
Funkcijska varnost električnih/elektronskih/programljivih elektronskih varnostnih sistemov - 2. del: Zahteve za električne/elektronske/programljive elektronske varnostne sisteme

Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems

Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme - Teil 2: Anforderungen an sicherheitsbezogene elektrische/elektronische/programmierbare elektronische Systeme

Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité - Partie 2: Exigences pour les systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité

Ta slovenski standard je istoveten z: prEN IEC 61508-2:2025

ICS:

25.040.40	Merjenje in krmiljenje industrijskih postopkov	Industrial process measurement and control
35.240.50	Uporabniške rešitve IT v industriji	IT applications in industry

oSIST prEN IEC 61508-2:2025

en,fr,de



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 72, TC 77,TC 80,TC 108,SyC AAL,SyC SM,SC 41	HORIZONTAL FUNCTION(S):
ASPECTS CONCERNED: Safety	
<input checked="" type="checkbox"/> 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.	<input type="checkbox"/> 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.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47

CONTENTS

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

	IEC CDV 61508-2 ED3 © IEC 2025	3	65A/1165/CDV
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		

133

INTERNATIONAL ELECTROTECHNICAL COMMISSION

134

135

136

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

137

138

139

**Part 2: Requirements for electrical/electronic/programmable
electronic safety-related systems**

140

141

142

FOREWORD

143 1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising

144 all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international

145 co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and

146 in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports,

147 Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their

148 preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with

149 may participate in this preparatory work. International, governmental and non-governmental organizations liaising

150 with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for

151 Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.

152 2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international

153 consensus of opinion on the relevant subjects since each technical committee has representation from all

154 interested IEC National Committees.

155 3) IEC Publications have the form of recommendations for international use and are accepted by IEC National

156 Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC

157 Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any

158 misinterpretation by any end user.

159 4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications

160 transparently to the maximum extent possible in their national and regional publications. Any divergence between

161 any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.

162 5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity

163 assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any

164 services carried out by independent certification bodies.

165 6) All users should ensure that they have the latest edition of this publication.

166 7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and

167 members of its technical committees and IEC National Committees for any personal injury, property damage or

168 other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and

169 expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC

170 Publications.

171 8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is

172 indispensable for the correct application of this publication.

173 9) IEC draws attention to the possibility that the implementation of this document may involve the use of (a)

174 patent(s). IEC takes no position concerning the evidence, validity or applicability of any claimed patent rights in

175 respect thereof. As of the date of publication of this document, IEC had not received notice of (a) patent(s), which

176 may be required to implement this document. However, implementers are cautioned that this may not represent

177 the latest information, which may be obtained from the patent database available at <https://patents.iec.ch>. IEC

178 shall not be held responsible for identifying any or all such patent rights.

179

180 IEC 61508-2 has been prepared by subcommittee 65A: System aspects, of IEC technical

181 committee 65: Industrial-process measurement, control and automation. It is an International

182 Standard.

183 This third edition cancels and replaces the second edition published in 2010. This edition

184 constitutes a technical revision.

185 This edition includes the following significant technical changes with respect to the previous

186 edition (the following list does refer to this document; other parts do mention specific further

187 details):

188 a) Document was upgraded to the 2024 version of the ISO/IEC Directives; this does

189 introduce a significant number of editorial changes, clause renumbering and rewording

190 of the information provided in Notes;

- 191 b) The interfaces to other parts of IEC 61508 have been clarified and duplication of
192 requirements in other Parts has been removed;
- 193 c) The differentiation between the required Safety Integrity Level (SIL) and the achieved
194 Systematic Capability (SC) has been clarified;
- 195 d) Semiconductor content moved to the new IEC 61508-2-1. This includes the old annex
196 E, annex F and the semiconductor V-model.
- 197 e) Requirements on diagnostic functions (7.4.12) have been added;
- 198 f) Requirements on common cause failures (Annex E) have been added;
- 199 g) Reference to software off-line support tools has been added (7.4.6.4);
- 200 h) Requirements on traceability have been clarified (Annex B);
- 201 i) Various minor editorial errors have been corrected, the normative references and the
202 bibliography has been updated.

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

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

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

205 Full information on the voting for its approval can be found in the report on voting indicated in
206 the above table.
207

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

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

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

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

- 219 • reconfirmed,
- 220 • withdrawn,
- 221 • replaced by a revised edition, or
- 222 • amended.

223

224

225

INTRODUCTION

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

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

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

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

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

254 This document

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

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

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

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

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

280 – sets requirements for the avoidance and control of systematic faults, which are based on
281 experience and judgement from practical experience gained in industry. Even though the
282 probability of occurrence of systematic failures cannot in general be quantified this
283 document does, however, allow a claim to be made, for a specified safety function, that the
284 target failure rate associated with the safety function can be considered to be achieved if
285 all the requirements in this document have been met;

286 –

287 – adopts a broad range of principles, techniques and measures to achieve functional safety
288 for E/E/PE safety-related systems, but does not explicitly use the concept of fail safe.
289 However, the concepts of “fail safe” and “inherently safe” principles may be applicable and
290 adoption of such concepts is acceptable providing the requirements of the relevant clauses
291 in this document are met.

292

293

iTeh Standards (<https://standards.iteh.ai>) Document Preview

[oSIST prEN IEC 61508-2:2025](https://standards.iteh.ai/catalog/standards/sist/f4183771-6957-4d41-a166-529cb15e44d6/osist-pren-iec-61508-2-2025)

<https://standards.iteh.ai/catalog/standards/sist/f4183771-6957-4d41-a166-529cb15e44d6/osist-pren-iec-61508-2-2025>

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;

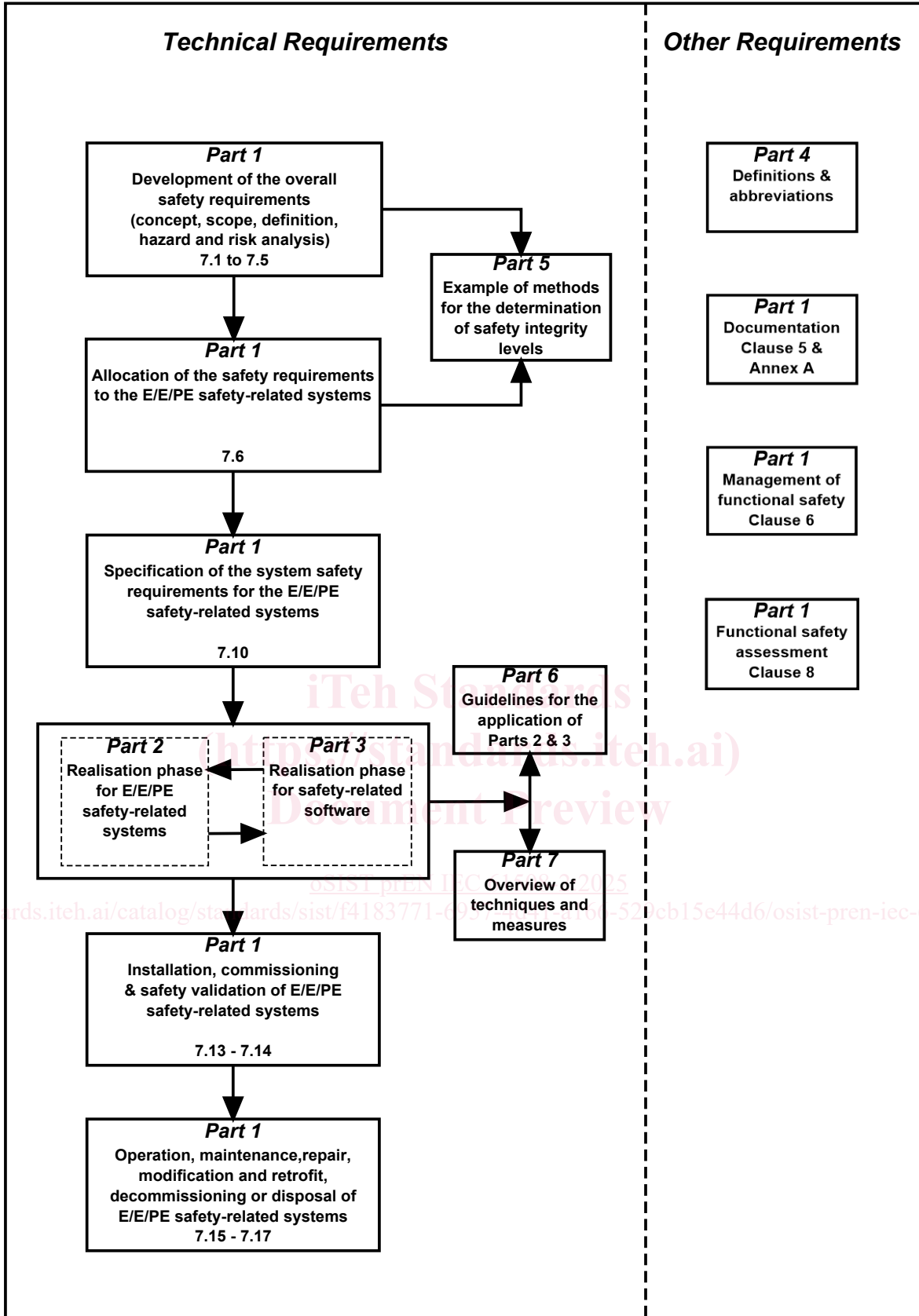
NOTE 1 This part of IEC 61508 is mainly directed at suppliers and/or in-company engineering departments, hence the inclusion of requirements for modification.

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.



343

344

Figure 1 – Overall framework of the IEC 61508 series

345

2 Normative references

346

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.

347

348 For undated references, the latest edition of the referenced document (including any
349 amendments) applies.

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

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

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

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

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

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

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

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

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

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

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

<https://standards.iteh.ai/catalog/standards/sist/f4183771-6957-4d41-a166-529cb15e44d6/osist-pren-iec-61508-2-2025>

371 **3 Definitions and abbreviations**

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

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

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

378 **4 Conformance to this document**

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

381 **5 Documentation**

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

383 **6 Additional requirements for management of functional safety for E/E/PE**
384 **system**

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

387 **6.1 Objectives**

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

389 **6.2 Requirements**

390 **6.2.1** The requirements are as detailed in 6.2 of IEC 61508-1 and apply with the following
391 additional requirements.

392 **6.2.2** The functional safety planning shall define the strategy for E/E/PE system procurement,
393 development, integration, verification, validation and modification to the extent required by the
394 systematic capability and safety integrity level of the safety functions implemented by the
395 E/E/PE safety-related system.

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

399 **6.2.3** The configuration management requirements are as detailed in IEC 61508-1 6.2 with the
400 following additional requirements:

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

418

419 **7 E/E/PE system safety lifecycle requirements**

420 **7.1 General**

421 **7.1.1 Objectives and requirements – general**

422 **7.1.1.1** This subclause sets out the objectives and requirements for the E/E/PE system safety
423 lifecycle phases.

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

426 **7.1.1.2** For all phases of the E/E/PE system safety lifecycle, Table 1 indicates

427 – the objectives to be achieved;