE (CDV)

PROJECT NUMBER: IEC 61508-2 ED3	
DATE OF CIRCULATION: 2025-02-14	CLOSING DATE FOR VOTING: 2025-05-09
SUPERSEDES DOCUMENTS: 65A/1057A/CD, 65A/1076A/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 2: Requirements for electrical/electronic/programmable electronic safety-related systems

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	10
7	3 Definitions and abbreviations.....	11
8	4 Conformance to this document	11
9	5 Documentation	11
10	6 Additional requirements for management of functional safety for E/E/PE system	12
11	6.1 Objectives.....	12
12	6.2 Requirements	12
13	7 E/E/PE system safety lifecycle requirements	12
14	7.1 General.....	12
15	7.1.1 Objectives and requirements – general.....	12
16	7.1.2 Objectives	13
17	7.1.3 Requirements	13
18	7.2 E/E/PE system design requirements specification	15
19	7.2.1 Objective	15
20	7.2.2 General	16
21	7.2.3 E/E/PE system design requirements specification.....	16
22	7.3 E/E/PE system safety validation planning	18
23	7.3.1 Objective	18
24	7.3.2 Requirements	18
25	7.4 E/E/PE system design and development	18
26	7.4.1 Objective	18
27	7.4.2 General requirements	18
28	7.4.3 Synthesis of elements to achieve the required systematic capability	21
29	7.4.4 Hardware safety integrity architectural constraints	22
30	7.4.5 Requirements for quantifying the effect of random hardware failures	33
31	7.4.6 Requirements for the avoidance of systematic faults	35
32	7.4.7 Requirements for the control of systematic faults.....	36
33	7.4.8 Requirements for system behaviour on detection of a fault	37
34	7.4.9 Requirements for E/E/PE system implementation	37
35	7.4.10 Requirements for systematic safety integrity of proven in use elements (Route 2s)	39
37	7.4.11 Additional requirements for data communications	40
38	7.4.12 Requirements for diagnostic functions	42
39	7.5 E/E/PE system integration	43
40	7.5.1 Objective	43
41	7.5.2 Requirements	43
42	7.6 E/E/PE system operation and maintenance procedures	44
43	7.6.1 Objective	44
44	7.6.2 Requirements	44
45	7.7 E/E/PE system safety validation.....	45
46	7.7.1 Objective	45
47	7.7.2 Requirements	46

48	7.8	E/E/PE system modification	47
49	7.8.1	Objective	47
50	7.8.2	Requirements	47
51	7.9	E/E/PE system verification	48
52	7.9.1	Objective	48
53	7.9.2	Requirements	48
54	8	Functional safety assessment.....	49
55	Annex A (normative)	Techniques and measures for E/E/PE safety-related systems –	
56		control of failures during operation	50
57	A.1	General.....	50
58	A.2	Hardware safety integrity	51
59	A.3	Systematic capability	59
60	Annex B (normative)	Techniques and measures for E/E/PE safety-related systems –	
61		avoidance of systematic failures during the different phases of the lifecycle	65
62	Annex C (normative)	Diagnostic coverage and safe failure fraction	75
63	C.1	Calculation of diagnostic coverage and safe failure fraction of a hardware	
64		element.....	75
65	C.2	Determination of diagnostic coverage factors	76
66	Annex D (normative)	Safety manual for compliant items	78
67	D.1	General.....	78
68	D.2	Contents	78
69	Annex E (normative)	Common Cause Failure Analysis (CCFA)	80
70	E.1	General.....	80
71	E.2	Methodology	80
72	E.3	Propagation of common cause failures.....	80
73	E.4	Architecture	81
74	E.5	Common cause failure analysis.....	82
75	E.6	Common cause initiators.....	83
76	Bibliography.....		84
77			
78	Figure 1 – Overall framework of the IEC 61508 series		10
79	Figure 2 – E/E/PE system safety lifecycle (in realisation phase).....		14
80	Figure 3 – Relationship between and scope of IEC 61508-2 and IEC 61508-3		14
81	Figure 4 – Determination of the maximum SIL for specified architecture (E/E/PE safety-		
82	related subsystem comprising a number of series elements, see 7.4.4.2.3)		28
83	Figure 5 – Determination of the maximum SIL for a safety function carried out by a		
84	specified architecture (E/E/PE safety-related subsystem comprised of two subsystems		
85	X & Y, see 7.4.4.2.4).....		31
86	Figure 6 - Architectures for data communication – “white channel”		41
87	Figure 7 – Architectures for data communication – “black channel”		41
88	Figure G.1 – Methodology.....		80
89	Figure G.2 – Propagation of common cause failures		81
90	Figure G.3 – Example of an architecture		82
91	Figure G.4 – Common cause failure analysis		82
92			
93	Table 1 – Overview – realisation phase of the E/E/PE system safety lifecycle		14
94	Table 2 – Maximum allowable safety integrity level for a safety function carried out by		
95	a type A safety-related element		26
96	Table 3 – Maximum allowable safety integrity level for a safety function carried out by		
97	a type B safety-related element		27

98	Table A.1 – Faults or failures to be assumed when quantifying the effect of random	
99	hardware failures or to be taken into account in the derivation of safe failure fraction	52
100	Table A.2 – Electrical components	53
101	Table A.3 – Electronic components	54
102	Table A.4 – Processing units	54
103	Table A.5 – Invariable memory ranges	55
104	Table A.6 – Variable memory ranges	56
105	Table A.7 – I/O units and interface (external communication).....	56
106	Table A.8 – Data paths (internal communication)	57
107	Table A.9 – Power supply	57
108	Table A.10 – Program sequence (watch-dog).....	58
109	Table A.11 – Clock	58
110	Table A.12 – Communication and mass-storage	58
111	Table A.13 – Sensors	59
112	Table A.14 – Final elements (actuators).....	59
113	Table A.15 – Techniques and measures to control systematic failures caused by	
114	hardware design	61
115	Table A.16 – Techniques and measures to control systematic failures caused by	
116	environmental stress or influences	62
117	Table A.17 – Techniques and measures to control systematic operational failures	63
118	Table A.18 – Effectiveness of techniques and measures to control systematic failures	64
119	Table B.1 – Techniques and measures to avoid mistakes during specification of	
120	E/E/PE system design requirements (see 7.2)	67
121	Table B.2 – Techniques and measures to avoid introducing faults during E/E/PE	
122	system design and development (see 7.4)	68
123	Table B.3 – Techniques and measures to avoid faults during E/E/PE system	
124	integration (see 7.5).....	69
125	Table B.4 – Techniques and measures to avoid faults and failures during E/E/PE	
126	system operation and maintenance procedures (see 7.6).....	70
127	Table B.5 – Techniques and measures to avoid faults during E/E/PE system safety	
128	validation (see 7.7)	71
129	Table B.6 – Effectiveness of techniques and measures to avoid systematic failures.....	72
130	Table G.1 – Common cause initiator CCI (non-exhaustive)	83

131

132

INTERNATIONAL ELECTROTECHNICAL COMMISSION

**FUNCTIONAL SAFETY OF ELECTRICAL/ELECTRONIC/
PROGRAMMABLE ELECTRONIC SAFETY-RELATED SYSTEMS –****Part 2: Requirements for electrical/electronic/programmable
electronic safety-related 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) 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 61508-2 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 interfaces to other parts of IEC 61508 have been clarified and duplication of requirements in other Parts has been removed;
- c) The differentiation between the required Safety Integrity Level (SIL) and the achieved Systematic Capability (SC) has been clarified;
- d) Semiconductor content moved to the new IEC 61508-2-1. This includes the old annex E, annex F and the semiconductor V-model.
- e) Requirements on diagnostic functions (7.4.12) have been added;
- f) Requirements on common cause failures (Annex E) have been added;
- g) Reference to software off-line support tools has been added (7.4.6.4);
- h) Requirements on traceability have been clarified (Annex B);
- i) 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.

INTRODUCTION

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

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

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

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

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

This document

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

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

- sets target failure rates for safety functions carried out by E/E/PE safety-related systems, which are linked to the safety integrity levels;

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

NOTE 4 It may 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 rate 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 concepts 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 2: Requirements for electrical/electronic/programmable electronic safety-related systems

1 Scope

1.1 This part of the IEC 61508 series

- a) is intended to be used only after a thorough understanding of IEC 61508-1, which provides the overall framework for the achievement of functional safety;
- b) applies to any safety-related system, as defined by IEC 61508-1, that contains at least one electrical, electronic or programmable electronic element;
- c) applies to all elements within an E/E/PE safety-related system (including sensors, actuators and the operator interface);
- d) specifies how to refine the E/E/PE system safety requirements specification, developed in accordance with IEC 61508-1 (comprising the E/E/PE system safety functions requirements specification and the E/E/PE system safety integrity requirements specification), into the E/E/PE system design requirements specification;
- e) specifies the requirements for activities that are to be applied during the design and manufacture of the E/E/PE safety-related systems (i.e. establishes the E/E/PE system safety lifecycle model) except software, which is dealt with in IEC 61508-3 (see Figures 2 to 4). These requirements include the application of techniques and measures that are graded against the safety integrity level, for the avoidance of, and control of, faults and failures;
- f) specifies the information necessary for carrying out the installation, commissioning and final safety validation of the E/E/PE safety-related systems;
- g) does not apply to the operation and maintenance phase of the E/E/PE safety-related systems – this is dealt with in IEC 61508-1 – however, IEC 61508-2 does provide requirements for the preparation of information and procedures needed by the user for the operation and maintenance of the E/E/PE safety-related systems;
- h) specifies requirements to be met by the organisation carrying out any modification of the E/E/PE safety-related systems;

NOTE 1 This part of IEC 61508 is mainly directed at suppliers and/or in-company engineering departments, hence the inclusion of requirements for modification.

NOTE 2 The relationship between IEC 61508-2 and IEC 61508-3 is illustrated in Figure 4.

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

NOTE The functional safety of an E/E/PE safety-related system can only be achieved when all related requirements are met. Therefore, it is important that all related requirements are carefully considered and adequately referenced.

1.3 Figure 1 shows the overall framework of the IEC 61508 series and indicates the role that IEC 61508-2 plays in the achievement of functional safety for E/E/PE safety-related systems. Annex A of IEC 61508-6 describes the application of IEC 61508-2 and IEC 61508-3.

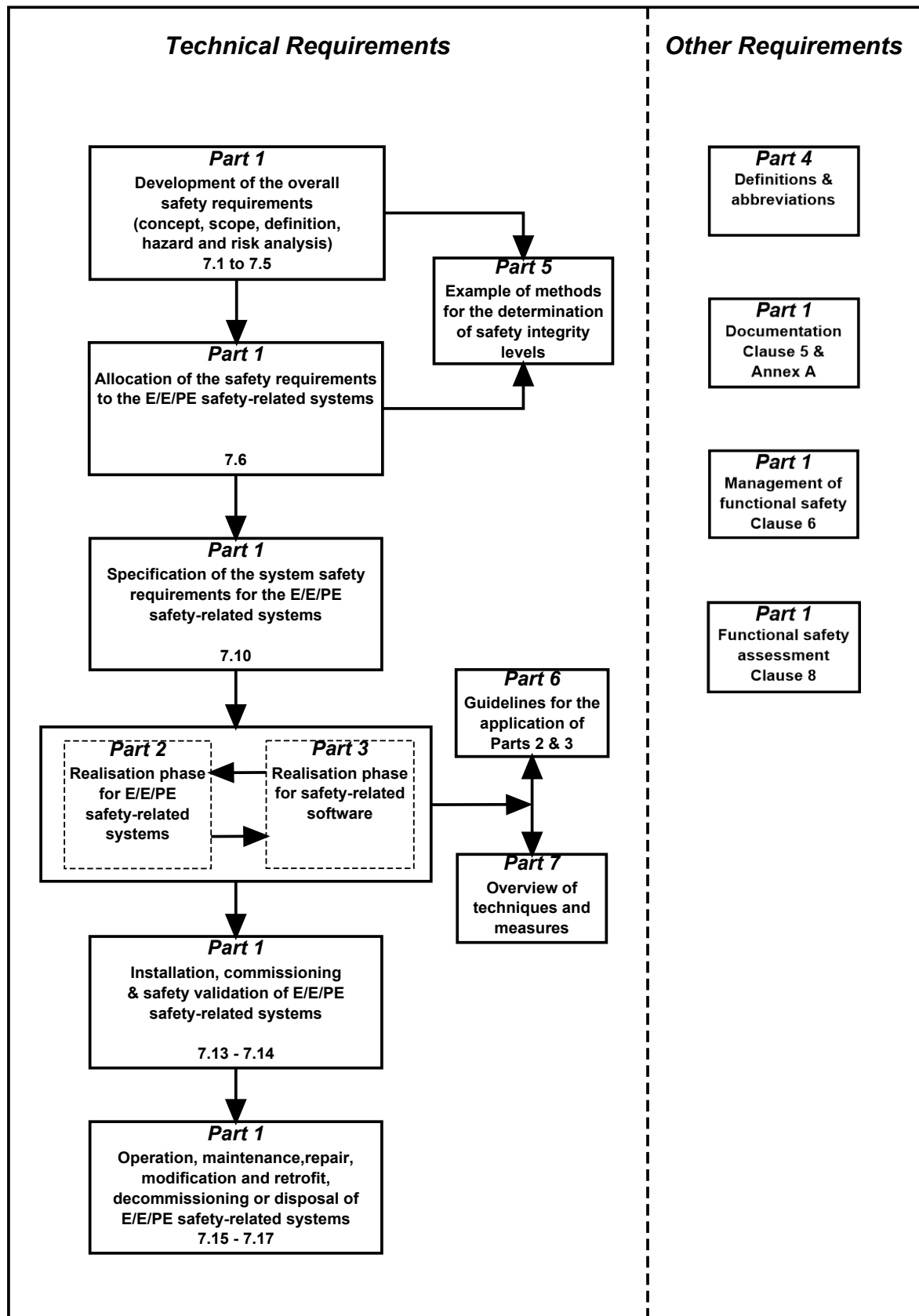


Figure 1 – Overall framework of the IEC 61508 series

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 60947-5-1, *Low-voltage switchgear and controlgear – Part 5-1: Control circuit devices and switching elements – Electromechanical control circuit devices*

IEC 61000-1-2, *Electromagnetic compatibility (EMC) – Part 1-2: General – Methodology for the achievement of functional safety of electrical and electronic systems including equipment with regard to electromagnetic phenomena*

IEC 61508-1:202X, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements*

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 61508-7:202X, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 7: Overview of techniques and measures*

IEC 61784-3, *Industrial communication networks – Profiles – Part 3: Functional safety fieldbuses – General rules and profile definitions*

IEC 62280, *Railway applications – Communication, signalling and processing systems – Safety-related communication in closed transmission systems*

IEC Guide 104:1997, *The preparation of safety publications and the use of basic safety publications and group safety publications*

ISO/IEC Guide 51:1999, *Safety aspects – Guidelines for their inclusion in standards*

EN 50205, *Relays with forcibly guided (mechanically linked) contacts*

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

The requirements for conformance to this document are as detailed in Clause 4 of IEC 61508-1.

5 Documentation

The requirements for documentation are as detailed in Clause 5 of IEC 61508-1.

6 Additional requirements for management of functional safety for E/E/PE system

The requirements for management of functional safety are as detailed in Clause 6 of IEC 61508-1.

6.1 Objectives

The objectives are as detailed in 6.1 of IEC 61508-1.

6.2 Requirements

6.2.1 The requirements are as detailed in 6.2 of IEC 61508-1 and apply with the following additional requirements.

6.2.2 The functional safety planning shall define the strategy for E/E/PE system procurement, development, integration, verification, validation and modification to the extent required by the systematic capability and safety integrity level of the safety functions implemented by the E/E/PE safety-related system.

NOTE The philosophy of this approach is to use the functional safety planning as an opportunity to customize this document to take account of the required safety integrity for each safety function implemented by the E/E/PE safety-related system.

6.2.3 The configuration management requirements are as detailed in IEC 61508-1 6.2 with the following additional requirements:

- a) apply administrative and technical controls throughout the safety lifecycle to ensure that the specified requirements for the E/E/PE safety-related system are satisfied;
- b) guarantee that all necessary operations have been carried out to demonstrate that the required systematic capability of the E/E/PE safety-related system is achieved;
- c) maintain accurately and with unique identification all configuration items which are necessary to meet the safety integrity requirements of the E/E/PE safety-related system. Configuration items include at least the following: safety analysis and requirements; design documents; test plans and results; verification documents; pre-existing elements and packages which are incorporated into the E/E/PE safety-related system; all tools and development environments which are used to create or test, or carry out any action on, the hardware, firmware or software elements of the E/E/PE safety-related system;
- d) apply modification procedures to authorize, conduct and document modification requests and prevent unauthorized modifications and if explicit combination of versions is necessary, modification procedures need to ensure that versions match for the intended purpose;
- e) formally document the release of the E/E/PE system. Copies of all associated documentation and version of design shall be kept to permit maintenance and modification throughout the operational lifetime of the E/E/PE system.

7 E/E/PE system safety lifecycle requirements

7.1 General

7.1.1 Objectives and requirements – general

7.1.1.1 This subclause sets out the objectives and requirements for the E/E/PE system safety lifecycle phases.

NOTE The objectives and requirements for the overall safety lifecycle, together with a general introduction to the structure of this document, are given in IEC 61508-1.

7.1.1.2 For all phases of the E/E/PE system safety lifecycle, Table 1 indicates

- the objectives to be achieved;

- the scope of the phase;
- a reference to the subclause containing the requirements;
- the required inputs to the phase;
- the outputs required to comply with the subclause.

7.1.2 Objectives

7.1.2.1 The first objective of the requirements of this subclause is to structure, in a systematic manner, the phases in the E/E/PE system safety lifecycle that shall be considered in order to achieve the required functional safety of the E/E/PE safety-related systems.

7.1.2.2 The second objective of the requirements of this subclause is to document all information relevant to the functional safety of the E/E/PE safety-related systems throughout the E/E/PE system safety lifecycle.

7.1.3 Requirements

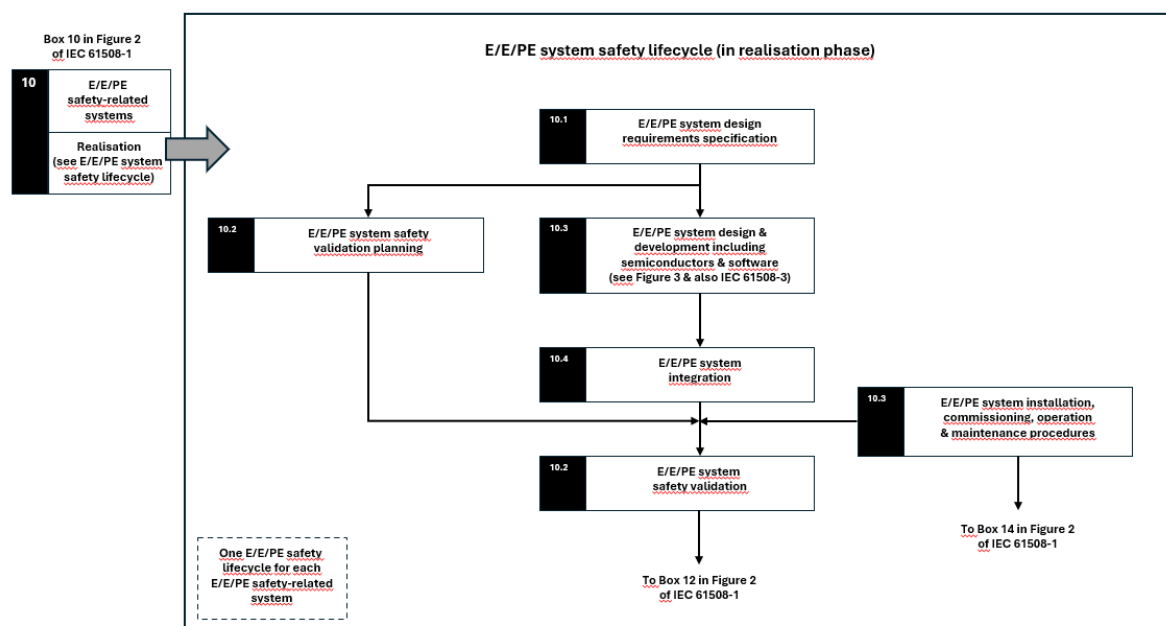
7.1.3.1 The E/E/PE system safety lifecycle that shall be used in claiming conformance with this document is that specified in Figure 2.

7.1.3.2 The procedures for management of functional safety (see Clause 6) shall run in parallel with the E/E/PE system safety lifecycle phases.

7.1.3.3 Each phase of the E/E/PE system safety lifecycle shall be divided into elementary activities, with the scope, inputs and outputs specified for each phase (see Table 1).

7.1.3.4 Unless justified as part of the management of functional safety activities (see Clause 6 of IEC 61508-1), the outputs of each phase of the E/E/PE system safety lifecycle shall be documented (see Clause 5 of IEC 61508-1).

7.1.3.5 The outputs for each E/E/PE system safety lifecycle phase shall meet the objectives and requirements specified for each phase (see 7.2 to 7.9).



NOTE 1 See also IEC 61508-6, A.2 b).

NOTE 2 This figure shows only those phases of the E/E/PE system safety lifecycle that are within the realisation phase of the overall safety lifecycle. It is possible, that the complete E/E/PE system safety lifecycle also contains

instances, specific to the E/E/PE safety-related system, of the subsequent phases of the overall safety lifecycle (Boxes 12 to 16 in Figure 2 of IEC 61508-1).

Figure 2 – E/E/PE system safety lifecycle (in realisation phase)

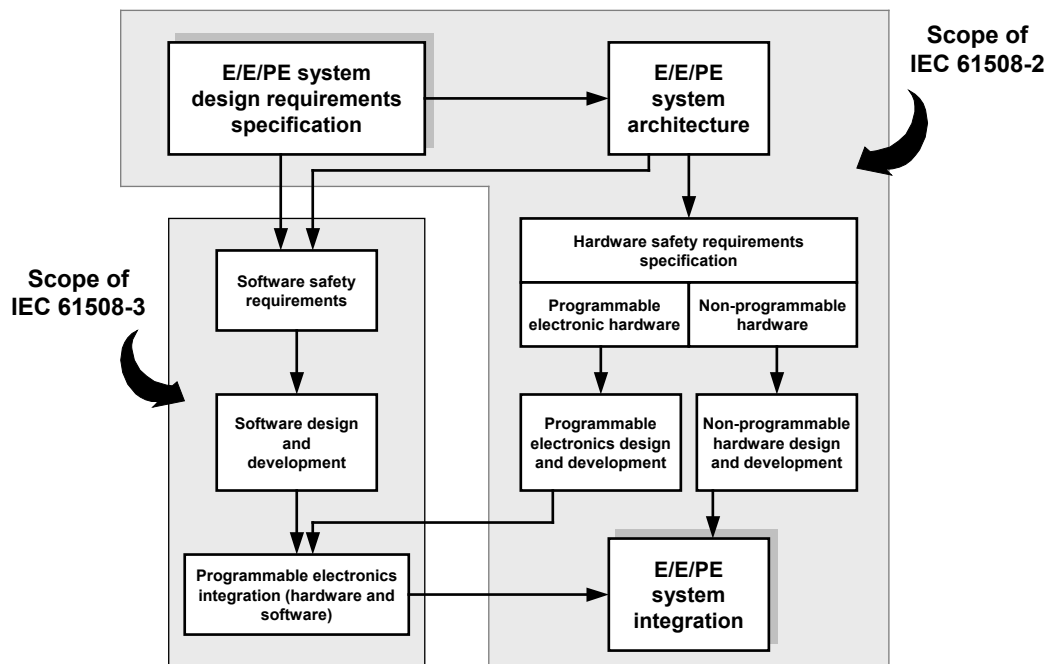


Figure 3 – Relationship between and scope of IEC 61508-2 and IEC 61508-3

Table 1 – Overview – realisation phase of the E/E/PE system safety lifecycle

Safety lifecycle phase or activity		Objectives	Scope	Requirements sub-clause	Inputs	Outputs
Figure 2 box number	Activities					
10.1	E/E/PE system design requirements specification	To specify the design requirements for each E/E/PE safety-related system, in terms of the subsystems and elements (see 7.10.2 of IEC 61508-1)	E/E/PE safety-related system	7.2.2	E/E/PE system safety requirements specification (see IEC 61508-1, 7.10)	E/E/PE system design requirements specification, describing the equipment and architectures for the E/E/PE system
10.2	E/E/PE system safety validation planning	To plan the validation of the safety of the E/E/PE safety-related system	E/E/PE safety-related system	7.3.2	E/E/PE system safety requirements specification and E/E/PE system design requirements specification	Plan for the safety validation of the E/E/PE safety-related systems
10.3	E/E/PE system design & development including semiconductors & software (see IEC 61508-2-1, Figure A.1 & also IEC 61508-3)	To design and develop the E/E/PE safety-related system (including semiconductors if appropriate) to meet the E/E/PE system design requirements specification (with respect to the safety functions requirements and the safety integrity requirements (see 7.2))	E/E/PE safety-related system	7.4.2 to 7.4.11	E/E/PE system design requirements specification	Design of the E/E/PE safety-related system in conformance with the E/E/PE system design requirements specification Plan for the E/E/PE system integration test PE system architectural information as an input to the software requirements specification

Safety lifecycle phase or activity		Objectives	Scope	Requirements sub-clause	Inputs	Outputs
Figure 2 box number	Activities					
10.4	E/E/PE system integration	To integrate and test the E/E/PE safety-related system	E/E/PE safety-related system	7.5.2	E/E/PE system design E/E/PE system integration test plan Programmable electronics hardware and software	Fully functioning E/E/PE safety-related systems in conformance with the E/E/PE system design Results of E/E/PE system integration tests
10.5	E/E/PE system installation, commissioning, operation and maintenance procedures	To develop procedures to ensure that the required functional safety of the E/E/PE safety-related system is maintained during operation and maintenance	E/E/PE safety-related system EUC	7.6.2	E/E/PE system design requirements specification E/E/PE system design	E/E/PE system installation, commissioning, operation and maintenance procedures for each individual E/E/PE system
10.6	E/E/PE system safety validation	To validate that the E/E/PE safety-related system meets, in all respects, the requirements for safety in terms of the required safety functions and safety integrity	E/E/PE safety-related system	7.7.2	E/E/PE system safety requirements specification and E/E/PE system design requirements specification Plan for the safety validation of the E/E/PE safety-related systems	Fully safety validated E/E/PE safety-related systems Results of E/E/PE system safety validation
–	E/E/PE system modification	To make corrections, enhancements or adaptations to the E/E/PE safety-related system, ensuring that the required safety integrity is achieved and maintained	E/E/PE safety-related system	7.8.2	E/E/PE system design requirements specification	Results of E/E/PE system modification
–	E/E/PE system verification	To test and evaluate the outputs of a given phase to ensure correctness and consistency with respect to the products and standards provided as input to that phase	E/E/PE safety-related system	7.9.2	As above – depends on the phase Plan for the verification of the E/E/PE safety-related systems for each phase	As above – depends on the phase Results of the verification of the E/E/PE safety-related systems for each phase
–	E/E/PE system functional safety assessment	To investigate and arrive at a judgement on the functional safety achieved by the E/E/PE safety-related system	E/E/PE safety-related system	8	Plan for E/E/PE system functional safety assessment	Results of E/E/PE system functional safety assessment

7.2 E/E/PE system design requirements specification

NOTE This phase is Box 10.1 of Figure 2.

7.2.1 Objective

The objective of the requirements of this subclause is to specify the design requirements for each E/E/PE safety-related system, in terms of the subsystems and elements.

NOTE The E/E/PE system design requirements specification can normally be derived from the E/E/PE system safety requirements specification by decomposing the safety functions and allocating parts of the safety function to subsystems (for example groups of sensors, logic solvers or actuators). The requirements for the subsystems can be included in the E/E/PE system design requirements specification or can be separate and referenced from the E/E/PE system design requirements specification. Subsystems can be further decomposed into elements and architectures to satisfy the design and development requirements of 7.4. The requirements for these elements can

be included in the requirements for the subsystems or can be separate and referenced from the subsystem requirements.

7.2.2 General

7.2.2.1 The specification of the E/E/PE system design requirements shall be derived from the E/E/PE system safety requirements specification, specified in 7.10 of IEC 61508-1.

NOTE Caution should be exercised if non-safety functions and safety functions are implemented in the same E/E/PE safety-related system. While this is allowed in this document, it can lead to greater complexity and increase the difficulty in carrying out E/E/PE safety lifecycle activities (for example design, validation, functional safety assessment and maintenance). See also 7.4.2.3.

7.2.2.2 The specification of the E/E/PE system design requirements shall be expressed and structured in such a way that they are:

- a) clear, precise, unambiguous, verifiable, testable, maintainable and feasible;
- b) written to aid comprehension by those who are likely to utilise the information at any phase of the E/E/PE safety lifecycle; and
- c) traceable to the E/E/PE system safety requirements specification.

NOTE The concept of traceability is explained in IEC 61508-7 cl. B.1.5.

7.2.3 E/E/PE system design requirements specification

7.2.3.1 The specification of the E/E/PE system design requirements shall contain design requirements relating to safety functions (see 7.2.3.2) and design requirements relating to safety integrity (see 7.2.3.3).

7.2.3.2 The specification of the E/E/PE system design requirements shall contain details of all the hardware and software and the interfaces necessary to implement the required safety functions as specified by the E/E/PE system safety functions requirements specification (see 7.10.2.6 of IEC 61508-1). For each safety function the specification shall include:

- a) requirements for the subsystems and requirements for their hardware and software elements as appropriate;
- b) requirements for the integration of the subsystems and their hardware and software elements to meet the E/E/PE system safety functions requirements specification;
- c) throughput performance that enables response time requirements to be met;
- d) accuracy and stability requirements for measurements and controls;
- e) E/E/PE safety-related system and operator interfaces;
- f) interfaces between the E/E/PE safety-related systems and any other systems (either within, or outside, the EUC);
- g) all modes of behaviour of the E/E/PE safety-related systems, in particular, failure behaviour and the required response (for example alarms, automatic shut-down) of the E/E/PE safety-related systems;
- h) the significance of all hardware/software interactions and, where relevant, any required constraints between the hardware and the software;

NOTE Where these interactions are not known before finishing the design, only general constraints can be stated.

- i) any limiting and constraint conditions for the E/E/PE safety-related systems and their associated elements, for example timing constraints or constraints due to the possibility of common cause failures;
- i) any requirements related to the procedures for starting-up and restarting the E/E/PE safety-related systems;
- j) any specific requirements on installation, commissioning, operation, maintenance, and decommissioning;
- k) measures to reduce the possibility and effect of reasonably foreseeable misuse,.

7.2.3.3 The specification of the E/E/PE system design requirements shall contain details, relevant to the design, to achieve the safety integrity level and the required target failure rate for the safety function, as specified by the E/E/PE system safety integrity requirements specification (see 7.10.2.7 of IEC 61508-1), including:

- a) the architecture of each subsystem required to meet the architectural constraints on the hardware safety integrity (see 7.4.4);

NOTE 1 The description of subsystems can be a very general view on architecture. However, a more detailed description can be beneficial (see IEC 61508-1 clause 7.6.2.3).

- b) all relevant reliability modelling parameters such as the required proof testing frequency of all hardware elements necessary to achieve the target failure rate;

NOTE 2 Information on the specific application can be important. This is particularly important for maintenance, where the specified proof test interval cannot be less than can be reasonably expected for the particular application. For example, the time between services that can be realistically attained for mass-produced items used by the public is likely to be greater than in a more controlled application.

- c) the actions taken in the event of a dangerous failure being detected by diagnostic functions;
- d) the requirements, constraints, functions and facilities to enable the proof testing of the E/E/PE hardware to be undertaken;
- e) the capabilities of equipment used to meet the extremes of all environmental conditions (e.g. temperature, humidity, mechanical, electrical) that are specified as required during the E/E/PE system safety lifecycle including manufacture, storage, transport, testing, installation, commissioning, operation and maintenance;
- f) the electromagnetic immunity levels.

NOTE 1 See IEC 61000-1-2 for guidance on identifying appropriate levels for specific applications.

NOTE 2 The required immunity levels can vary for different elements of the safety-related system, depending on physical location and power supply arrangements.

NOTE 3 Generic application-specific EMC standards (e.g. IEC 61000-6-2) or product family standards (e.g. IEC 60947-5-2) not intended for the achievement of functional safety provide typical test requirements for the specific intended environment. However, it is important to understand that these requirements are intended to support and achieve adequate operation under normal conditions while accepting that the equipment or system can be temporarily disturbed. The content of the generic application-specific or product-specific EMC standards do not fully address the needs for systems performing safety-related functions.

NOTE 4 For some specific product families or applications, standards exist that can contain requirements derived from the approach prescribed in IEC 61000-1-2 (e.g. for industrial see IEC 61326-3-1 or IEC 61000-6-7). If no applicable EMC standard for achieving functional safety exists, the approach of IEC 61000-1-2 can be applied.

NOTE 5 Guidance on electromagnetic immunity levels is located in IEC 61508-7, A.11.3.

NOTE 6 IEEE 1848-2020 supplements IEC 61000-1-2:2016 for the achievement of functional safety for E/E/PE safety-related systems regarding electromagnetic disturbances. This is achieved by providing a set of practical techniques and measures for helping to manage such disturbances throughout all relevant safety lifecycle phases, including functional safety assurance activities (see Part 4, clause 3.8.18).

- g) the quality assurance/quality control measures necessary to safety management (see 6.2.5 of IEC 61508-1);

7.2.3.4 The E/E/PE system design requirements specification shall be completed in detail as the design progresses and updated as necessary after modification.

7.2.3.5 For the avoidance of mistakes during the development of the specification for the E/E/PE system design requirements, an appropriate group of techniques and measures according to Table B.1 shall be used.

7.2.3.6 The implications imposed on the architecture by the E/E/PE system design requirements shall be considered.

NOTE This can include the consideration of the simplicity of the implementation to achieve the required safety integrity level (including architectural considerations and apportionment of functionality to configuration data or to the embedded system).

7.2.3.7 The E/E/PE system design requirements specification shall express the required safety properties of the **E/E/PE system**, but not of the project as this is covered by safety planning (see clause 6).

Additional to the previous clauses the following shall be specified:

- 1) functions that enable the EUC to achieve or maintain a safe state;
- 2) functions related to the detection, annunciation and management of faults;
- 3) functions related to periodic testing of the safety functions on-line and off-line;
- 4) functions that allow the system to be safely modified;
- 5) interfaces to non safety-related functions;
- 6) capacity and response time performance;
- 7) interfaces between software and other elements of the PE system;
- 8) safety-related communications (see 7.4.11) including data definition (see IEC 61508-3 clause 7.2.2.12)
- 9) any limiting and constraint conditions for the E/E/PE safety-related systems and their associated elements, for example timing constraints or independence constraints (including cascading and common cause failures);
- 10) all necessary data including permitted range and authorized combinations of operational parameters.
- 11) human-system interfaces

7.3 E/E/PE system safety validation planning

NOTE This phase is Box 10.2 of Figure 2. It can normally be carried out in parallel with E/E/PE system design and development (see 7.4).

7.3.1 Objective

The objective of the requirements of this subclause is to plan the validation of the safety of the E/E/PE safety-related system.

7.3.2 Requirements

7.3.2.1 Planning shall be carried out to specify the steps (both procedural and technical) that are to be used to demonstrate that the E/E/PE safety-related system satisfies the E/E/PE system safety requirements specification (see 7.10 of IEC 61508-1) and the E/E/PE system design requirements specification (see 7.2).

7.3.2.2 Planning for the validation of the E/E/PE safety-related system **be in accordance with 7.8 of IEC 61508-1.**

7.4 E/E/PE system design and development

NOTE This phase is Box 10.3 of Figure 2. It will normally be carried out in parallel with E/E/PE system safety validation planning (see 7.3).

7.4.1 Objective

The objective of the requirements of this subclause is to design and develop the E/E/PE safety-related system (including semiconductors if appropriate, see IEC 61508-4, 3.2.15) to meet the E/E/PE system design requirements specification (with respect to the safety functions requirements and the safety integrity requirements (see 7.2).

7.4.2 General requirements

7.4.2.1 The design of the E/E/PE safety-related system shall be created in accordance with the E/E/PE system design requirements specification (see 7.2.3), taking into account all the requirements of 7.2.3.

7.4.2.2 The design of the E/E/PE safety-related system (including the overall hardware and software architecture, sensors, actuators, programmable electronics, semiconductors,

embedded software, application software, data etc.), shall meet all of the following requirements:

- a) the requirements for hardware safety integrity comprising;
 - the architectural constraints on hardware safety integrity (see 7.4.4), and
 - the requirements for quantifying the effect of random failures (see 7.4.5);
- b) the requirements for semiconductors as outlined in IEC 61508-2-1 (under development); the requirements for systematic safety integrity (systematic capability), which can be met by achieving one of the following compliance routes:
 - Route 1_S: compliance with the requirements for the avoidance of systematic faults (see 7.4.6 and IEC 61508-3) and the requirements for the control of systematic faults (see 7.4.7 and IEC 61508-3), or
 - Route 2_S: compliance with the requirements for evidence that the equipment is proven in use (see 7.4.10), or
 - Route 3_S (pre-existing software elements only): compliance with the requirements of IEC 61508-3, 7.4.2.14;

NOTE 1 The “S” subscript in the above routes designates systematic safety integrity to distinguish it from Route 1_H, and Route 2_H for hardware safety integrity.

NOTE 2 While they are not software, route 3S can be applied to HDL artefacts as software like artefacts.

- c) the requirements for system behaviour on detection of a fault (see 7.4.8);
- d) the requirements for data communication processes (see 7.4.11);
- e) requirements for diagnostic functions in conformance with 7.4.12.

7.4.2.3 Where an E/E/PE safety-related system is to implement both safety and non-safety functions, then all the hardware and software shall be treated as safety-related unless it can be shown that the implementation of the safety and non-safety functions is sufficiently independent (i.e. that the failure of any non-safety-related functions does not cause a dangerous failure of the safety-related functions).

NOTE 1 Sufficient independence of implementation can be established by showing that the probability of a dependent failure between the non-safety and safety-related parts can be sufficiently low in comparison with the highest safety integrity level associated with the safety functions involved.

NOTE 2 Caution can be exercised if non-safety functions and safety functions are implemented in the same E/E/PE safety-related system. While this can be allowed in this document, it can lead to greater complexity and increase the difficulty in carrying out E/E/PE system safety lifecycle activities (for example design, validation, functional safety assessment and maintenance).

7.4.2.4 The requirements for hardware and software shall be determined by the safety integrity level of the safety function having the highest safety integrity level unless it can be shown that the implementation of the safety functions of the different safety integrity levels is sufficiently independent.

NOTE 1 Sufficient independence of implementation can be established by showing that the probability of a dependent failure between the parts implementing safety functions of different integrity levels can be sufficiently low in comparison with the highest safety integrity level associated with the safety functions involved.

NOTE 2 Where several safety functions are implemented in an E/E/PE safety-related system then it can be necessary to consider the possibility that a single fault can cause a failure of several safety functions. In such a situation, it can be appropriate to determine the requirements for hardware and software on the basis of a higher safety integrity level than is associated with any one of the safety functions, depending on the risk associated with such a failure.

7.4.2.5 When independence between safety functions is required (see 7.4.2.3 and 7.4.2.4) then the following shall be documented during the design:

- a) the method of achieving independence;
- b) the justification of the method.

EXAMPLE Addressing foreseeable failure modes, that can undermine independence, and their failure rates, use of FMECA or dependant failure analysis.

7.4.2.6 The requirements for safety-related software (see IEC 61508-3) shall be made available to the developer of the E/E/PE safety-related system.

7.4.2.7 The developer of the E/E/PE safety-related system shall review the requirements for safety-related software and hardware and interfaces between the two to ensure that they are adequately specified. In particular, the E/E/PE system developer shall consider the following:

- a) safety functions;
- b) E/E/PE safety-related system safety integrity requirements;
- c) equipment and operator interfaces.

7.4.2.8 The E/E/PE safety-related system design documentation shall specify those techniques and measures necessary during the E/E/PE system safety lifecycle phases to achieve the safety integrity level.

7.4.2.9 The E/E/PE safety-related system design documentation shall justify the techniques and measures chosen to form an integrated set that satisfies the required safety integrity level.

NOTE The adoption of an overall approach employing independent type approval of the E/E/PE safety-related systems (including sensors, actuators, etc) for hardware and software, diagnostic tests and programming tools, and using appropriate languages for software wherever possible, can potentially reduce the complexity of E/E/PE system application engineering.

7.4.2.10 The hardware-software interface shall be described in a way that specifies the hardware and software interaction and is consistent with the E/E/PE system design requirements specification (see 7.2.3).

The objective of the interface specification is to specify the safety-related functionality, precautions against interference and diagnostic mechanisms.

7.4.2.11 The hardware-software interface specification shall include the component's hardware devices that are controlled by software and hardware resources that support the execution of software.

NOTE The hardware-software interface specification can be an information provided as part of a larger document.

The hardware-software interface specification shall include the following characteristics:

- a) the relevant operating modes of hardware devices and the relevant configuration parameters;

EXAMPLE 1 Operating modes of hardware devices can be default, unit or test modes.

EXAMPLE 2 Configuration parameters can be: activation/deactivation of safety-related functions, gain control, band pass frequency or clock prescaler.

- b) the hardware features that ensure the independence between elements and that support software partitioning;

EXAMPLE Memory protection units.

- c) shared and exclusive use of hardware resources and measures for synchronization of the access;

EXAMPLE Memory mapping, allocation of registers, timers, interrupts, I/O ports.

- d) the hardware diagnostic features relevant to hardware-software interface;

NOTE For semiconductors the hardware diagnostic features to be used or configured by software may be described in safety manual instead of hardware-software interface specification.

EXAMPLE Detection of configuration registers manipulation.

- e) the access mechanism to hardware devices;

EXAMPLE Access of A/D converter with serial or parallel communication.

- f) the timing constraints defined for each function;

- g) specification of all data transferred over the interface, their functions and value ranges.

h) the hardware diagnostic features to be used or configured by software shall be defined (see IEC 61508-2, 7.4.2.2 and following subclauses);

EXAMPLE Detection of over-current, short-circuit or over-temperature.

i) the diagnostic features concerning the hardware, to be implemented in software.

7.4.2.13 The design shall be based on a decomposition into subsystems with each subsystem having a specified design and set of integration tests (see 7.5.2).

NOTE 1 A subsystem can be considered to comprise a single element or any group of elements. See IEC 61508-4 for definitions. A complete E/E/PE safety-related system can be made up from a number of identifiable and separate subsystems, which when put together implement the safety function under consideration. A subsystem can have more than one channel (see 7.4.9.3 and 7.4.9.4).

NOTE 2 Wherever practicable, existing verified subsystems or elements can be used in the implementation. This statement is generally valid only if there is almost 100 % mapping of the existing subsystem or element functionality, capacity and performance on to the new requirement or the verified subsystem or element is structured in such a way that the user can be able to select only the functions, capacity or performance required for the specific application. Excessive functionality, capacity or performance can be detrimental to system safety if the existing subsystem or element is overly complicated or has unused features and if protection against unintended functions cannot be obtained.

7.4.2.14 When the initial design of the E/E/PE safety-related system has been completed, an analysis shall be undertaken to determine whether any reasonably foreseeable failure of the E/E/PE safety-related system could cause a hazardous situation or place a demand on any other risk control measure. If any reasonably foreseeable failure could have either of these effects, then the first priority shall be to change the design of the E/E/PE safety-related system to avoid such failure modes. If this cannot be done, then measures shall be taken to reduce the likelihood of such failure modes to a level commensurate with the target failure rate. These measures shall be subject to the requirements of this document.

NOTE The intention of this clause is to identify failure modes of the E/E/PE safety-related system that place a demand on other risk control measures. There can be cases where the failure rate of the specified failure modes cannot be reduced and either a new safety function can be required or the SIL of the other safety functions reconsidered taking into account the failure rate.

7.4.2.15 De-rating should be considered for all hardware components. Justification for operating any hardware components at their limits shall be documented (see IEC 61508-1, Clause 5).

NOTE Where de-rating is appropriate, a de-rating factor of approximately two-thirds is typical.

7.4.2.16 Where the design of an E/E/PE safety-related system includes one or more semi-conductors to implement a safety function, a system safety lifecycle (see 7.1.3.1) shall be used.

7.4.3 Synthesis of elements to achieve the required systematic capability

NOTE The requirements of this subclause are also relevant for software elements and extended by the specific requirements in IEC 61508-3 clause 7.4.2.11.

7.4.3.1 To meet the requirements for systematic capability, the designated safety-related E/E/PE system may, in the circumstances described in this subclause, be partitioned into elements of different systematic capability.

NOTE 1 The systematic capability of an element determines the potential for systematic faults of that element to lead to a failure of the safety function. The concept of systematic capability of an element can be applicable to both hardware and software elements.

NOTE 2 Subclause 7.6.2.7 of IEC 61508-1 recognises the value of independence and diversity at the level of a safety function and the E/E/PE safety-related system to which it can be allocated. These concepts can also be applied at the detailed design level where an assembly of elements implementing a safety function can potentially achieve a better systematic performance than the individual elements.

7.4.3.2 For an element of systematic capability SC N (N=1, 2, 3), where a systematic fault of that element does not cause a failure of the specified safety function but does so only in combination with a second systematic fault of another element of systematic capability SC N, the systematic capability of the combination of the two elements can be treated as having a systematic capability of SC (N + 1) providing that:

– sufficient independence exists between the two elements (see 7.4.3.4) and

integration activities of the combined elements shall meet systematic capability of SC (N + 1).

NOTE 1 The independence of elements can be assessed only when the specific application of the elements is known in relation to the defined safety functions.

NOTE 2 It is important to distinguish between (1) the *end-to-end safety function* that can be supported by one or more elements and (2) the *element safety function* of each of the supporting elements. Where two elements combine to achieve a higher systematic capability in combination, each of the paired elements can be capable of preventing/mitigating the hazardous event, but the paired elements are not required to have identical element safety functions.

EXAMPLE An Engine Control System can have a number of safety functions, one of those being an end-to-end safety function with the task "prevent excessive acceleration".

The end-to-end safety function can be implemented by two elements, each of systematic capability SC1. These two elements (Element #1 and Element #2) can be sufficiently independent to meet the Synthesis of Elements requirements specified in IEC 61508-2, clause 7.4.3.

It is possible that the element safety function of Element #1 is not identical to the element safety function Element #2 but both element safety functions form part of the end-to-end safety function. That is, each element safety function can be an integral part of the end-to-end safety function. Both element safety functions can measure the acceleration in different ways. In this case, the combination of the two Elements can be treated as having a systematic capability of SC 2, providing that sufficient independence exists between the two elements.

7.4.3.3 The systematic capability that can be claimed for a combination of elements each of systematic capability SC N can at most be SC (N+1). A SC N element may be used in this way only once. It is not permitted to achieve SC (N+2) and higher by successively building assemblies of SC N elements.

7.4.3.4 Sufficient independence, in the design between elements and in the application of elements, shall be justified by common cause failure analysis (refer to Annex E) to show that the likelihood of interference between elements and between the elements and the environment is sufficiently low in comparison with the safety integrity level of the safety function under consideration.

NOTE 1 For systematic capability, with respect to hardware design, realisation, operation and maintenance, possible approaches to the achievement of sufficient independence can include:

- functional diversity: use of different approaches to achieve the same results;
- diverse technologies: use of different types of equipment to achieve the same results;
- common parts/services: ensuring that there are no common parts or services or support systems (for example power supplies) whose failure could result in a dangerous mode of failure of all systems;
- common procedures: ensuring that there are no common operational, maintenance or test procedures.

NOTE 2 Independence of application means that it is not possible that elements adversely interfere with each other's execution behaviour such that a dangerous failure would occur.

NOTE 3 For independence of software elements see 7.4.2.8 and 7.4.2.9 of IEC 61508-3.

A systematic approach and the methodology are described in Annex E.

7.4.4 Hardware safety integrity architectural constraints

NOTE 1 The equation, relating to the hardware safety integrity constraints, are specified in Annex C and the safety integrity constraints are summarized in Table 2 and Table 3

NOTE 2 Clause A.2 of IEC 61508-6 gives an overview of the necessary steps in achieving required hardware safety integrity, and shows how this subclause relates to other requirements of this document.

In the context of hardware safety integrity, the highest safety integrity level that can be claimed for a safety function is limited by the hardware safety integrity constraints which shall be achieved by implementing one of two possible routes (to be implemented at system or subsystem level):

- Route 1_H based on hardware fault tolerance and safe failure fraction concepts; or,
- Route 2_H based on reliability data from field feedback from end users, increased confidence levels and hardware fault tolerance of the subsystem for specified safety integrity levels.

Application standards based on the IEC 61508 series may indicate the preferred Route (i.e. Route 1_H or Route 2_H).

NOTE 3 The “H” subscript in the above routes designates hardware safety integrity to distinguish it from Route 1_S, Route 2_S and Route 3_S for systematic safety integrity.

It is assumed that when a safe state needs to be achieved as a consequence of the detection of a fault, either:

- there is only one safe state to be achieved, or
- there are multiple possibly safe states to be achieved.

NOTE 4 For a system with multiple possible safe states (to be achieved after the detection of a fault) which can be mutually exclusive, or which can have different priorities, then the overall safety has to be considered taking into account the priority of the multiple states and the system status at the time of the detection of the fault.

7.4.4.1 General requirements

7.4.4.1.1 With respect to the hardware fault tolerance requirements

- a) a hardware fault tolerance of N means that N+1 is the minimum number of faults that could cause a loss of the safety function (for further clarification see Note 1 and Table 2 and Table 3). In determining the hardware fault tolerance no account shall be taken of other measures that may control the effects of faults such as diagnostics; and
- b) where one fault directly leads to the occurrence of one or more subsequent faults, these are considered as a single fault;
- c) when determining the hardware fault tolerance achieved, certain faults may be excluded, provided that the likelihood of them occurring is very low in relation to the safety integrity requirements of the subsystem. Any such fault exclusions shall be justified and documented (see Note 3).

The constraints on hardware safety integrity have been included in order to achieve a sufficiently robust architecture, taking into account the level of element and subsystem complexity (see 7.4.4.1.2 and 7.4.4.1.3). The highest allowable safety integrity level for the safety function implemented by the E/E/PE safety-related system, derived through applying these requirements, is the maximum that is permitted to be claimed for the safety function even though, in some cases reliability calculations show that a higher safety integrity level could be achieved.

NOTE 1 Even if the hardware fault tolerance is achieved for all subsystems, a reliability calculation can still be necessary to demonstrate that the specified target failure rate has been achieved and this can require that the hardware fault tolerance be increased to meet design requirements.

NOTE 2 The hardware fault tolerance requirements can apply to the subsystem architecture that is used under normal operating conditions. The hardware fault tolerance requirements can be relaxed while the E/E/PE safety-related system is being repaired on-line, if the key parameters relating to any relaxation have been previously evaluated (for example MTTR compared to the probability of a demand).

NOTE 3 Certain faults can be excluded because if an element clearly has a very low probability of failure by virtue of properties inherent to its design and construction (for example, a mechanical actuator linkage), then it is still possible to not constrain (on the basis of hardware fault tolerance) the safety integrity of any safety function that uses the element.

NOTE 4 The choice of the route is application and sector dependent and the following can be considered when selecting the Route:

- a safe failure of one function can create a new hazard or be an additional cause for an existing hazard;
- it is possible that redundancy is not practicable for all functions;
- repair is not always possible or rapid (e.g. not feasible within a time that is negligible compared to the proof test interval).

NOTE 5 Special architecture requirements for ICs with on-chip redundancy are given in IEC 61508-2-1 Annex B (under development).

7.4.4.1.2 An element can be regarded as type A if, for the components required to achieve the element safety function

- a) the failure modes of all constituent components are well defined; and

b) the behaviour of the element under fault conditions can be completely determined; and

c) there is sufficient dependable failure data to show that the claimed rates of failure for detected and undetected dangerous failures are met (see 7.4.9.3 to 7.4.9.5).

NOTE Because a type A element benefits from sufficient failure data, it can be assessed with regards to Route 2H based on element reliability data (see 7.4.4).

7.4.4.1.3 An element shall be regarded as type B if, for the components required to achieve the element safety function,

a) the failure mode of at least one constituent component is not well defined; or

b) the behaviour of the element under fault conditions cannot be completely determined; or

c) there is insufficient dependable failure data to support claims for rates of failure for detected and undetected dangerous failures (see 7.4.9.3 to 7.4.9.5).

NOTE This means that if at least one of the components of an element itself satisfies the conditions for a type B element then that element will be regarded as type B rather than type A.

7.4.4.1.4 When estimating the safe failure fraction of an element, intended to be used in a subsystem having a hardware fault tolerance of 0, and which is implementing a safety function, or part of a safety function, operating in high demand mode or continuous mode of operation, credit shall only be taken for the diagnostic functions if:

– the sum of the diagnostic test interval and the time to perform the specified action to achieve or maintain a safe state is less than the process safety time; or,

– when operating in continuous or high demand mode of operation, the ratio of the diagnostic test rate to the demand rate equals or exceeds 100.

NOTE See Annex C.2.

7.4.4.1.5 When estimating the safe failure fraction of an element which,

– is implementing a safety function, or part of a safety function, operating in low demand mode of operation; or

– has a hardware fault tolerance greater than 0, and which is implementing a safety function, or part of a safety function, operating in high demand mode or continuous mode of operation,

credit shall only be taken for the diagnostic functions if the sum of the diagnostic test interval and the time to perform the repair of a detected failure is less than the MTTR used in the calculation to determine the achieved safety integrity for that safety function.

7.4.4.2 Route 1_H

7.4.4.2.1 To determine the maximum safety integrity level that can be claimed, with respect to a specified safety function, the following procedure shall be followed:

1) Define the subsystems making up the E/E/PE safety-related system.

2) For each subsystem determine the safe failure fraction for all elements in the subsystem separately (i.e. on an individual element basis with each element having a hardware fault tolerance of 0). In the case of redundant element configurations, the SFF may be calculated by taking into consideration the additional diagnostic functions that may be available (e.g. by comparison of redundant elements).

3) For each element, use the achieved safe failure fraction and hardware fault tolerance of 0 to determine the maximum safety integrity level that can be claimed from column 2 of Table 2 (for Type A elements) and column 2 of Table 3 (for Type B elements).

4) Use the method in 7.4.4.2.3 and 7.4.4.2.4 for determining the maximum safety integrity level that can be claimed for the subsystem.

5) The maximum safety integrity level that can be claimed for an E/E/PE safety-related system shall be determined by the subsystem that has achieved the lowest safety integrity level.