



SLOVENSKI STANDARD
oSIST prEN IEC 61508-7:2025
01-april-2025

Funkcijska varnost električnih/elektronskih/elektronsko programirljivih varnostnih sistemov - 7. del: Pregled tehnik in ukrepov

Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 7: Overview of techniques and measures

Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme - Teil 7: Überblick über Verfahren und Maßnahmen

Sécurité fonctionnelle des systèmes électriques / électroniques / électroniques programmables relatifs à la sécurité - Partie 7: Présentation de techniques et mesures

Ta slovenski standard je istoveten z: prEN IEC 61508-7:2025

<https://standards.iteh.ai/catalog/standards/sist/aed087fd-8651-4186-bbd7-71f7386bf4dc/osist-pren-iec-61508-7-2025>

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 61508-7:2025

en,fr,de



65A/1168/CDV

COMMITTEE DRAFT FOR VOTE (CDV)

PROJECT NUMBER: IEC 61508-7 ED3	
DATE OF CIRCULATION: 2025-02-14	CLOSING DATE FOR VOTING: 2025-05-09
SUPERSEDES DOCUMENTS: 65A/1062A/CD, 65A/1081A/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 7: Overview of techniques and measures

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
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
48

FOREWORD.....	8
INTRODUCTION.....	10
1 Scope.....	12
2 Normative references	14
3 Definitions and abbreviations.....	14
Annex A (informative) Overview of techniques and measures for E/E/PE safety-related systems: control of random hardware failures (see IEC 61508-2).....	15
A.1 Electric	15
A.1.1 Failure detection by on-line monitoring	15
A.1.2 Monitoring of relay contacts	15
A.1.3 Comparator	15
A.1.4 Majority voter.....	16
A.1.5 Idle current principle (de-energised to trip)	16
A.2 Electronic.....	16
A.2.1 Tests by redundant hardware	16
A.2.2 Dynamic principles	16
A.2.3 Standard test access port and boundary-scan architecture	17
A.2.4 (Not used)	17
A.2.5 Monitored redundancy	17
A.2.6 Electrical/electronic components with automatic check	17
A.2.7 Analogue signal monitoring.....	18
A.2.8 De-rating	18
A.3 Processing units	18
A.3.1 Self-test by software: limited number of patterns (one-channel).....	18
A.3.2 Self-test by software: walking bit (one-channel)	18
A.3.3 Self-test supported by hardware (one-channel).....	19
A.3.4 Coded processing (one-channel)	19
A.3.5 Reciprocal comparison by software	19
A.4 Invariable memory ranges.....	19
A.4.1 Word-saving multi-bit redundancy (for example ROM monitoring with a modified Hamming code)	19
A.4.2 Modified checksum	20
A.4.3 Signature of one word (8-bit)	20
A.4.4 Signature of a double word (16-bit).....	20
A.4.5 Block replication (for example double ROM with hardware or software comparison).....	20
A.5 Variable memory ranges	21
A.5.1 RAM test "checkerboard"	21
A.5.2 RAM test "walkpath"	21
A.5.3 RAM test "galpat" or "transparent galpat".....	21
A.5.4 RAM test "Abraham"	22
A.5.5 One-bit redundancy (for example RAM monitoring with a parity bit)	22
A.5.6 RAM monitoring with a modified Hamming code, or detection of data failures with error-detection-correction codes (EDC).....	22
A.5.7 Double RAM with hardware or software comparison and read/write test.....	22
A.5.8 RAM test "march"	23

49	A.6	I/O-units and interfaces (external communication).....	23
50	A.6.1	Test pattern	23
51	A.6.2	Code protection	23
52	A.6.3	Multi-channel parallel output.....	24
53	A.6.4	Monitored outputs.....	24
54	A.6.5	Input comparison/voting.....	24
55	A.7	Data paths (internal communication).....	24
56	A.7.1	One-bit hardware redundancy.....	24
57	A.7.2	Multi-bit hardware redundancy.....	24
58	A.7.3	Complete hardware redundancy	25
59	A.7.4	Inspection using test patterns	25
60	A.7.5	Transmission redundancy.....	25
61	A.7.6	Information redundancy	25
62	A.8	Power supply	25
63	A.8.1	Overvoltage protection with safety shut-off	25
64	A.8.2	Voltage control (secondary).....	26
65	A.8.3	Power-down with safety shut-off	26
66	A.9	Temporal and logical program sequence monitoring	26
67	A.9.1	Watch-dog with separate time base without time-window.....	26
68	A.9.2	Watch-dog with separate time base and time-window	26
69	A.9.3	Logical monitoring of program sequences.....	26
70	A.9.4	Combination of temporal and logical monitoring of program sequences	27
71	A.9.5	Temporal monitoring with on-line check	27
72	A.10	Ventilation and heating	27
73	A.10.1	Temperature sensor	27
74	A.10.2	Fan control	27
75	A.10.3	Actuation of the safety shut-off via thermal fuse.....	27
76	A.10.4	Staggered message from thermo-sensors and conditional alarm.....	27
77	A.10.5	Connection of forced-air cooling and status indication	28
78	A.11	Communication and mass-storage	28
79	A.11.1	Separation of electrical energy lines from information lines.....	28
80	A.11.2	Spatial separation of multiple lines	28
81	A.11.3	Design for immunity to electromagnetic interference.....	28
82	A.11.4	Antivalent signal transmission.....	29
83	A.12	Sensors	29
84	A.12.1	Reference sensor	29
85	A.12.2	Positive-activated switch	29
86	A.13	Final elements (actuators)	30
87	A.13.1	Monitoring	30
88	A.13.2	Cross-monitoring of multiple actuators.....	30
89	A.14	Measures against the physical environment.....	30
90	Annex B (informative) Overview of techniques and measures for E/E/PE safety related		
91	systems: avoidance of systematic failures (see IEC 61508-2 and IEC 61508-3).....		31
92	B.1	General measures and techniques	31
93	B.1.1	Project management.....	31
94	B.1.2	Documentation	32
95	B.1.3	Separation of E/E/PE system safety functions from non-safety functions	33
96	B.1.4	Diverse hardware	33
97	B.1.5	Traceability.....	33

98	B.1.6	Functional Safety Assurance Role Independence	34
99	B.2	E/E/PE system design requirements specification	36
100	B.2.1	Structured specification	36
101	B.2.2	Formal methods.....	37
102	B.2.3	Semi-formal methods.....	38
103	B.2.4	Computer-aided specification tools	40
104	B.2.5	Checklists.....	41
105	B.2.6	Inspection of the specification.....	42
106	B.3	E/E/PE system design and development	43
107	B.3.1	Observance of guidelines and standards	43
108	B.3.2	Structured design	43
109	B.3.3	Use of well-tried components.....	43
110	B.3.4	Modularisation	44
111	B.3.5	Computer-aided design tools	44
112	B.3.6	Simulation	45
113	B.3.7	Inspection (reviews and analysis)	45
114	B.3.8	Walk-through	45
115	B.4	E/E/PE system operation and maintenance procedures	46
116	B.4.1	Operation and maintenance instructions	46
117	B.4.2	User friendliness.....	46
118	B.4.3	Maintenance friendliness	47
119	B.4.4	Limited operation possibilities.....	47
120	B.4.5	Operation only by skilled operators.....	47
121	B.4.6	Protection against operator mistakes	48
122	B.4.7	(Not used)	48
123	B.4.8	Modification protection.....	48
124	B.4.9	Input acknowledgement	48
125	B.5	E/E/PE system integration	48
126	B.5.1	Functional testing	49
127	B.5.2	Black-box testing	49
128	B.5.3	Statistical testing	50
129	B.5.4	Field experience	50
130	B.6	E/E/PE system safety validation.....	51
131	B.6.1	Functional testing under environmental conditions.....	51
132	B.6.2	Electromagnetic interference immunity testing	52
133	B.6.3	Static analysis	52
134	B.6.4	Dynamic analysis and testing	53
135	B.6.5	Failure analysis	53
136	B.6.6	Worst-case analysis	59
137	B.6.7	Expanded functional testing.....	60
138	B.6.8	Worst-case testing.....	60
139	B.6.9	Fault insertion testing	60
140	Annex C (informative)	Overview of techniques and measures for achieving systematic capability for software (see IEC 61508-3)	62
141			
142	C.1	General.....	62
143	C.2	Requirements and detailed design	62
144	C.2.1	Structured methods	62
145	C.2.2	Data flow diagrams	64
146	C.2.3	Structure diagrams	65

147	C.2.4	Not used	66
148	C.2.5	Defensive programming	66
149	C.2.6	Design and coding standards	67
150	C.2.7	Structured programming	71
151	C.2.8	Information hiding/encapsulation	72
152	C.2.9	Modular approach	72
153	C.2.10	Use of trusted/verified software elements	73
154	C.2.11	Not Used	75
155	C.2.12	Aim: To maintain consistency between lifecycle stages.	75
156	C.2.13	Stateless software design (or limited state design)	76
157	C.2.14	Offline numerical analysis	77
158	C.2.15	Message sequence charts	77
159	C.3	Architecture design	77
160	C.3.1	Fault detection and diagnosis	77
161	C.3.2	Error detecting and correcting codes	78
162	C.3.3	Failure assertion programming	78
163	C.3.4	Diverse monitor	79
164	C.3.5	Software diversity (diverse programming)	80
165	C.3.6	Backward recovery	80
166	C.3.7	Re-try fault recovery mechanisms	81
167	C.3.8	Graceful degradation	81
168	C.3.9	Not Used	82
169	C.3.10	Dynamic reconfiguration	82
170	C.3.11	Safety and Performance in real time: Time-Triggered Architecture	82
171	C.3.12	UML	83
172	C.4	Development tools and programming languages	85
173	C.4.1	Strongly typed programming languages	85
174	C.4.2	Language subsets	85
175	C.4.3	Not used	85
176	C.4.4	Not used	86
177	C.4.5	Suitable programming languages	86
178	C.4.6	Automatic software generation	88
179	C.4.7	Test management and automation tools	89
180	C.5	Verification and modification	89
181	C.5.1	Probabilistic testing	89
182	C.5.2	Data recording and analysis	90
183	C.5.3	Interface testing	90
184	C.5.4	Boundary value analysis	91
185	C.5.5	Error guessing	91
186	C.5.6	Error seeding	92
187	C.5.7	Equivalence classes and input partition testing	92
188	C.5.8	Structure-based testing	93
189	C.5.9	Control flow analysis	94
190	C.5.10	Data flow analysis	94
191	C.5.11	Symbolic execution	95
192	C.5.12	Formal proof (verification)	95
193	C.5.13	Complexity metrics	96
194	C.5.14	Formal inspections	97
195	C.5.15	Walk-through (software)	98

196	C.5.16	Design review.....	98
197	C.5.17	Prototyping/animation.....	99
198	C.5.18	Process simulation.....	99
199	C.5.19	Performance requirements.....	100
200	C.5.20	Performance modelling.....	100
201	C.5.21	Avalanche/stress testing.....	101
202	C.5.22	Response timing and memory constraints.....	101
203	C.5.23	Impact analysis.....	102
204	C.5.24	Software configuration management.....	102
205	C.5.25	Regression validation.....	103
206	C.5.26	Animation of specification and design.....	103
207	C.5.27	Model based testing (test case generation).....	104
208	C.6	Functional safety assessment.....	106
209	C.6.1	Decision tables (truth tables).....	106
210	C.6.2	Software failure analysis.....	106
211	C.6.3	Common cause failure analysis.....	115
212	C.6.4	Reliability block diagrams.....	115
213	C.6.5	V&V Methods and Techniques Supporting IEC61508-3 CI 7.3.2.3.....	116
214	Table C.6.5 : V&V Methods and Techniques supporting Part 3 Clause 7.3.2.3.....		117
215	Annex D (informative) Statistical evaluation techniques for in service software		
216	elements.....		119
217	D.1	Introduction.....	119
218	D.2	Theoretical aspects.....	119
219	D.2.1	General.....	119
220	D.2.2	References.....	119
221	D.2.3	Terms and Definitions.....	119
222	D.2.4	Estimates of Software Statistical Parameters.....	120
223	D.2.5	The Sum Total of Operational Data Required.....	122
224	D.2.6	Required Conditions for Operational History to be an Effective Guide to	
225		Future Use.....	123
226	D.3	Deployment aspects.....	123
227	D.3.1	Statistical evaluation deployment guidance.....	123
228	D.3.2	Some Examples of Difficulties with Software Statistical Modelling.....	125
229	D.4	Route 2s proven in use claim.....	127
230	D.5	Bibliography.....	127
231	Annex E (informative) Overview of techniques and measures for design of complex		
232	integrated circuits.....		129
233	Annex F (informative) Definitions of properties of software lifecycle phases.....		
234	Annex G (informative) Guidance for the development of safety-related object oriented		
235	software.....		136
236	Annex H (informative) NOTE The overview of techniques and measures contained in		
237	this annex has been moved to IEC 61508-2-1.....		138
238	Bibliography.....		
239	Index		
240			
241	Figure 1 – Overall framework of IEC 61508.....		13
242	Figure C.6.2.1 – Typical (qualitative) software functional fault tree.....		110
243			

244	Table B.1 – Significance of Independence Concern vs. Functional Safety Assurance	
245	Activity.....	35
246	Table B.2 – Effectiveness of Independence Measure vs. Independence Concern.....	35
247	Table B.3 – Effectiveness of Independence Measure vs. Functional Safety Assurance	
248	Activity.....	36
249	Table C.1 – Recommendations for specific programming languages	87
250	Table C.6.2.1 - Example of the Guidewords as used in SHARD	110
251	Table C.6.2.2 - Example of the Guidewords as used in SHARD	113
252	Table D.1 – Failure-free observations required to reach confidence in a failure	
253	probability per demand	121
254	Table D.2 – Failure-free hours of observation required to reach confidence in a failure	
255	probability per hour.....	122
256	Table F.1 – Software Safety Requirements Specification	130
257	Table F.2 – Software design and development: software architecture design	131
258	Table F.2 – Software design and development: support tools and programming	
259	language.....	132
260	Table F.2 – Software design and development: detailed design	132
261	Table F.2 – Software design and development: software module testing and integration.....	133
262	Table F.2 – Programmable electronics integration (hardware and software).....	133
263	Table F.2 – Software aspects of system safety validation	134
264	Table F.2 – Software modification.....	134
265	Table F.2 – Software verification.....	135
266	Table F.2 – Functional safety assessment	135
267	Table G.1 – Object Oriented Software Architecture.....	136
268	Table G.2 – Object Oriented Detailed Design.....	137
269	Table G.2 – Some Oriented Detailed terms.....	137
270		
271		

272

INTERNATIONAL ELECTROTECHNICAL COMMISSION

273

274

275

276

277

278

279

280

**FUNCTIONAL SAFETY OF ELECTRICAL/ELECTRONIC/
PROGRAMMABLE ELECTRONIC SAFETY-RELATED SYSTEMS –****Part 7: Overview of techniques and measures****FOREWORD**

281

282

283

284

285

286

287

288

289

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.

290

291

292

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.

293

294

295

296

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.

297

298

299

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.

300

301

302

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.

303

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

304

305

306

307

308

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.

309

310

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.

311

312

313

314

315

316

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.

317

318

IEC 61508-7 has been prepared by subcommittee 65A: System aspects, of IEC technical committee 65: Industrial-process measurement, control and automation.

319

320

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

321

322

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

323

324

325

- the contents of annex E have been moved to IEC 61508-2-1;
- A revision of Annex D covering proven in use to include new wording, explanations and examples.

326 The text of this International Standard is based on the following documents:

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

327

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

330 The language used for the development of this International Standard is English.

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

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

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

- 341 • reconfirmed,
- 342 • withdrawn,
- 343 • replaced by a revised edition, or
- 344 • amended.

345

[oSIST prEN IEC 61508-7:2025](http://standards.iteh.ai/catalog/standards/sist/aed087fd-8651-4186-bbd7-71f7386bf4dc/osist-pren-iec-61508-7-2025)

346 standards.iteh.ai/catalog/standards/sist/aed087fd-8651-4186-bbd7-71f7386bf4dc/osist-pren-iec-61508-7-2025

347

INTRODUCTION

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

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

361 NOTE 1 Examples of product and application sector international standards based on the IEC 61508 series are
362 given in the bibliography (see references [21], [22] and [37]).

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

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

376 This International Standard

- 377 – considers all relevant overall, E/E/PE system and software safety lifecycle phases (for
378 example, from initial concept, through design, implementation, operation and maintenance
379 to decommissioning) when E/E/PE systems are used to perform safety functions;
- 380 – has been conceived with a rapidly developing technology in mind; the framework is
381 sufficiently robust and comprehensive to cater for future developments;
- 382 – enables product and application sector international standards, dealing with E/E/PE safety-
383 related systems, to be developed; the development of product and application sector
384 international standards, within the framework of this document, should lead to a high level
385 of consistency (for example, of underlying principles, terminology etc.) both within
386 application sectors and across application sectors; this will have both safety and economic
387 benefits;
- 388 – provides a method for the development of the safety requirements specification necessary
389 to achieve the required functional safety for E/E/PE safety-related systems;
- 390 – adopts a risk-based approach by which the safety integrity requirements can be determined;
- 391 – introduces safety integrity levels for specifying the target level of safety integrity for the
392 safety functions to be implemented by the E/E/PE safety-related systems.
- 393 – The standard does not specify the safety integrity level requirements for any safety function,
394 nor does it mandate how the safety integrity level is determined. Instead it provides a risk-
395 based conceptual framework and example techniques.
- 396 – sets target failure measures for safety functions carried out by E/E/PE safety-related
397 systems, which are linked to the safety integrity levels;

- 398 – sets a lower limit on the target failure measures for a safety function carried out by a single
399 E/E/PE safety-related system. For E/E/PE safety-related systems operating in
- 400 • a low demand mode of operation, the lower limit is set at an average probability of a
401 dangerous failure on demand of 10^{-5} ;
 - 402 • a high demand or a continuous mode of operation, the lower limit is set at an average
403 frequency of a dangerous failure of 10^{-9} [h⁻¹];
- 404 NOTE 2 A single E/E/PE safety-related system does not necessarily mean a single-channel architecture.
- 405 NOTE 3 It can be possible to achieve designs of safety-related systems with lower values for the target safety
406 integrity for non-complex systems, but these limits are considered to represent what can be achieved for relatively
407 complex systems (for example programmable electronic safety-related systems) at the present time.
- 408 – sets requirements for the avoidance and control of systematic faults, which are based on
409 experience and judgement from practical experience gained in industry. Even though the
410 probability of occurrence of systematic failures cannot in general be quantified the standard
411 does, however, allow a claim to be made, for a specified safety function, that the target
412 failure measure associated with the safety function can be considered to be achieved if all
413 the requirements in the standard have been met;
 - 414 – introduces systematic capability which applies to an element with respect to the confidence
415 that its systematic safety integrity meets the requirements of the specified safety integrity
416 level;
 - 417 – adopts a broad range of principles, techniques and measures to achieve functional safety
418 for E/E/PE safety-related systems, but does not explicitly use the concept of fail safe.
419 However, the concepts of “fail safe” and “inherently safe” principles may be applicable and
420 adoption of such concepts is acceptable providing the requirements of the relevant clauses
421 in the standard are met.

422

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

[oSIST prEN IEC 61508-7:2025](https://standards.iteh.ai/catalog/standards/sist/aed087fd-8651-4186-bbd7-71f7386bf4dc/osist-pren-iec-61508-7-2025)

<https://standards.iteh.ai/catalog/standards/sist/aed087fd-8651-4186-bbd7-71f7386bf4dc/osist-pren-iec-61508-7-2025>

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

425 **Part 7: Overview of techniques and measures**
426
427
428
429

430 **1 Scope**

431 **1.1** This part of IEC 61508 contains an overview of various safety techniques and measures
432 relevant to IEC 61508-2 and IEC 61508-3.

433 The references should be considered as basic references to methods and tools or as examples,
434 and may not represent the state of the art.

435 **1.2** IEC 61508-1, IEC 61598-2, IEC 61508-3 and IEC 61508-4 are basic safety publications,
436 although this status does not apply in the context of low complexity E/E/PE safety-related
437 systems (see 3.4.3 of IEC 61508-4). This document provides further information to complement
438 these basic safety publications.

439 **1.3** One of the responsibilities of a technical committee is, wherever applicable, to make
440 use of basic safety publications in the preparation of its publications. In this context, the
441 requirements, test methods or test conditions of this basic safety publication will not apply
442 unless specifically referred to or included in the publications prepared by those technical
443 committees.

444 **1.4** Figure 1 shows the overall framework for parts 1 to 7 of IEC 61508 and indicates the role
445 that IEC 61508-7 plays in the achievement of functional safety for E/E/PE safety-related
446 systems.

[oSIST prEN IEC 61508-7:2025](https://standards.iteh.ai/catalog/standards/sist/aed087fd-8651-4186-bbd7-71f7386bf4dc/osist-pren-iec-61508-7-2025)

<https://standards.iteh.ai/catalog/standards/sist/aed087fd-8651-4186-bbd7-71f7386bf4dc/osist-pren-iec-61508-7-2025>