SLOVENSKI STANDARD
oSIST prEN IEC 61508-1:2025

01-april-2025

Funkcijska varnost električnih/elektronskih/elektronsko programirljivih varnostnih sistemov - 1. del: Splošne zahteve

Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 1: General requirements

Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme - Teil 1: Allgemeine Anforderungen

Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité - Partie 1: Exigences générales

Ta slovenski standard je istoveten z: **prEN IEC 61508-1:2025**

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 61508-1:2025 **en,fr,de**

65A/1164/CDV

COMMITTEE DRAFT FOR VOTE (CDV)

PROJECT NUMBER: **IEC 61508-1 ED3**	
DATE OF CIRCULATION: **2025-02-14**	CLOSING DATE FOR VOTING: **2025-05-09**
SUPERSEDES DOCUMENTS: **65A/1056A/CD, 65A/1075A/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	☐ NOT 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.

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 1: General requirements

PROPOSED STABILITY DATE: 2028

NOTE FROM TC/SC OFFICERS:

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

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

Part 1: General requirements

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 61508-1 has been prepared by subcommittee 65A: System aspects, of IEC technical committee 65: Industrial-process measurement, control and automation. It is an International Standard.

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;

b) The scope includes clarification on ‘artificial Intelligence’ (software technology class), human factors and security. The related requirements are limited to the hazard and risk analysis (refer to 7.1.2.3 on human factors and 7.4.2.3 for security) and further references to external guidance;

c) The interfaces to other parts of IEC 61508 have been clarified and duplication of requirements in other Parts has been removed;

d) The differentiation between the required Safety Integrity Level (SIL) and the achieved Systematic Capability (SC) has been clarified;

e) Requirements on levels of independence for functional safety assurance activities (Annex B) have been introduced;

f) Various 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 international standards based on the IEC 61508 series.

NOTE 1 Examples of product and application sector international standards 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. The safety strategy shall also consider the influence of humans on the achievement of functional safety. 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 international standards 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, through 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 international standards, dealing with E/E/PE safety-related systems, to be developed; the development of product and application sector international standards, 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;

NOTE 2 This 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 3 A single E/E/PE safety-related system does not necessarily mean a single-channel architecture.

NOTE 4 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 this 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 this 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 concept 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 this documentare met.

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

Part 1: General requirements

1 Scope

1.1 This document covers those aspects to be considered when electrical/electronic/programmable electronic (E/E/PE) systems are used to carry out safety functions. A major objective of t

The goal of this document is to facilitate the development of product and application sector international standards by the technical committees responsible for the product or application sector. This will allow all the relevant factors, associated with the product or application, to be fully taken into account and thereby meet the specific needs of users of the product and the application sector. A second objective of this document is to enable the development of E/E/PE safety-related systems where product or application sector international standards do not exist.

The scope of this document is functional safety for E/E/PE safety-related systems but, apart from normative requirements in the hazard and risk analysis phase, does not itself provide normative requirements for malevolent action arising from a cybersecurity risk. However, if a cybersecurity assessment has identified that a reasonably foreseeable cyber security risk will arise, it is essential that measures be taken for all relevant phases of the overall, E/E/PE and software safety lifecycles in order to protect against such threats to ensure that functional safety is achieved.

NOTE 1 For requirements and/or guidance on cybersecurity see IEC 62443 series and ISO/IEC 27000 series.

NOTE 2 For guidance on the coordination between safety and security refer to IEC TR 63069.

1.2 In particular, this document

a) applies to safety-related systems when one or more of such systems incorporates electrical/electronic/programmable electronic elements;

NOTE 1 In the context of low complexity E/E/PE safety-related systems, certain requirements specified in this document can be unnecessary, and exemption from compliance with such requirements is possible (see 4.2, and the definition of a low complexity E/E/PE safety-related system in 3.4.3 of IEC 61508-4).

NOTE 2 Although a person can form part of a safety-related system (see 3.4.1 of IEC 61508-4), human factor requirements related to those aspects of the design of E/E/PE safety-related systems are not considered in detail in this document.

NOTE 3 This document can be applied to custom, low-volume and high volume production safety-related systems, subsystems, elements and compliant items.

NOTE 4 This document can be applied to parts of the safety function (e.g., compliant item or tool) but it does not provide a final SIL statement to a part of the safety function.

b) is generically based and applicable to all E/E/PE safety-related systems irrespective of the application;

c) covers the achievement of a tolerable risk through the application of E/E/PE safety-related systems, but does not cover hazards arising from the E/E/PE equipment itself (for example electric shock);

d) applies to all types of E/E/PE safety-related systems, including protection systems and control systems;

e) does not cover E/E/PE systems where

– a single E/E/PE system is capable on its own of meeting the tolerable risk, and

– the required quantitative performance and integrity of the safety functions of the single E/E/PE system is less than that specified for safety integrity level 1 (the lowest safety integrity level in this document).

f) is mainly concerned with the E/E/PE safety-related systems whose failure could have an impact on the safety of persons and/or the environment; however, it is recognized that the consequences of failure could also have serious economic implications and in such cases this document could be used to specify any E/E/PE system used for the protection of equipment or product;

NOTE 7 See 3.1.1 of IEC 61508-4.

g) considers E/E/PE safety-related systems and other risk reduction measures, in order that the safety requirements specification for the E/E/PE safety-related systems can be determined in a systematic, risk-based manner;

h) uses an overall safety lifecycle model as the organisational framework for dealing systematically with the processes and activities necessary for ensuring the functional safety of the E/E/PE safety-related systems;

NOTE 8 Although the overall safety lifecycle is primarily concerned with E/E/PE safety-related systems, it might also provide a technical framework for considering any safety-related system irrespective of the technology of that system (for example mechanical, hydraulic or pneumatic).

i) specifies the essential concept of safety integrity levels applicable to any sector application;

j) does not specify the selection of safety integrity levels required to address risks specific to sector applications (which must be based on detailed information and knowledge of the sector application).

k) provides general requirements for E/E/PE safety-related systems where no product or application sector international standards exist;

l) requires malevolent and unauthorised actions to be considered during hazard and risk analysis. The scope of the analysis includes all relevant safety lifecycle phases;

NOTE 9 For further details refer to ISO/IEC TR 19791 and IEC 62443 series.

m) does not cover the precautions that may be necessary to prevent unauthorized persons damaging, and/or otherwise adversely affecting, the functional safety of E/E/PE safety-related systems (see k) above);

n) does not specify the requirements for the development, implementation, maintenance and/or operation of security policies or security services needed to meet a security policy that may be required by the E/E/PE safety-related system;

o) does apply to software algorithms of software technology class I;

does apply to software algorithms of software technology class II and in combination with the additional requirements provided in ISO/IEC TS 22440.

NOTE 1 The software technology classes relate to the generically used term “artificial intelligence” as defined in ISO/IEC 22989; for defintions refer to 61508-4, Clauses 3.2.15, 3.2.16 and 3.2.17.

NOTE 2 Refer to ISO/IEC TR 5469:2024 and to ISO/IEC TS 22440-1 for further details.

NOTE 3 The concept of safety integrity level as described in this document can be applied to the hardware used to execute or implement software algorithms of software technology class I, II or III

1.3 This part of the IEC 61508 series of standards includes general requirements that are applicable to all parts. Other parts of the IEC 61508 series concentrate on topics that are more specific:

– parts 2 and 3 provide additional and specific requirements for E/E/PE safety-related systems (part 2 for hardware and part 3 for software);

– part 4 gives definitions and abbreviations that are used throughout all parts of this document;

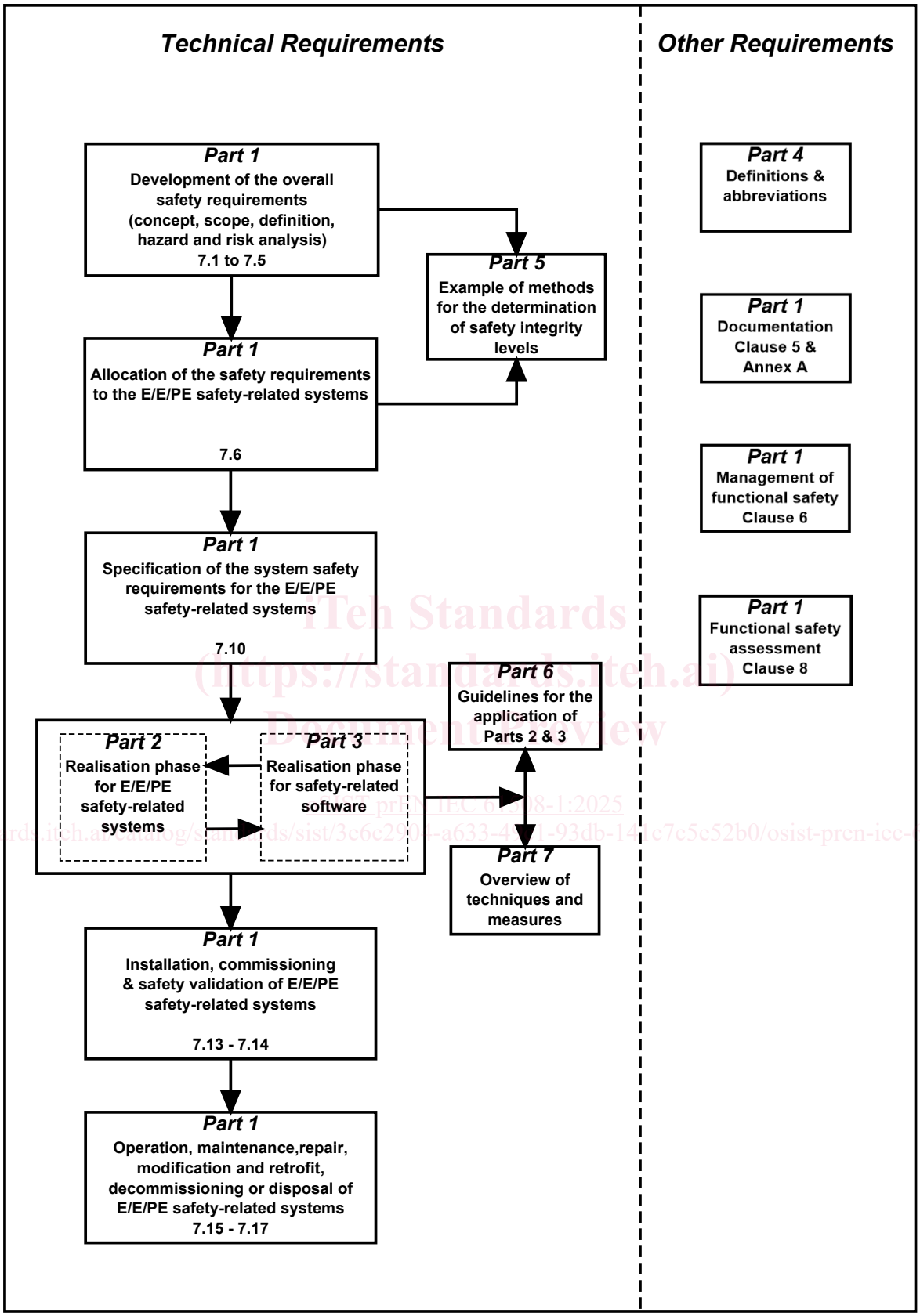
– part 5 provides guidelines on the application of part 1 in determining safety integrity levels, by showing example methods;

– part 6 provides guidelines on the application of parts 2 and 3;

– part 7 contains an overview of techniques and measures.

1.4 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).

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



390

391 **Figure 1 – Overall framework of the IEC 61508 series**