



SLOVENSKI STANDARD
oSIST prEN IEC 61508-3:2025
01-april-2025

Funkcijska varnost električnih/elektronskih/elektronsko programirljivih varnostnih sistemov - 3. del: Programske zahteve

Functional safety of electrical/electronic/programmable electronic safety-related systems
- Part 3: Software requirements

Funktionale Sicherheit sicherheitsbezogener
elektrischer/elektronischer/programmierbarer elektronischer Systeme - Teil 3:
Anforderungen an Software

Sécurité fonctionnelle des systèmes électriques / électroniques / électroniques
programmables relatifs à la sécurité - Partie 3: Exigences concernant les logiciels

Ta slovenski standard je istoveten z: prEN IEC 61508-3:2025

<https://standards.iteh.ai/catalog/standards/sist/c723ba8f-6b4c-4384-9e1b-de16b5fd7c03/osist-pren-iec-61508-3-2025>

ICS:

25.040.40	Merjenje in krmiljenje industrijskih postopkov	Industrial process measurement and control
-----------	---	---

oSIST prEN IEC 61508-3:2025

en,fr,de



65A/1169/CDV

COMMITTEE DRAFT FOR VOTE (CDV)

PROJECT NUMBER: IEC 61508-3 ED3	
DATE OF CIRCULATION: 2025-02-21	CLOSING DATE FOR VOTING: 2025-05-16
SUPERSEDES DOCUMENTS: 65A/1058A/CD, 65A/1077A/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

<https://standards.iteh.ai/catalog/standards/sist/c723ba8f-6b4c-4384-9e1b-del6b5fd7c03/osist-pren-iec-61508-3-2025>

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 3: Software requirements

PROPOSED STABILITY DATE: 2028

NOTE FROM TC/SC OFFICERS:

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

1

CONTENTS

2	FOREWORD	7
3	INTRODUCTION	10
4	1 Scope	12
5	2 Normative references	16
6	3 Terms, definitions, symbols and abbreviations	16
7	4 Conformance to this document	16
8	5 Documentation	16
9	6 Requirements for management of safety-related software	16
10	6.1 Objectives	16
11	6.2 Requirements	16
12	7 Software safety lifecycle requirements	17
13	7.1 General	17
14	7.1.1 Objective	17
15	7.1.2 Requirements	17
16	7.2 Software safety requirements specification	24
17	7.2.1 Objectives	24
18	7.2.2 Requirements	24
19	7.3 Validation plan for software aspects of system safety	28
20	7.3.1 Objective	28
21	7.3.2 Requirements	28
22	7.4 Software design and development	29
23	7.4.1 Objectives	29
24	7.4.2 General requirements	29
25	7.4.3 Requirements for software architecture design	35
26	7.4.4 Requirements for support tools, including programming languages	37
27	7.4.5 Requirements for detailed design and development – software system	
28	design	38
29	7.4.6 Requirements for code implementation	39
30	7.4.7 Requirements for software module testing	39
31	7.4.8 Requirements for software integration testing	40
32	7.5 Programmable electronics integration (hardware and software)	41
33	7.5.1 Objectives	41
34	7.5.2 Requirements	41
35	7.6 Software operation and modification procedures	42
36	7.6.1 Objective	42
37	7.6.2 Requirements	42
38	7.7 Software aspects of system safety validation	43
39	7.7.1 Objective	43
40	7.7.2 Requirements	43
41	7.8 Software modification	44
42	7.8.1 Objective	44
43	7.8.2 Requirements	44
44	7.9 Software verification	46
45	7.9.1 Objective	46
46	7.9.2 Requirements	46

47	8	Functional safety assessment.....	50
48	9	Bibliography	51
49		Annex A (normative) Guide to the selection of techniques and measures.....	52
50		Annex B (informative) Detailed tables	61
51		Annex C (informative) Properties for systematic capability of software elements.....	65
52	C.1	Introduction.....	65
53	C.1.1	Structure of Annex C, relating to Annexes A and B	65
54	C.1.2	Method of use – 1	67
55	C.1.3	Method of use – 2.....	68
56	C.2	Properties for systematic capability.....	70
57	C.3	Properties for systematic capability – Detailed tables.....	96
58		Annex D (normative) Safety manual for compliant items – additional requirements for	
59		software elements	110
60	D.1	Purpose of the safety manual.....	110
61	D.2	Contents of the safety manual for a software element	110
62	D.3	Justification of claims in the safety manual for compliant items	112
63		Annex E (informative) Relationships between IEC 61508-2 and this document.....	113
64		Annex F (informative) Techniques for achieving non-interference between software	
65		elements on a single computer	116
66	F.1	Introduction.....	116
67	F.2	Domains of behaviour	116
68	F.3	Causal factor analysis.....	117
69	F.4	Achieving spatial independence	117
70	F.5	Achieving temporal independence.....	118
71	F.6	Requirements for supporting software	119
72	F.7	Independence of software modules – programming language aspects	119
73		Annex G (informative) Guidance for systems configured by application data	125
74	G.1	Introduction.....	125
75	G.2	Aspects influencing lifecycle requirements	125
76	G.2.1	Complexity of E/E/PE systems.....	125
77	G.2.2	Rationale for the lifecycle requirements	126
78	G.2.3	Complexity in software.....	127
79	G.2.4	Programming language characteristics and safety	128
80	G.2.5	Role of the tools	129
81	G.3	Guidance for tailoring the lifecycle	130
82	G.3.1	Recommendations for tailoring the lifecycle	130
83	G.3.2	Tailoring principles	130
84	G.3.3	Fixed functionalities and configuration	130
85	G.3.4	Fixed functionalities and programming.....	131
86	G.3.5	Limited functionalities and configuration	132
87	G.3.6	Limited functionalities and programming	132
88	G.3.7	Open functionalities and configuration	133
89	G.3.8	Open functionalities and programming.....	133
90		Annex H (normative) Confidence in the usage of Software Off-line Support Tools.....	134
91	H.1	Scope and conventions	134
92	H.2	Software off-line support tool usage confidence approach overview	134
93	H.2.1	Software off-line support tool usage confidence objectives	134
94	H.2.2	Software off-line support tool confidence approach.....	135

95	H.2.3	Software off-line support tool usage confidence measures overview	136
96	H.3	Measures concerning software off-line support tool usage	137
97	H.3.1	Software off-line support tool usage planning and qualification planning	137
98	H.3.2	Software off-line support tool classification in the usage context.....	138
99	H.3.3	Software off-line support tool user documentation.....	140
100	H.3.4	Software off-line support tool integration and assessment in the usage	
101		environment.....	141
102	H.3.5	Software off-line support tool configuration management in the tool user	
103		context	141
104	H.3.6	Software off-line support tool operation	142
105	H.4	Measures concerning software off-line support tool development including	
106		verification	142
107	H.4.1	Software off-line support tool development with avoidance of systematic	
108		faults	142
109	H.4.2	Confidence from software off-line support tool usage history	143
110	H.4.3	Software off-line support tool documentation and problem management	144
111	H.5	Required evidence for software off-line support tool usage confidence	145
112	Annex I (informative) Model Based Software Development and Verification Guidelines.....		147
113	I.1	Objectives and scope of this annex.....	147
114	I.2	Rationale for this annex	147
115	I.3	Approach and relationship with the body of this document	148
116	I.4	Documentation.....	148
117	I.5	Safety lifecycle planning	148
118	I.6	Techniques and measures	150
119	I.7	Software safety requirements specification	151
120	I.8	Software architecture design.....	151
121	I.9	Requirements for software off-line support tools, including programming	
122		languages.....	152
123	I.10	Detailed design and development	152
124	I.11	Code Implementation	153
125	I.12	Software module testing.....	153
126	I.13	Software integration testing	154
127	I.14	Model Verification	155
128	I.15	Model-Based verification.....	155
129	Annex J (Informative) Data Driven Systems		157
130	J.1	General.....	157
131	J.2	Systems with Minimal Configurable Parameters	158
132	J.3	Systems with Comprehensive Configurability	158
133	J.4	Role of the tools.....	159
134			
135	Figure 1 – Overall framework of the IEC 61508 series		14
136	Figure 2 – Overall E/E/PE system safety lifecycle		15
137	Figure 3 – E/E/PE system safety lifecycle (in realisation phase).....		19
138	Figure 4 – Software safety lifecycle (in realisation phase).....		19
139	Figure 5 – Relationship and scope for IEC 61508-2 and this document (see also		
140	Annex E).....		20
141	Figure 6 – Systematic capability for software and the development lifecycle (the V-		
142	model)		20
143	Figure H.1 – Tool Confidence Principle		135

144	Figure H.2 – Data flow overview of software off-line support tool usage confidence	
145	measures for an on-demand software off-line support tool	136
146	Figure H.3 – Data flow overview of software off-line support tool usage confidence	
147	measures for a COTS software off-line support tool	137
148		
149		
150	Table 1 – Software safety lifecycle – overview (1 of 4)	21
151	Table A.1 – Software safety requirements specification	53
152	Table A.2 – Software design and development – software architecture design	53
153	Table A.3 – Software design and development – programming language	55
154	Table A.4 – Software design and development – detailed design	55
155	Table A.5 – Software design and development – software module testing and	
156	integration	56
157	Table A.6 – Programmable electronics integration (hardware and software).....	57
158	Table A.7 – Software aspects of system safety validation	57
159	Table A.8 – Modification	57
160	Table A.9 – Software verification	59
161	Table A.10 – Not Used : Replaced by additional requirements in Table A.2	59
162	Table A.11 – Software life cycle through lifecycle activities	60
163	Table B.1 – Design and coding standards	61
164	Table B.2 – Dynamic analysis and testing	61
165	Table B.3 – Functional and black-box testing	62
166	Table B.4 – Not Used : Replaced by additional requirements in Table A.2	62
167	Table B.5 – Modelling	63
168	Table B.6 – Performance testing	63
169	Table B.7 – Not Used	63
170	Table B.8 – Static analysis	64
171	Table B.9 – Modular approach	64
172	Table C.1.1 – Extract of Table A.1 for illustration	65
173	Table C.1.2 – Extract of Table C.1 for illustration	66
174	Table C.1.3 – Extract of Table C.1 for illustration	66
175	Table C.1.4 – Rigour of techniques	67
176	Table C.1.5 – Use of rigour ranking	67
177	Table C.1.2.1 Method of Use 1 : link between rigour and CS.....	68
178	Table C.1 – Properties for systematic capability – Software safety requirements	
179	specification.....	70
180	Table C.2 – Properties for systematic capability – Software design and development –	
181	software Architecture Design	73
182	Table C.3 – Properties for systematic capability – Software design and development –	
183	programming language	84
184	Table C.4 – Properties for systematic capability – Software design and development –	
185	detailed design (includes software system design, software module design and	
186	coding)	85
187	Table C.5 – Properties for systematic capability – Software design and development –	
188	software module testing and integration	89

189	Table C.6 – Properties for systematic capability – Programmable electronics	
190	integration (hardware and software).....	91
191	Table C.7 – Properties for systematic capability – Software aspects of system safety	
192	validation.....	92
193	Table C.8 – Properties for systematic capability – Software modification	93
194	Table C.9 – Properties for systematic capability – Software verification	95
195	Table C.11 – Detailed properties – Design and coding standards.....	96
196	Table C.12 – Detailed properties – Dynamic analysis and testing.....	98
197	Table C.13 – Detailed properties – Functional and black-box testing.....	100
198	Table C.14 – Deleted – Replaced by additional information in Table C.2.....	101
199	Table C.15 – Detailed properties – Modelling.....	101
200	Table C.16 – Detailed properties – Performance testing.....	102
201	Table C.17 – Not Used.....	103
202	Table C.18 – Properties for systematic capability – Static analysis	103
203	Table C.19 – Detailed properties – Modular approach.....	104
204	Table C.20 – Properties for systematic capability - through lifecycle aspects	106
205	Technique/Measure	106
206	Table E.1 – Categories of IEC 61508-2 requirements.....	113
207	Table E.2 – Requirements of IEC 61508-2 for software and their typical relevance to	
208	certain types of software.....	113
209	Table F.1 – Types of module coupling	121
210	Table G.1 – Variability in complexity of E/E/PE systems	126
211	Table H.1 – TD Levels	139
212	Table H.2 –TIC/FSI/TD/TUS Balancing Rules	140
213	Table H.3 – Required Tool Usage Confidence Evidence per TUS.....	145
214	Table I.1 – Comparison of Separation vs Merging Development Layers	149
215		
216		

217 INTERNATIONAL ELECTROTECHNICAL COMMISSION

218

219

220

221

222

223

224

225

**FUNCTIONAL SAFETY OF ELECTRICAL/ELECTRONIC/
PROGRAMMABLE ELECTRONIC SAFETY-RELATED SYSTEMS –****Part 3: Software requirements****FOREWORD**

226

227

228

229

230

231

232

233

234

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.

235

236

237

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.

238

239

240

241

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.

242

243

244

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.

245

246

247

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.

248

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

249

250

251

252

253

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.

254

255

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.

256

257

258

259

260

261

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> [and/or] www.iso.org/patents. IEC shall not be held responsible for identifying any or all such patent rights.

262

263

264

IEC 61508-3 has been prepared by subcommittee SC65A: SYSTEM ASPECTS, of IEC technical committee TC65: INDUSTRIAL PROCESS MEASUREMENT, CONTROL AND AUTOMATION. It is an International Standard.

265

266

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

267

268

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

269

270

271

This document has been upgraded to the 2024 version of the ISO/IEC Directives; this does introduce a significant number of editorial changes and Clause renumbering throughout. In addition, the following technical changes have been made:

- 272 a) All requirements on use of artificial Intelligence, security and human factors are limited
273 to the references in Scope to external guidance
- 274 b) The requirements of IEC TS 61508-3-1 have been incorporated into Clause 7 and
275 extended to address requirements to achieve Systematic Capability SC3 and SC4
- 276 c) The interfaces to other Parts of IEC 61508 have been clarified and duplication of
277 requirements in other Parts has been removed
- 278 d) The requirement to undertake software functional failure analysis has been transferred
279 from the requirements for functional safety assessment to the requirements on
280 architectural design and renamed software failure analysis; the differentiation between
281 functional safety audit, functional safety assessment and software failure analysis has
282 been clarified in IEC 61508-7
- 283 e) The differentiation between the required Safety Integrity Level (SIL) and the achieved
284 Systematic Capability (SC) has been clarified
- 285 f) The requirements for formal methods has been clarified throughout all software lifecycle
286 phases, the requirements of TS 61508-3-2 have been referenced in this document and
287 IEC 61508-7 and the concept of semi-formal methods has been re-instated to the status
288 in Edition 2 of this document; the meaning of 'unambiguously defined' methods has been
289 clarified
- 290 g) Rules for synthesis of software elements has been clarified; detailed requirements on
291 software used in diagnostics is now addressed in IEC 61508-2
- 292 h) The requirements on software off-line support tools have been refined
- 293 i) The guidance on data driven systems has been provided in a separate Annex from the
294 guidance on data configuration and limited variability programming; the guidance on
295 limited variability programming has been updated to be consistent with IEC 61131-1.
- 296 j) The requirements in Annex A on modification have been re-instated to the status in
297 Edition 2 and clarified
- 298 k) An additional table has been added to define requirements on management activities
299 which occur throughout the entire software lifecycle; this table includes requirements on
300 traceability, which have been removed from individual phase requirements
- 301 l) Requirements on regression testing have been clarified
- 302 m) The use of the terminology 'verification' and 'validation' has been brought in line with the
303 definitions in IEC 61508-4; much supplementary information added at Ed 3 CD has been
304 transferred to IEC 61508-7 as informative guidance, or else deleted
- 305 n) The requirements on the use of object oriented design and development have been
306 brought in line with practical applications; further detail is being developed in TR 61508-
307 3-3
- 308 o) Various minor editorial errors have been corrected.

309 NOTE In order to avoid the need for extensive editing to existing compliance tools, the methods and techniques
310 specified in Annex A and Annex B of this document have retained their original reference ID. Where methods and
311 techniques have been deleted the phrase 'Not Used' has been entered. Where methods and techniques have been
312 added an additional row with additional reference ID have been added. As far as possible this also applies to Clauses
313 in the body of the document, but some renumbering has been inevitable where information has been added.

314 This edition has been subject to a thorough review and incorporates many comments received
315 at the various revision stages.

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

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

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

318
319 Full information on the voting for its approval can be found in the report on voting indicated in
320 the above table.

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

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

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

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

- 332
- replaced by a revised edition, or
 - amended.
- 333

334

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

[oSIST prEN IEC 61508-3:2025](https://standards.iteh.ai/catalog/standards/sist/c723ba8f-6b4c-4384-9e1b-de16b5fd7c03/osist-pren-iec-61508-3-2025)

<https://standards.iteh.ai/catalog/standards/sist/c723ba8f-6b4c-4384-9e1b-de16b5fd7c03/osist-pren-iec-61508-3-2025>

335

INTRODUCTION

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

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

349 NOTE 1 Examples of product and application sector international standards based on the IEC 61508 series are
350 given in the bibliography.

351 In most situations, safety is achieved by a number of systems which rely on many technologies (for
352 example mechanical, hydraulic, pneumatic, electrical, electronic, programmable electronic). Any
353 safety strategy considers not only all the elements within an individual system (for example sensors,
354 controlling devices and actuators) and humans as part of the system, as part of the realization
355 process, operation, and management of verification/decision making), but also all the safety-related
356 systems making up the total combination of safety-related systems. Therefore, while this document is
357 concerned with E/E/PE safety-related systems, it can also provide a framework within which safety-
358 related systems based on other technologies can be considered.

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

365 This document

366— considers all relevant overall, E/E/PE system and software safety lifecycle phases (for example,
367 from initial concept, through design, implementation, operation and maintenance to
368 decommissioning) when E/E/PE systems are used to perform safety functions;

369— has been conceived with a rapidly developing technology in mind; the framework is sufficiently
370 robust and comprehensive to cater for future developments;

371— enables product and application sector international standards, dealing with E/E/PE safety-
372 related systems, to be developed; the development of product and application sector
373 international standards, within the framework of this document, should lead to a high level of
374 consistency (for example, of underlying principles, terminology etc.) both within application
375 sectors and across application sectors; this will have both safety and economic benefits;

376— provides a method for the development of the safety requirements specification necessary to
377 achieve the required functional safety for E/E/PE safety-related systems;

378— adopts a risk-based approach by which the safety integrity requirements can be determined;

379— introduces safety integrity levels for specifying the target level of safety integrity for the safety
380 functions to be implemented by the E/E/PE safety-related systems;

381 NOTE 1 The standard does not specify the safety integrity level requirements for any safety function, nor does it
382 mandate how the safety integrity level is determined. Instead, it provides a risk-based conceptual framework and
383 example techniques.

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

386— sets a lower limit on the target failure measures for a safety function carried out by a single
387 E/E/PE safety-related system. For E/E/PE safety-related systems operating in

388 • a low demand mode of operation, the lower limit is set at an average probability of a
389 dangerous failure on demand of 10^{-5} ;

390 • a high demand or a continuous mode of operation, the lower limit is set at an average
391 frequency of a dangerous failure of 10^{-9} [h^{-1}];

392 NOTE 2 A single E/E/PE safety-related system does not necessarily mean a single-channel architecture.

393 NOTE 3 It can be possible to achieve designs of safety-related systems with lower values for the target safety
394 integrity for non-complex systems, but these limits are considered to represent what can be achieved for relatively
395 complex systems (for example programmable electronic safety-related systems) at the present time.

396— sets requirements for the avoidance and control of systematic faults, which are based on
397 experience and judgement from practical experience gained in industry. Even though the
398 probability of occurrence of systematic failures cannot in general be quantified the standard
399 does, however, allow a claim to be made, for a specified safety function, that the target failure
400 measure associated with the safety function can be considered to be achieved if all the
401 requirements in the standard have been met;

402— introduces systematic capability as a measure of confidence that an E/E/PE system meets the
403 safety requirements with regards to avoidance and control of systematic faults;

404— adopts a broad range of principles, techniques and measures to achieve functional safety for
405 E/E/PE safety-related systems but does not explicitly use the concept of fail safe. However, the
406 concepts of “fail safe” can be applicable and adoption of such concepts is acceptable providing
407 the requirements of the relevant clauses in the standard are met.

408

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

[oSIST prEN IEC 61508-3:2025](https://standards.iteh.ai/catalog/standards/sist/c723ba8f-6b4c-4384-9e1b-de16b5fd7c03/osist-pren-iec-61508-3-2025)

<https://standards.iteh.ai/catalog/standards/sist/c723ba8f-6b4c-4384-9e1b-de16b5fd7c03/osist-pren-iec-61508-3-2025>

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

Part 3: Software requirements

409
410
411
412
413
414
415

416 1 Scope

417 1.1 This part of the IEC 61508 series:

- 418 a) is intended to be utilized only after a thorough understanding of, and in conjunction with,
419 the requirements of IEC 61508-1 and IEC 61508-2;
- 420 b) applies to any software forming part of a safety-related system or used to develop a safety-
421 related system within the scope of IEC 61508-1 and IEC 61508-2. Such software is termed
422 safety-related software (including operating systems, system software, software in
423 communication networks, human-computer interface functions, and firmware as well as
424 application software);
- 425 c) provides specific requirements applicable to support tools used to develop and configure a
426 safety-related system within the scope of IEC 61508-1 and IEC 61508-2;
- 427 d) requires that the software safety functions and their systematic capability are specified;

428 NOTE 1 If this has already been done as part of the specification of the E/E/PE safety-related systems (see 7.2 of
429 IEC 61508-2), then it does not have to be repeated in this part.

430 NOTE 2 Specifying the software safety functions and their systematic capability is an iterative procedure;
431 see Figure 5 and Figure 6.

432 NOTE 3 See IEC 61508-1 Clause 5 and IEC 61508-1 Annex A for documentation structure. The documentation
433 structure can be organised to take account of company procedures, and of the working practices of specific
434 application sectors.

435 NOTE 4 See IEC 61508-4 3.5.8 for definition of the term "systematic capability".

- 436 e) establishes requirements for safety lifecycle phases and activities which shall be applied
437 during the design and development of the safety-related software (the software safety
438 lifecycle model). These requirements include the application of measures and techniques,
439 which are graded against the required systematic capability, for the avoidance of and control
440 of faults and failures in the software;
- 441 f) provides requirements for information relating to the software aspects of system safety
442 validation to be passed to the organisation carrying out the E/E/PE system integration;
- 443 g) provides requirements for the preparation of information and procedures concerning
444 software needed by the user for the operation and maintenance of the E/E/PE safety-related
445 system;
- 446 h) provides requirements to be met by the organisation carrying out modifications to safety-
447 related software;
- 448 i) provides, in conjunction with IEC 61508-1 and IEC 61508-2, requirements for support tools
449 such as development and design tools, language translators, testing and debugging tools,
450 configuration management tools;

451 NOTE 5 Figure 5 shows the relationship between IEC 61508-2 and this document.

452 j) Not used;

453 k) Does apply to software algorithms

454 i. software technology class I (see definition in IEC 61508-4 Clause 3.2.14);

455 ii. software technology class II and III (see definitions in IEC 61508-4, Clause 3.2.15 and
456 Clause 3.2.16)