SLOVENSKI STANDARD
oSIST prEN IEC 61508-5:2025

01-april-2025

Funkcijska varnost električnih/elektronskih/elektronsko programirljivih varnostnih sistemov - 5. del: Primeri metod za ugotavljanje ravni celovite varnosti

Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 5: Examples of methods for the determination of safety integrity levels

Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme - Teil 5: Beispiele zur Ermittlung der Stufe der Sicherheitsintegrität (safety integrety level)

Sécurité fonctionnelle des systèmes électriques / électroniques / électroniques programmables relatifs à la sécurité - Partie 5: Exemples de méthodes pour la détermination des niveaux d'intégrité de sécurité

Ta slovenski standard je istoveten z: **prEN IEC 61508-5:2025**

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 61508-5:2025 **en,fr,de**

65A/1167/CDV

COMMITTEE DRAFT FOR VOTE (CDV)

PROJECT NUMBER: **IEC 61508-5 ED3**	
DATE OF CIRCULATION: **2025-02-14**	CLOSING DATE FOR VOTING: **2025-05-09**
SUPERSEDES DOCUMENTS: **65A/1060A/CD, 65A/1079A/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 5: Examples of methods for the determination of safety integrity levels

PROPOSED STABILITY DATE: 2028

NOTE FROM TC/SC OFFICERS:

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

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

Part 5: Examples of methods for the determination of safety integrity levels

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 61508-5 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 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 and rewording of the information provided in Notes;

b) Various minor editorial errors have been corrected, the normative references and the bibliography has been updated.

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 should 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 international standards and in revisions of those that already exist.

This International Standard

- 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 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 standard, 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 standard 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 may 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 standard 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 standard have been met;

– introduces systematic capability which applies to an element with respect to the confidence that its systematic safety integrity meets the requirements of the specified safety integrity level;

– 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 standard are met.

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

Part 5: Examples of methods for the determination of safety integrity levels

1 Scope

1.1 This part of IEC 61508 provides information on

– the underlying concepts of risk and the relationship of risk to safety integrity (see Annex A);

– the criteria in selecting the most appropriate method for determining safety integrity level requirements (see Annex B);

– a number of methods that will enable the safety integrity levels for the E/E/PE safety-related systems to be determined (see Annexes C, D, E, F and G).

The method selected will depend upon the application sector and the specific circumstances under consideration. Annexes C, D, E, F and G illustrate quantitative and qualitative approaches and have been simplified in order to illustrate the underlying principles. These annexes have been included to illustrate the general principles of a number of methods but do not provide a definitive account.

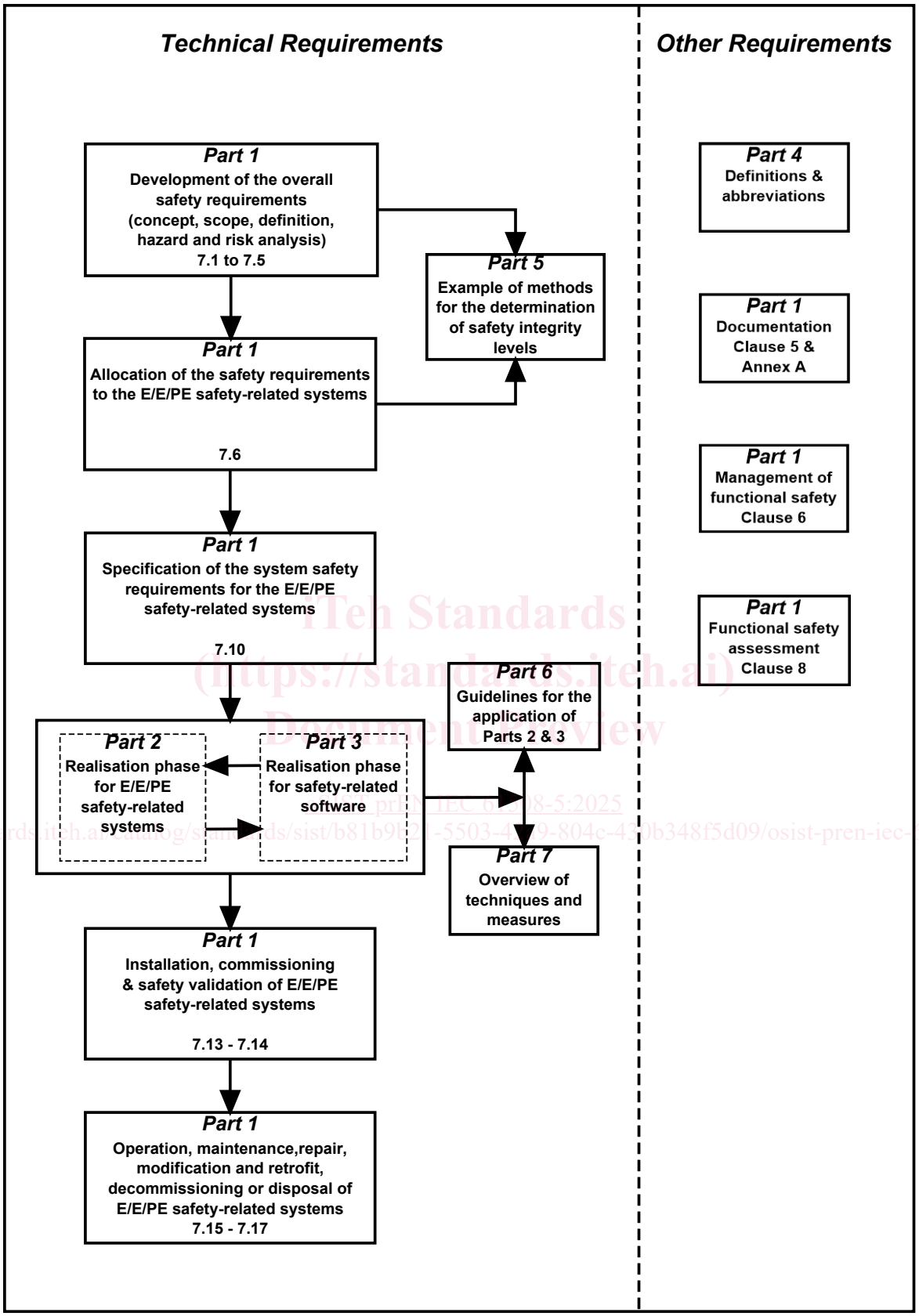
NOTE 1 Those intending to apply the methods indicated in these annexes can consult the source material referenced.

NOTE 2 For more information on the approaches illustrated in Annexes B, and E, see references [5] and [8] in the Bibliography. See also reference [6] in the Bibliography for a description of an additional approach.

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

1.3 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.

1.4 Figure 1 shows the overall framework of the IEC 61508 series and indicates the role that IEC 61508-5 plays in the achievement of functional safety for E/E/PE safety-related systems.



297

298 **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 61508-1:20XX, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements*

IEC 61508-4:20XX, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 4: Definitions and abbreviations*

3 Definitions and abbreviations

For the purposes of this document, the definitions and abbreviations given in IEC 61508-4 apply.

Annex A
(informative)

Risk and safety integrity – General concepts

A.1 General

This annex provides information on the underlying concepts of risk and the relationship of risk to safety integrity.

A.2 Necessary risk reduction

The necessary risk reduction is the reduction in risk that has to be achieved to meet the tolerable risk for a specific situation (which may be stated either qualitatively[1] or quantitatively[2]). The concept of necessary risk reduction is of fundamental importance in the development of the safety requirements specification for the E/E/PE safety-related systems (in particular, the safety integrity requirements part of the safety requirements specification). The purpose of determining the tolerable risk for a specific hazardous event is to state what is deemed reasonable with respect to both the frequency (or probability) of the hazardous event and its specific consequences. Safety-related systems are designed to reduce the frequency (or probability) of the hazardous event and/or the consequences of the hazardous event.

The tolerable risk will depend on many factors (for example, severity of injury, the number of people exposed to danger, the frequency at which a person or people are exposed to danger and the duration of the exposure). Important factors will be the perception and views of those exposed to the hazardous event. In arriving at what constitutes a tolerable risk for a specific application, a number of inputs are considered. These include:

- legal requirements, both general and those directly relevant to the specific application;
- guidelines from the appropriate safety regulatory authority;
- discussions and agreements with the different parties involved in the application;
- industry standards and guidelines;
- international discussions and agreements; the role of national and international standards is becoming increasingly important in arriving at tolerable risk criteria for specific applications;
- the best independent industrial, expert and scientific advice from advisory bodies.

In determining the safety integrity requirements of the E/E/PE safety-related system(s) and other risk reduction measures, in order to meet the tolerable frequency of a hazardous event, account needs to be taken of the characteristics of the risk that are relevant to the application. The tolerable frequency will depend on the legal requirements in the country of application and on the criteria specified by the user organisation. Issues that may need to be considered together with how they can be applied to E/E/PE safety-related systems are discussed below.

---

1 In achieving the tolerable risk, the necessary risk reduction will need to be established. Annexes E and G of this document outline qualitative methods, although in the examples quoted the necessary risk reduction is incorporated implicitly by specification of the SIL requirement rather than stated explicitly by a numeric value of risk reduction required.

2 For example, that the hazardous event, leading to a specific consequence, can not occur with a frequency greater than one in 10^8 h.