SLOVENSKI STANDARD
oSIST prEN IEC 61508-4:2025

01-april-2025

Funkcijska varnost električnih/elektronskih/elektronsko programirljivih varnostnih sistemov - 4. del: Definicije in kratice

Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 4: Definitions and abbreviations

Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme - Teil 4: Begriffe und Abkürzungen

Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité - Partie 4: Définitions et abréviations

Ta slovenski standard je istoveten z: **prEN IEC 61508-4:2025**

ICS:

01.040.25	Izdelavna tehnika (Slovarji)	Manufacturing engineering (Vocabularies)
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 61508-4:2025 **en,fr,de**

65A/1166/CDV

COMMITTEE DRAFT FOR VOTE (CDV)

PROJECT NUMBER: **IEC 61508-4 ED3**	
DATE OF CIRCULATION: **2025-02-14**	CLOSING DATE FOR VOTING: **2025-05-09**
SUPERSEDES DOCUMENTS: **65A/1059A/CD, 65A/1078A/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	
☒ SUBMITTED FOR CENELEC PARALLEL VOTING **Attention IEC-CENELEC parallel voting** The attention of IEC National Committees, members of CENELEC, is drawn to the fact that this Committee Draft for Vote (CDV) is submitted for parallel voting. The CENELEC members are invited to vote through the CENELEC online voting system.	☐ NOT SUBMITTED FOR CENELEC PARALLEL VOTING

This document is still under study and subject to change. It should not be used for reference purposes.

Recipients of this document are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

Recipients of this document are invited to submit, with their comments, notification of any relevant "In Some Countries" clauses to be included should this proposal proceed. Recipients are reminded that the CDV stage is the final stage for submitting ISC clauses. (SEE AC/22/2007 OR NEW GUIDANCE DOC).

TITLE:

Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 4: Definitions and abbreviations

PROPOSED STABILITY DATE: 2028

NOTE FROM TC/SC OFFICERS:

CONTENTS

FOREWORD 4
INTRODUCTION 6
1 Scope 8
2 Normative references 10
3 Definitions and abbreviations 10
3.1 Safety terms 11
3.1.15 human factors <functional safety>, ergonomics usability and interaction between persons and products, devices, services, systems and environments, both real and virtual 13
3.1.16 human error <functional safety> discrepancy between the human action taken or omitted, and the intended or required 13
3.2 Equipment and devices 13
3.2.17 direct verification <software tool output> verification of a software tool’s output that does not depend upon any other software tool 15
3.2.18 indirect verification <software tool output> verification of a software tool’s output that depends upon one or more other software tool(s) or verification of software tool’s output after integration with one or more elements of the system. 15
3.2.19 software lifecycle data all data produced during the software lifecycle 15
3.3 Systems – general aspects 16
3.4 Systems – safety-related aspects 17
3.5 Safety functions and safety integrity 19
3.5.16 low demand mode 22
3.5.17 high demand mode 22
3.5.18 continuous demand mode 22
3.6 Fault, failure and error (see Figure 6) 22
3.7 Lifecycle activities 29
3.7.6 Formal methods 29
3.8 Confirmation of safety measures 30
3.9 Selection of techniques and measures 33
4 Figures and illustrations for definitions and abbreviations 34
4.1 General 34
4.2 Programmable electronic system 34
4.3 E/E/PE system 35
4.4 E/E/PE safety-related system 35
NOTE Subsystem A is a multi-channel subsystem and subsystems B & C are single channel subsystems. 36
4.5 E/E/PE safety-related system 36
4.6 Overall safety function 37
Index 40

Figure 1 – Overall framework of the IEC 61508 series 9
Figure 2 – Programmable electronic system 34
Figure 3 – Electrical/electronic/programmable electronic system (E/E/PE system) – structure and terminology 35
Figure 4 – Physical diagram of the key concepts of E/E/PE safety-related system, subsystem (see 3.4.4) and element (see 3.4.5) 35

Figure 5 – Failure model 36

Table 1 – Abbreviations used in this standard 10

INTERNATIONAL ELECTROTECHNICAL COMMISSION

____

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

Part 4: Definitions and abbreviations

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 61508-4 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 has been subject to a thorough review and incorporates many comments received at the various revision stages.

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,rewording of the information provided in Notes and editing of definitions (e.g. figures and illustratons are moved to clause 4 and referenced by relevant defintions);

b) Set of defintions introduced to cover aspects of:

   i) software off-line support tools;

   ii) software technology classes (‘artificial Intelligence’)

   iii) diagnostic functions;

   iv) levels of independence;

   v) selection of techniques and methods (shortcuts in tables)

c) Various clarifications in defintions and minor editorial errors have been corrected; the normative references and the bibliography has been updated.

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

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

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

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

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

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

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

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

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

INTRODUCTION

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

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

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

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

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

This document

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

- sets a lower limit on the target failure measures for a safety function carried out by a single E/E/PE safety-related system. For E/E/PE safety-related systems operating in
  - a low demand mode of operation, the lower limit is set at an average probability of a dangerous failure on demand of $10^{–5}$;
  - a high demand or a continuous mode of operation, the lower limit is set at an average frequency of a dangerous failure of $10^{–9}$ [$h^{–1}$];

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

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

- sets requirements for the avoidance and control of systematic faults, which are based on experience and judgement from practical experience gained in industry. Even though the probability of occurrence of systematic failures cannot in general be quantified the document does, however, allow a claim to be made, for a specified safety function, that the target failure measure associated with the safety function can be considered to be achieved if all the requirements in the document have been met;
- adopts a broad range of principles, techniques and measures to achieve functional safety for E/E/PE safety-related systems, but does not explicitly use the concept of fail safe However**,** the concepts of “fail safe” and “inherently safe” principles may be applicable and adoption of such concepts is acceptable providing the requirements of the relevant clauses in the document are met.

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

Part 4: Definitions and abbreviations

1 Scope

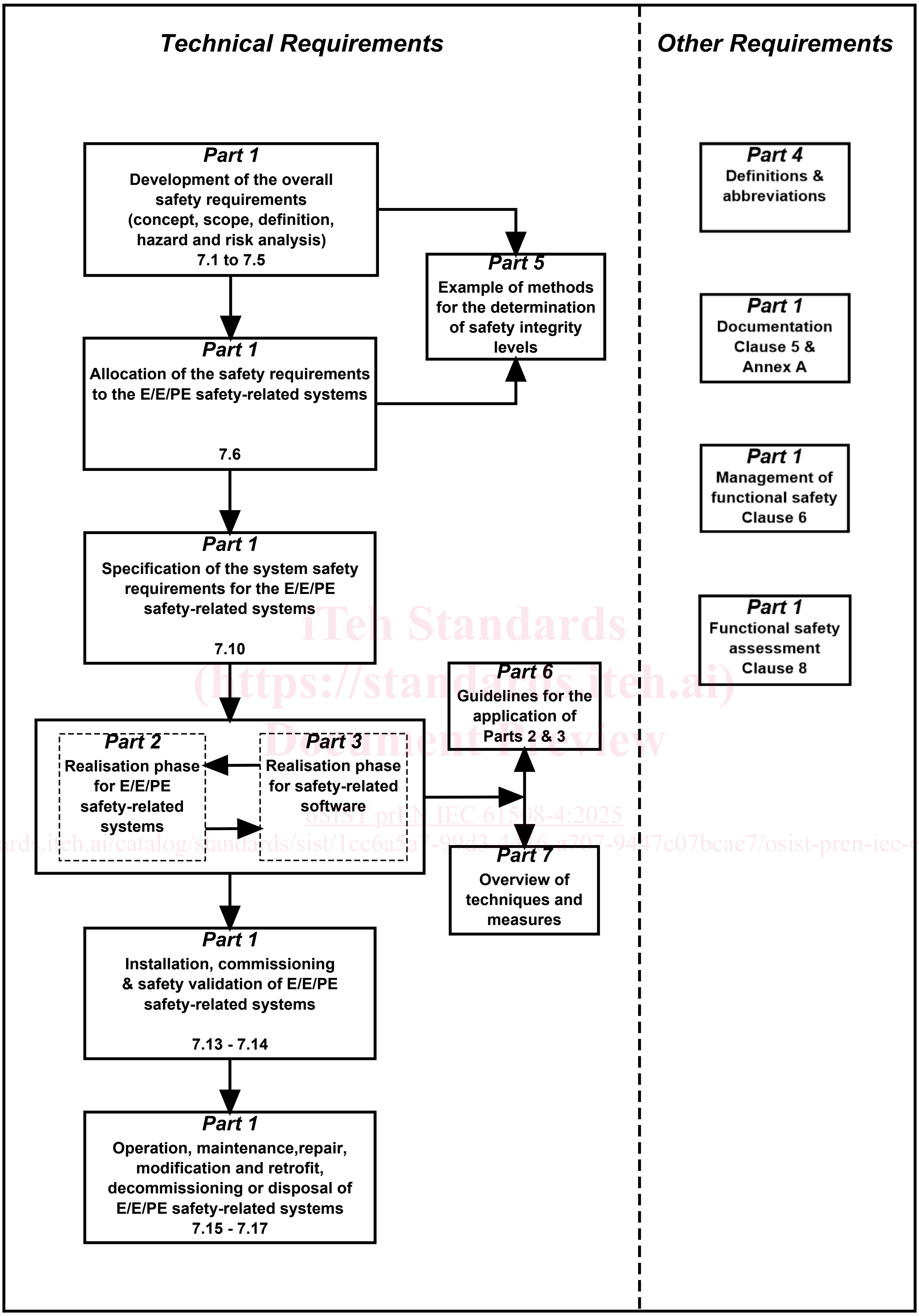
1.1 This part of IEC 61508 contains the definitions and explanation of terms that are used in parts 1 to 7 of the IEC 61508 series of documents.

1.2 The definitions are grouped under general headings so that related terms can be understood within the context of each other. However, it should be noted that these headings are not intended to add meaning to the definitions.

1.3 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).

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

1.5 Figure 1 shows the overall framework of the IEC 61508 series and indicates the role that IEC 61508-4 plays in the achievement of functional safety for E/E/PE safety-related systems.


Technical Requirements
Other Requirements
Part 1
Development of the overall safety requirements (concept, scope, definition, hazard and risk analysis)
7.1 to 7.5
Part 5
Example of methods for the determination of safety integrity levels
Part 1
Allocation of the safety requirements to the E/E/PE safety-related systems
7.6
Part 1
Specification of the system safety requirements for the E/E/PE safety-related systems
7.10
Part 6
Guidelines for the application of Parts 2 & 3
Part 2
Realisation phase for E/E/PE safety-related systems
Part 3
Realisation phase for safety-related software
Part 7
Overview of techniques and measures
Part 1
Installation, commissioning & safety validation of E/E/PE safety-related systems
7.13 - 7.14
Part 1
Operation, maintenance,repair, modification and retrofit, decommissioning or disposal of E/E/PE safety-related systems
7.15 - 7.17
Part 4
Definitions & abbreviations
Part 1
Documentation
Clause 5 &
Annex A
Part 1
Management of functional safety
Clause 6
Part 1
Functional safety assessment
Clause 8

240

241 Figure 1 – Overall framework of the IEC 61508 series

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC Guide 104:2019, *The preparation of safety publications and the use of basic safety publications and group safety publications*

ISO/IEC Guide 51:2014, *Safety aspects – Guidelines for their inclusion in standards*

3 Definitions and abbreviations

For the purposes of this document, the definitions and the abbreviations given in Table 1 below, as well as the following apply.

Table 1 – Abbreviations used in this document

Abbreviation	Full expression	Definition and/or explanation of term
ALARP	As Low As Reasonably Practicable	IEC 61508-5, Annex C
CCF	Common Cause Failure	3.6.10
DC	Diagnostic Coverage	3.8.6
(E)EPLD	(Electrically) Erasable Programmable Logic Device	
E/E/PE	Electrical/Electronic/Programmable Electronic	3.2.13, example: E/E/PE safety-related system
E/E/PE system	Electrical/Electronic/Programmable Electronic System	3.3.2
EEPROM	Electrically Erasable Programmable Read-Only Memory	
EPROM	Erasable Programmable Read-Only Memory	
EUC	Equipment Under Control	3.2.1
FPGA	Field Programmable Gate Array	
GAL	Generic Array Logic	
HFT	Hardware Fault Tolerance	7.4.4 of IEC 61508-2
MooN	M out of N channel architecture (for example 1oo2 is 1 out of 2 architecture, where either of the two channels can perform the safety function)	IEC 61508-6, Annex D
MooND	M out of N channel architecture with Diagnostics (for example 1oo2D is 1 out of 2 architecture, where either of the two channels can perform the safety function and “D” is referred to as either Diagnostics or Degradation)	IEC 61508-6, Annex D
MTBF	Mean Time Between Failures	3.6.19, NOTE 3
MTTR	Mean Time To Restoration	3.6.21
MRT	Mean Repair Time	3.6.22
PAL	Programmable Array Logic	
PE	Programmable Electronic	3.2.12
PEsystem	Programmable Electronic system	3.3.1
PFD	Probability of dangerous Failure on Demand	3.6.17
PFD_{avg}	Average Probability of dangerous Failure on Demand	3.6.18