



# SLOVENSKI STANDARD

## oSIST prEN IEC 61508-6:2025

01-maj-2025

---

**Funkcijska varnost električnih/elektronskih/elektronsko programirljivih varnostnih sistemov - 6. del: Smernice za uporabo IEC 61508-2 in IEC 61508-3 (glej Funkcijska varnost in IEC 61508)**

Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3 (see Functional Safety and IEC 61508)

iTeh Standards

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

Sécurité fonctionnelle des systèmes électriques / électroniques / électroniques programmables relatifs à la sécurité - Partie 6: Lignes directrices pour l'application de la cei 61508-2 et de la cei 61508-3

[oSIST prEN IEC 61508-6:2025](https://standards.iteh.ai/en/standards/osist-pr-en-iec-61508-6-2025)

<https://standards.iteh.ai/en/standards/osist-pr-en-iec-61508-6-2025> Ta slovenski standard je istoveten z: [prEN IEC 61508-6:2025](https://standards.iteh.ai/en/standards/osist-pr-en-iec-61508-6-2025)

---

**ICS:**

25.040.40

Merjenje in krmiljenje  
industrijskih postopkov

Industrial process  
measurement and control

**oSIST prEN IEC 61508-6:2025**

**en,fr,de**





PROJECT NUMBER:

**IEC 61508-6 ED3**

DATE OF CIRCULATION:

**2025-03-14**

CLOSING DATE FOR VOTING:

**2025-06-06**

SUPERSEDES DOCUMENTS:

**65A/1061A/CD, 65A/1080B/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  <b>Attention IEC-CENELEC parallel voting</b>  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/62d25bef-3aa2-47fc-8cb3-85085ccc60c0/osist-pren-iec-61508-6-2025>

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 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3 (see Functional Safety and IEC 61508)**

PROPOSED STABILITY DATE: 2027

NOTE FROM TC/SC OFFICERS:

"Due to committee meetings planned at the end of May in Pisa, Italy, it is appreciated to voluntarily submit comments on this Part of the IEC 61508 series by 2025-05-12 already. Of course, there will be all comments accepted for consideration be the committee arriving within the official circulation period, but it will help the committee for starting their work on the project phase."

CONTENTS	
FOREWORD.....	5
INTRODUCTION.....	7
1 Scope.....	9
2 Normative references .....	11
3 Definitions and abbreviations.....	11
Annex A (informative) Application of IEC 61508-2 and of IEC 61508-3.....	12
A.1 General.....	12
A.2 Functional steps in the application of IEC 61508-2.....	14
A.3 Functional steps in the application of IEC 61508-3.....	17
A.4 Architecture considerations.....	19
A.4.1 Architecture Description Identification and Overview .....	20
A.4.2 Stakeholders and Concerns .....	20
Annex B (informative) Example of technique for evaluating probabilities of hardware failure .....	22
B.1 General.....	22
B.2 Considerations about basic probabilistic calculations .....	23
B.2.1 Introduction .....	23
B.2.2 Low demand E/E/PE safety-related system.....	23
B.2.3 Continuous or high demand mode E/E/PE safety-related system .....	24
B.3 Methods of calculating PFD or PFH of a system.....	25
B.3.1 Other available guidance .....	25
B.3.2 Reliability block diagram approach, assuming constant failure rate .....	26
B.3.3 Average frequency of dangerous failure (for high demand or continuous mode of operation) .....	45
B.4 Determination of SILs for E/E/PE Safety-Related Systems with (a) Common Functional Element(s) .....	56
B.4.1 Necessity of multiple protection layers (Multi-PLs).....	56
B.4.2 Redundant channels (CHs) and multi-PLs.....	57
B.4.3 Classification of independency between (E/E/PE) safety-related systems .....	59
B.4.4 Illustrative example of multi-PLs with common FEs classified into Case 2-2.....	59
B.5 Safety integrity and modes of operation of the systems with analytical complexity .....	63
B.6 Handling uncertainties .....	63
B.7 References .....	64
Annex C (informative) Calculation of diagnostic coverage and safe failure fraction – worked example .....	65
Annex D (informative) A methodology for quantifying the effect of hardware-related common cause failures in E/E/PE systems .....	69
D.1 General.....	69
D.1.1 Introduction .....	69
D.1.2 Brief overview.....	69
D.1.3 Defence against common cause failures .....	70
D.1.4 Approach adopted in the IEC 61508 series .....	71
D.2 Scope of the methodology.....	73

49	D.3	Points taken into account in the methodology .....	73
50	D.4	Using the $\beta$ -factor to calculate the probability of failure in an E/E/PE safety- related system due to common cause failures .....	74
51			
52	D.5	Redundancy at system level estimate of $\beta$ .....	75
53	D.6	Redundancy at PCB device level estimation of $\beta$ .....	78
54	D.7	Estimation of $\beta$ suitable for complex semiconductor .....	80
55	D.8	casecasecasecasecaseCaseCaseBinomial failure rate (Shock model) – CCF approach .....	81
56			
57	D.9	References .....	83
58	Annex E (informative)	Example applications of systematic capability tables of IEC 61508-3 .....	84
59			
60	E.1	General.....	84
61	E.2	Example for safety integrity level 2 .....	84
62	E.3	Example for safety integrity level 3 .....	91
63	Annex F Annex F (informative)	Examples on how to include failures of the diagnostic function in the PFH / PFD <sub>AVG</sub> calculation .....	101
64			
65	F.1	Possible approach A .....	101
66	F.2	Possible approach B .....	102
67	F.3	Possible approach C .....	104
68	Annex G (informative)	Failure rate estimation from field feedback, with confidence intervals .....	107
69			
70	G.1	Introduction.....	107
71	G.2	Assumptions for data collection.....	107
72	G.3	Assumptions and notations for parameters estimation.....	108
73	G.4	Failure rate estimation for detected failures .....	108
74	G.5	Failure rate estimation for undetected failures.....	109
75	G.6	Examples of failure rates estimation with upper confidence bound .....	111
76	Annex H	Guidance for robust safety architecture.....	113
77	Bibliography	.....	116
78			
79	Figure A.1	– Application of IEC 61508-2 .....	16
80	Figure A.2	– Application of IEC 61508-2 (Figure A.1 <i>continued</i> ).....	17
81	Figure A.3	– Application of IEC 61508-3 .....	19
82	Figure B.1	– Reliability Block Diagram of a whole safety loop .....	23
83	Figure B.2	– Example configuration for two sensor channels.....	28
84	Figure B.3	– Subsystem structure .....	29
85	Figure B.4	– 1oo1 physical block diagram.....	31
86	Figure B.5	– 1oo1 reliability block diagram.....	31
87	Figure B.6	– 1oo2 physical block diagram .....	32
88	Figure B.7	– 1oo2 reliability block diagram.....	32
89	Figure B.8	– 2oo2 physical block diagram.....	33
90	Figure B.9	– 2oo2 reliability block diagram.....	33
91	Figure B.10	– 1oo2D physical block diagram.....	34
92	Figure B.11	– 1oo2D reliability block diagram .....	34
93	Figure B.12	– – 2oo3 physical block diagram .....	35
94	Figure B.13	– 2oo3 reliability block diagram.....	36
95	Figure B.14	– – Systems block diagram of biped nursing robot .....	57

96	Figure B.15 – – Hazardous event described by FT of multi-PLs .....	58
97	Figure B.16 – – Hazardous event described by FT of multi-CHs system.....	58
98	Figure B.17 – – Reliability block diagrams of typical multi-PLs to control a collision risk	
99	by biped nursing robot .....	60
100	Figure D.1 – Relationship of common cause failures to the failures of individual	
101	channels .....	71
102	Figure D.2 – Implementing shock model with fault trees.....	82
103		
104	Table B.1 – Terms used in this annex (applies to 1oo1, 1oo2, 2oo2, 1oo2D, 1oo3 and	
105	2oo3) .....	28
106	Table B.9 – Example for a non-perfect proof test .....	45
107	Table C.1 – Example calculations for diagnostic coverage and safe failure fraction .....	66
108	Table C.2 – Diagnostic coverage and effectiveness for different elements .....	67
109	Table D.1 – Scoring sensors/final elements .....	75
110	Table D.2 – Scoring Logic Subsystems .....	76
111	Table D.3 – Calculation of $\beta_{DU}$ and $\beta_{DD}$ .....	77
112	Table D.4 – Calculation of $\beta$ for systems with levels of redundancy greater than 1oo2 .....	78
113	Table D.5 – Example of a common cause failure analysis .....	79
114	Table D.6 – Additional Modifier .....	80
115	Table D.7 – Estimation of attributes of $\beta$ -value.....	80
116	Table D.8 – Measures to quantify a $\beta$ -factor.....	81
117	Table E.1 – Software safety requirements specification .....	85
118	Table E.2 – Software design and development – software architecture design .....	85
119	Table E.3 – Software design and development – support tools and programming	
120	language .....	87
121	Table E.4 – Software design and development – detailed design.....	87
122	Table E.5 – Software design and development – software module testing and	
123	integration .....	88
124	Table E.6 – Programmable electronics integration (hardware and software) .....	89
125	Table E.7 – Software aspects of system safety validation .....	89
126	Table E.8 – Software modification .....	90
127	Table E.9 – Software verification .....	90
128	Table E.10 – Functional safety assessment .....	91
129	Table E.11 – Software safety requirements specification .....	92
130	Table E.12 – Software design and development – software architecture design .....	92
131	Table E.13 – Software design and development – support tools and programming	
132	language .....	94
133	Table E.14 – Software design and development – detailed design .....	94
134	Table E.15 – Software design and development – software module testing and	
135	integration .....	96
136	Table E.16 – Programmable electronics integration (hardware and software) .....	97
137	Table E.17 – Software aspects of system safety validation .....	97
138	Table E.18 – Modification .....	98
139	Table E.19 – Software verification .....	99
140	Table E.20 – Software life cycle through lifecycle activities.....	99

## INTERNATIONAL ELECTROTECHNICAL COMMISSION

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

## Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3

## FOREWORD

- 1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as “IEC Publication(s)”). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
- 2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
- 3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
- 4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
- 5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
- 6) All users should ensure that they have the latest edition of this publication.
- 7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
- 8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
- 9) IEC draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). IEC takes no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, IEC had not received notice of (a) patent(s), which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at <https://patents.iec.ch>. IEC shall not be held responsible for identifying any or all such patent rights.

IEC 61508-6 has been prepared by subcommittee 65A: System aspects, of IEC technical committee 65: Industrial-process measurement, control and automation.

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

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

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