SLOVENSKI STANDARD
oSIST prEN IEC 61508-3:2025

01-april-2025

Funkcijska varnost električnih/elektronskih/elektronsko programirljivih varnostnih sistemov - 3. del: Programske zahteve

Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 3: Software requirements

Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme - Teil 3: Anforderungen an Software

Sécurité fonctionnelle des systèmes électriques / électroniques / électroniques programmables relatifs à la sécurité - Partie 3: Exigences concernant les logiciels

Ta slovenski standard je istoveten z: **prEN IEC 61508-3:2025**

ICS:

25.040.40	Merjenje in krmiljenje industrijskih postopkov	Industrial process measurement and control

oSIST prEN IEC 61508-3:2025 **en,fr,de**

65A/1169/CDV

COMMITTEE DRAFT FOR VOTE (CDV)

PROJECT NUMBER:	
IEC 61508-3 ED3	
DATE OF CIRCULATION:	CLOSING DATE FOR VOTING:
2025-02-21	**2025-05-16**
SUPERSEDES DOCUMENTS:	
65A/1058A/CD, 65A/1077A/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 3: Software 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 3: Software 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 [and/or] www.iso.org/patents. IEC shall not be held responsible for identifying any or all such patent rights.

IEC 61508-3 has been prepared by subcommittee SC65A: SYSTEM ASPECTS, of IEC technical committee TC65: 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:

This document has been upgraded to the 2024 version of the ISO/IEC Directives; this does introduce a significant number of editorial changes and Clause renumbering throughout. In addition, the following technical changes have been made:

a) All requirements on use of artificial Intelligence, security and human factors are limited to the references in Scope to external guidance

b) The requirements of IEC TS 61508-3-1 have been incorporated into Clause 7 and extended to address requirements to achieve Systematic Capability SC3 and SC4

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

d) The requirement to undertake software functional failure analysis has been transferred from the requirements for functional safety assessment to the requirements on architectural design and renamed software failure analysis; the differentiation between functional safety audit, functional safety assessment and software failure analysis has been clarified in IEC 61508-7

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

f) The requirements for formal methods has been clarified throughout all software lifecycle phases, the requirements of TS 61508-3-2 have been referenced in this document and IEC 61508-7 and the concept of semi-formal methods has been re-instated to the status in Edition 2 of this document; the meaning of ‘unambiguously defined’ methods has been clarified

g) Rules for synthesis of software elements has been clarified; detailed requirements on software used in diagnostics is now addressed in IEC 61508-2

h) The requirements on software off-line support tools have been refined

i) The guidance on data driven systems has been provided in a separate Annex from the guidance on data configuration and limited variability programming; the guidance on limited variability programming has been updated to be consistent with IEC 61131-1.

j) The requirements in Annex A on modification have been re-instated to the status in Edition 2 and clarified

k) An additional table has been added to define requirements on management activities which occur throughout the entire software lifecycle; this table includes requirements on traceability, which have been removed from individual phase requirements

l) Requirements on regression testing have been clarified

m) The use of the terminology ‘verification’ and ‘validation’ has been brought in line with the definitions in IEC 61508-4; much supplementary information added at Ed 3 CD has been transferred to IEC 61508-7 as informative guidance, or else deleted

n) The requirements on the use of object oriented design and development have been brought in line with practical applications; further detail is being developed in TR 61508-3-3

o) Various minor editorial errors have been corrected.

NOTE In order to avoid the need for extensive editing to existing compliance tools, the methods and techniques specified in Annex A and Annex B of this document have retained their original reference ID. Where methods and techniques have been deleted the phrase ‘Not Used’ has been entered. Where methods and techniques have been added an additional row with additional reference ID have been added. As far as possible this also applies to Clauses in the body of the document, but some renumbering has been inevitable where information has been added.

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

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
XX/XX/FDIS	XX/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

- 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.

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 considers not only all the elements within an individual system (for example sensors, controlling devices and actuators) and humans as part of the system, as part of the realization process, operation, and management of verification/decision making), 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 can also provide a framework within which safety-related systems based on other technologies can 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 1 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 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 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 as a measure of confidence that an E/E/PE system meets the safety requirements with regards to avoidance and control of systematic faults;

– 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” can 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 3: Software requirements

1 Scope

1.1 This part of the IEC 61508 series:

a) is intended to be utilized only after a thorough understanding of, and in conjunction with, the requirements of IEC 61508-1 and IEC 61508-2;

b) applies to any software forming part of a safety-related system or used to develop a safety-related system within the scope of IEC 61508-1 and IEC 61508-2. Such software is termed safety-related software (including operating systems, system software, software in communication networks, human-computer interface functions, and firmware as well as application software);

c) provides specific requirements applicable to support tools used to develop and configure a safety-related system within the scope of IEC 61508-1 and IEC 61508-2;

d) requires that the software safety functions and their systematic capability are specified;

NOTE 1 If this has already been done as part of the specification of the E/E/PE safety-related systems (see 7.2 of IEC 61508-2), then it does not have to be repeated in this part.

NOTE 2 Specifying the software safety functions and their systematic capability is an iterative procedure; see Figure 5 and Figure 6.

NOTE 3 See IEC 61508-1 Clause 5 and IEC 61508-1 Annex A for documentation structure. The documentation structure can be organised to take account of company procedures, and of the working practices of specific application sectors.

NOTE 4 See IEC 61508-4 3.5.8 for definition of the term "systematic capability".

e) establishes requirements for safety lifecycle phases and activities which shall be applied during the design and development of the safety-related software (the software safety lifecycle model). These requirements include the application of measures and techniques, which are graded against the required systematic capability, for the avoidance of and control of faults and failures in the software;

f) provides requirements for information relating to the software aspects of system safety validation to be passed to the organisation carrying out the E/E/PE system integration;

g) provides requirements for the preparation of information and procedures concerning software needed by the user for the operation and maintenance of the E/E/PE safety-related system;

h) provides requirements to be met by the organisation carrying out modifications to safety-related software;

i) provides, in conjunction with IEC 61508-1 and IEC 61508-2, requirements for support tools such as development and design tools, language translators, testing and debugging tools, configuration management tools;

NOTE 5 Figure 5 shows the relationship between IEC 61508-2 and this document.

j) Not used;

k) Does apply to software algorithms

  i. software technology class I (see definition in IEC 61508-4 Clause 3.2.14);

  ii. software technology class II and III (see definitions in IEC 61508-4, Clause 3.2.15 and Clause 3.2 16)