



SLOVENSKI STANDARD

SIST EN 61508-1:2011

01-maj-2011

Nadomešča:
SIST EN 61508-1:2007

Funkcijska varnost električnih/elektronskih/elektronsko programirljivih varnostnih sistemov - 1. del: Splošne zahteve (IEC 61508-1:2010)

Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 1: General requirements (IEC 61508-1:2010)

Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme - Teil 1: Allgemeine Anforderungen (IEC 61508-1:2010)

Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité - Partie 1: Prescriptions générales (CEI 61508-1:2010)

Ta slovenski standard je istoveten z: EN 61508-1:2010

ICS:

25.040.40	Merjenje in krmiljenje industrijskih postopkov	Industrial process measurement and control
-----------	--	--

SIST EN 61508-1:2011 en

iTeh STANDARD PREVIEW
(standards.iteh.ai)

SIST EN 61508-1:2011

<https://standards.iteh.ai/catalog/standards/sist/799a4626-1815-4454-b18b-747434d03920/sist-en-61508-1-2011>

EUROPEAN STANDARD
NORME EUROPÉENNE
EUROPÄISCHE NORM

EN 61508-1

May 2010

ICS 13.110; 25.040; 29.020

Supersedes EN 61508-1:2001

English version

**Functional safety of electrical/electronic/programmable electronic
safety-related systems -
Part 1: General requirements
(IEC 61508-1:2010)**

Sécurité fonctionnelle des systèmes
électriques/électroniques/électroniques
programmables relatifs à la sécurité -
Partie 1: Exigences générales
(CEI 61508-1:2010)

Funktionale Sicherheit sicherheitsbezogener
elektrischer/elektronischer/programmierbarer
elektronischer Systeme -Teil 1: Allgemeine
Anforderungen
(IEC 61508-1:2010)

iTeh STANDARD PREVIEW
(standards.iteh.ai)

This European Standard was approved by CENELEC on 2010-05-01. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the Central Secretariat or to any CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CENELEC member into its own language and notified to the Central Secretariat has the same status as the official versions.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland and the United Kingdom.

CENELEC

European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung

Management Centre: Avenue Marnix 17, B - 1000 Brussels

Foreword

The text of document 65A/548/FDIS, future edition 2 of IEC 61508-1, prepared by SC 65A, System aspects, of IEC TC 65, Industrial-process measurement, control and automation, was submitted to the IEC-CENELEC parallel vote and was approved by CENELEC as EN 61508-1 on 2010-05-01.

This European Standard supersedes EN 61508-1:2001.

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

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN and CENELEC shall not be held responsible for identifying any or all such patent rights.

The following dates were fixed:

- latest date by which the EN has to be implemented at national level by publication of an identical national standard or by endorsement (dop) 2011-02-01
- latest date by which the national standards conflicting with the EN have to be withdrawn (dow) 2013-05-01

Annex ZA has been added by CENELEC.

~~iTeh STANDARD PREVIEW~~ (standards.iteh.ai)

Endorsement notice

The text of the International Standard IEC 61508-1:2010 was approved by CENELEC as a European Standard without any modification. [SIST EN 61508-1:2011](https://standards.iteh.ai/catalog/standards/sist/799a4626-1815-4454-8100-747434059208/iec-61508-1-2011)

In the official version, for Bibliography, the following notes have to be added for the standards indicated:

- | | |
|-------------------------|--|
| [1] IEC 61511 series | NOTE Harmonized in EN 61511 series (not modified). |
| [2] IEC 62061 | NOTE Harmonized as EN 62061. |
| [3] IEC 61800-5-2 | NOTE Harmonized as EN 61800-5-2. |
| [5] IEC 61508-6:2010 | NOTE Harmonized as EN 61508-6:2010 (not modified). |
| [6] IEC 61508-7:2010 | NOTE Harmonized as EN 61508-7:2010 (not modified). |
| [10] IEC 60300-3-1:2003 | NOTE Harmonized as EN 60300-3-1:2004 (not modified). |
| [15] IEC 61326-3-1 | NOTE Harmonized as EN 61326-3-1. |
| [17] IEC 61355 series | NOTE Harmonized in EN 61355 series (not modified). |
| [18] IEC 60601 series | NOTE Harmonized in EN 60601 series (partially modified). |
| [20] IEC 61508-5:2010 | NOTE Harmonized as EN 61508-5:2010 (not modified). |

Annex ZA (normative)

Normative references to international publications with their corresponding European publications

The following referenced documents are indispensable for the application 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.

NOTE When an international publication has been modified by common modifications, indicated by (mod), the relevant EN/HD applies.

<u>Publication</u>	<u>Year</u>	<u>Title</u>	<u>EN/HD</u>	<u>Year</u>
IEC 61508-2	2010	Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems	EN 61508-2	2010
IEC 61508-3	2010	Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 3: Software requirements	EN 61508-3	2010
IEC 61508-4	2010	Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 4: Definitions and abbreviations	EN 61508-4	2010
IEC Guide 104	1997	The preparation of safety publications and the use of basic safety publications and group safety publications	-	-
ISO/IEC Guide 51	1999	Safety aspects - Guidelines for their inclusion in standards	-	-

iTeh STANDARD PREVIEW
(standards.iteh.ai)

SIST EN 61508-1:2011

<https://standards.iteh.ai/catalog/standards/sist/799a4626-1815-4454-b18b-747434d03920/sist-en-61508-1-2011>



IEC 61508-1

Edition 2.0 2010-04

INTERNATIONAL STANDARD

NORME INTERNATIONALE

BASIC SAFETY PUBLICATION

PUBLICATION FONDAMENTALE DE SÉCURITÉ

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

SÉCURITÉ FONCTIONNELLE DES SYSTÈMES ÉLECTRIQUES/ÉLECTRONIQUES/ÉLECTRONIQUES
PROGRAMMABLES RELATIFS À LA SÉCURITÉ –
Partie 1: Exigences générales

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

PRICE CODE **XB**
CODE PRIX

ICS 13.110; 25.040; 29.020

ISBN 978-2-88910-524-3

CONTENTS

FOREWORD.....	5
INTRODUCTION.....	7
1 Scope.....	9
2 Normative references.....	12
3 Definitions and abbreviations	12
4 Conformance to this standard	12
5 Documentation	13
5.1 Objectives	13
5.2 Requirements	13
6 Management of functional safety.....	14
6.1 Objectives	14
6.2 Requirements	14
7 Overall safety lifecycle requirements	17
7.1 General	17
7.1.1 Introduction	17
7.1.2 Objectives and requirements – general	20
7.1.3 Objectives	25
7.1.4 Requirements	25
7.2 Concept.....	25
7.2.1 Objective	25
7.2.2 Requirements	26
7.3 Overall scope definition	26
7.3.1 Objectives	26
7.3.2 Requirements	26
7.4 Hazard and risk analysis	27
7.4.1 Objectives	27
7.4.2 Requirements	27
7.5 Overall safety requirements	28
7.5.1 Objective	29
7.5.2 Requirements	29
7.6 Overall safety requirements allocation.....	30
7.6.1 Objectives	30
7.6.2 Requirements	31
7.7 Overall operation and maintenance planning	35
7.7.1 Objective	35
7.7.2 Requirements	35
7.8 Overall safety validation planning	37
7.8.1 Objective	37
7.8.2 Requirements	37
7.9 Overall installation and commissioning planning.....	38
7.9.1 Objectives	38
7.9.2 Requirements	38
7.10 E/E/PE system safety requirements specification	38
7.10.1 Objective	39
7.10.2 Requirements	39
7.11 E/E/PE safety-related systems – realisation	41

7.11.1	Objective	41
7.11.2	Requirements	41
7.12	Other risk reduction measures – specification and realisation.....	41
7.12.1	Objective	41
7.12.2	Requirements	41
7.13	Overall installation and commissioning.....	41
7.13.1	Objectives	41
7.13.2	Requirements	42
7.14	Overall safety validation.....	42
7.14.1	Objective	42
7.14.2	Requirements	42
7.15	Overall operation, maintenance and repair.....	43
7.15.1	Objective	43
7.15.2	Requirements	43
7.16	Overall modification and retrofit	46
7.16.1	Objective	46
7.16.2	Requirements	47
7.17	Decommissioning or disposal.....	48
7.17.1	Objective	48
7.17.2	Requirements	48
7.18	Verification.....	49
7.18.1	Objective	49
7.18.2	Requirements.....	49
8	Functional safety assessment.....	50
8.1	Objective	50
8.2	Requirements	50
https://standards.iteh.ai/catalog/standards/sist/799a4626-1813-4454-b18b-747434d03920/sist-en-61508-1-2011		
SIST EN 61508-1:2011		
(standards.iteh.ai)		
Annex A (informative) Example of a documentation structure.....		
Bibliography.....		
Figure 1 – Overall framework of the IEC 61508 series		
Figure 2 – Overall safety lifecycle		
Figure 3 – E/E/PE system safety lifecycle (in realisation phase).....		
Figure 4 – Software safety lifecycle (in realisation phase)		
Figure 5 – Relationship of overall safety lifecycle to the E/E/PE system and software safety lifecycles.....		
Figure 6 – Allocation of overall safety requirements to E/E/PE safety-related systems and other risk reduction measures.....		
Figure 7 – Example of operations and maintenance activities model		
Figure 8 – Example of operation and maintenance management model		
Figure 9 – Example of modification procedure model		
Figure A.1 – Structuring information into document sets for user groups		
Table 1 – Overall safety lifecycle – overview.....		
Table 2 – Safety integrity levels – target failure measures for a safety function operating in low demand mode of operation		
Table 3 – Safety integrity levels – target failure measures for a safety function operating in high demand mode of operation or continuous mode of operation		

Table 4 – Minimum levels of independence of those carrying out functional safety assessment (overall safety lifecycle phases 1 to 8 and 12 to 16 inclusive (see Figure 2))	53
Table 5 – Minimum levels of independence of those carrying out functional safety assessment (overall safety lifecycle phases 9 and 10, including all phases of E/E/PE system and software safety lifecycles (see Figures 2, 3 and 4))	53
Table A.1 – Example of a documentation structure for information related to the overall safety lifecycle	56
Table A.2 – Example of a documentation structure for information related to the E/E/PE system safety lifecycle.....	57
Table A.3 – Example of a documentation structure for information related to the software safety lifecycle	58

iTeh STANDARD PREVIEW **(standards.iteh.ai)**

SIST EN 61508-1:2011

<https://standards.iteh.ai/catalog/standards/sist/799a4626-1815-4454-b18b-747434d03920/sist-en-61508-1-2011>

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.
<https://standards.iteh.ai/catalog/standards/sist/799a4626-1815-4454-3103-109270381008/iec-61508-1-2010>
- 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) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

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

This second edition cancels and replaces the first edition published in 1998. 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.

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

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

FDIS	Report on voting
65A/548/FDIS	65A/572/RVD

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

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2

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 publication will remain unchanged until the maintenance result date indicated on the IEC web site under "<http://webstore.iec.ch>" in the data related to the specific publication. At this date, the publication will be

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)

SIST EN 61508-1:2011

<https://standards.iteh.ai/catalog/standards/sist/799a4626-1815-4454-b18b-747434d03920/sist-en-61508-1-2011>

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 International Standard 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 must 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 International Standard 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 International Standard, 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, 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 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;

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

NOTE 4 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 its confidence that the 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.

SIST EN 61508-1:2011

<https://standards.itech.ai/catalog/standards/sist/799a4626-1815-4454-b18b-747434d03920/sist-en-61508-1-2011>

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

Part 1: General requirements

1 Scope

1.1 This International Standard 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 this standard 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 standard is to enable the development of E/E/PE safety-related systems where product or application sector international standards do not exist.

1.2 In particular, this standard

- 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 standard may 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 the design of E/E/PE safety-related systems are not considered in detail in this standard.

- 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 safety 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 standard).
- 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 standard could be used to specify any E/E/PE system used for the protection of equipment or product;

NOTE 3 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 technical framework for dealing systematically with the activities necessary for ensuring the functional safety of the E/E/PE safety-related systems;