SLOVENSKI STANDARD
SIST EN 61508-2:2011

01-maj-2011

Nadomešča:
SIST EN 61508-2:2007

Funkcijska varnost električnih/elektronskih/programljivih elektronskih varnostnih sistemov - 2. del: Zahteve za električne/elektronske/programljive elektronske varnostne sisteme (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 (IEC 61508-2:2010)

iTeh STANDARD PREVIEW
(standards.iteh.ai)

Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme - Teil 2: Anforderungen an sicherheitsbezogene elektrische/elektronische/programmierbare elektronische Systeme (IEC 61508-2:2010)

SIST EN 61508-2:2011
https://standards.iteh.ai/catalog/standards/sist/37ac1149-cf81-4a42-8979-98c4b87bcb2d/sist-en-61508-2-2011

Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité - Partie 2: Prescriptions pour les systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité (CEI 61508-2:2010)

Ta slovenski standard je istoveten z: **EN 61508-2:2010**

ICS:

25.040.40	Merjenje in krmiljenje industrijskih postopkov	Industrial process measurement and control

SIST EN 61508-2:2011 **en**

2003-01.Slovenski inštitut za standardizacijo. Razmnoževanje celote ali delov tega standarda ni dovoljeno.

SIST EN 61508-2:2011

iTeh STANDARD PREVIEW
(standards.iteh.ai)

SIST EN 61508-2:2011
https://standards.iteh.ai/catalog/standards/sist/37ac1149-cf81-4a42-8979-98c4b876cb2d/sist-en-61508-2-2011

SIST EN 61508-2:2011

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 61508-2

May 2010

ICS 25.040.40

Supersedes EN 61508-2:2001

English version

Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems

(IEC 61508-2:2010)

Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité - Partie 2: Exigences pour les systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité

(CEI 61508-2:2010)

Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme - Teil 2: Anforderungen an sicherheitsbezogene elektrische/elektronische/programmierbare elektronische Systeme

(IEC 61508-2:2010)

iTeh STANDARD PREVIEW
(standards.iteh.ai)

SIST EN 61508-2:2011
https://standards.iteh.ai/catalog/standards/sist/37ac1149-cf81-4a42-8979-98c4b876cb2d/sist-en-61508-2-2011

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

© 2010 CENELEC - All rights of exploitation in any form and by any means reserved worldwide for CENELEC members.

Ref. No. EN 61508-2:2010 E

SIST EN 61508-2:2011

Foreword

The text of document 65A/549/FDIS, future edition 2 of IEC 61508-2, 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 61508-2 on 2010-05-01.

This European Standard supersedes EN 61508-2:2001.

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 61508-2:2010 was approved by CENELEC as a European Standard without any modification.

SIST EN 61508-2:2011
https://standards.iteh.ai/catalog/standards/sist/37ac1149-cf81-4a42-8979-

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

9bc4b87/0cb2/sist-en-61508-2-2011

[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.
[4] IEC 61508-5:2010	NOTE	Harmonized as EN 61508-5:2010 (not modified).
[5] IEC 61508-6:2010	NOTE	Harmonized as EN 61508-6:2010 (not modified).
[6] IEC 60601 series	NOTE	Harmonized in EN 60601 series (partially modified).
[7] IEC 61165	NOTE	Harmonized as EN 61165.
[8] IEC 61078	NOTE	Harmonized as EN 61078.
[9] IEC 61164	NOTE	Harmonized as EN 61164.
[10] IEC 62308	NOTE	Harmonized as EN 62308.
[11] IEC 61000-6-2	NOTE	Harmonized as EN 61000-6-2.
[12] ISO 14224	NOTE	Harmonized as EN ISO 14224.
[14] ISO 9000	NOTE	Harmonized as EN ISO 9000.
[15] IEC 60300-3-2	NOTE	Harmonized as EN 60300-3-2.

SIST EN 61508-2:2011

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.

Publication	Year	Title	EN/HD	Year
-	-	Relays with forcibly guided (mechanically linked) contacts	EN 50205	-
IEC 60947-5-1	-	Low-voltage switchgear and controlgear - Part 5-1: Control circuit devices and switching elements - Electromechanical control circuit devices	EN 60947-5-1	-
IEC/TS 61000-1-2	-	Electromagnetic compatibility (EMC) - Part 1-2: General - Methodology for the achievement of functional safety of electrical and electronic systems including equipment with regard to electromagnetic phenomena	-	-
IEC 61326-3-1	-	Electrical equipment for measurement, control and laboratory use - EMC requirements - Part 3-1: Immunity requirements for safety-related systems and for equipment intended to perform safety-related functions (functional safety) - General industrial applications	EN 61326-3-1	-
IEC 61508-1	2010	Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 1: General requirements	EN 61508-1	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 61508-7	2010	Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 7: Overview of techniques and measures	EN 61508-7	2010
IEC 61784-3	-	Industrial communication networks - Profiles - Part 3: Functional safety fieldbuses - General rules and profile definitions	EN 61784-3	-

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST EN 61508-2:2011
https://standards.iteh.ai/catalog/standards/sist/57ac1149-cf81-4a42-8979-98c4b876cb2d/sist-en-61508-2-2011

SIST EN 61508-2:2011

Publication	Year	Title	EN/HD	Year
IEC 62280-1	-	Railway applications - Communication, signalling and processing systems - Part 1: Safety-related communication in closed transmission systems	-	-
IEC 62280-2	-	Railway applications - Communication, signalling and processing systems - Part 2: Safety-related communication in open transmission systems	-	-
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 61508-2:2011
https://standards.iteh.ai/catalog/standards/sist/37ac1149-cf81-4a42-8979-98c4b876cb2d/sist-en-61508-2-2011

SIST EN 61508-2:2011

IEC 61508-2

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 2: Requirements for electrical/electronic/programmable electronic safety-related systems

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST EN 61508-2:2011
https://standards.iteh.ai/catalog/standards/sist/37ac1149-cf81-4a42-8979-

Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité –
Partie 2: Exigences pour les systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité

INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMISSION ELECTROTECHNIQUE INTERNATIONALE

PRICE CODE
CODE PRIX XD

ICS 25.040.40

ISBN 978-2-88910-525-0

® Registered trademark of the International Electrotechnical Commission
Marque déposée de la Commission Electrotechnique Internationale

SIST EN 61508-2:2011

CONTENTS

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST EN 61508-2:2011
https://standards.iteh.ai/catalog/standards/sist/37ac1149-cf81-4a42-8979-98c4b876cb2d/sist-en-61508-2-2011

SIST EN 61508-2:2011

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST EN 61508-2:2011
https://standards.iteh.ai/catalog/standards/sist/37ac1149-cf81-4a42-8979-
9b4837e62d1a/sist-en-61508-2-2011

SIST EN 61508-2:2011

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST EN 61508-2:2011
https://standards.iteh.ai/catalog/standards/sist/37ac1149-cf81-4a42-8979-98c4b876cb2d/sist-en-61508-2-2011

SIST EN 61508-2:2011

INTERNATIONAL ELECTROTECHNICAL COMMISSION

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

Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems

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) 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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST EN 61508-2:2011
https://standards.iteh.ai/catalog/standards/sist/37ac9149-c181-4a42-8979-98c4b876cb2d/sist-en-61508-2-2011

International Standard IEC 61508-2 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 2000. 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.

SIST EN 61508-2:2011

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

FDIS	Report on voting
65A/549/FDIS	65A/573/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 61508-2:2011
https://standards.iteh.ai/catalog/standards/sist/37ac1149-cf81-4a42-8979-98c4b876cb2d/sist-en-61508-2-2011

SIST EN 61508-2:2011

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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST EN 61508-2:2011
https://standards.iteh.ai/catalog/standards/sist/37ec1149-cf81-4a42-8979-
98a4b876cb2d/sist-en-61508-2-2011

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, 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;

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.

SIST EN 61508-2:2011

- sets target failure measures for safety functions carried out by E/E/PE safety-related systems, which are linked to the safety integrity levels;
- 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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST EN 61508-2:2011
https://standards.iteh.ai/catalog/standards/sist/37ac1149-cf81-4a42-8979-98c4b876cb2d/sist-en-61508-2-2011

SIST EN 61508-2:2011

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

Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems

1 Scope

1.1 This part of the IEC 61508 series

a) is intended to be used only after a thorough understanding of IEC 61508-1, which provides the overall framework for the achievement of functional safety;

b) applies to any safety-related system, as defined by IEC 61508-1, that contains at least one electrical, electronic or programmable electronic element;

c) applies to all elements within an E/E/PE safety-related system (including sensors, actuators and the operator interface);

d) specifies how to refine the E/E/PE system safety requirements specification, developed in accordance with IEC 61508-1 (comprising the E/E/PE system safety functions requirements specification and the E/E/PE system safety integrity requirements specification), into the E/E/PE system design requirements specification;

e) specifies the requirements for activities that are to be applied during the design and manufacture of the E/E/PE safety-related systems (i.e. establishes the E/E/PE system safety lifecycle model) except software, which is dealt with in IEC 61508-3 (see Figures 2 to 4). These requirements include the application of techniques and measures that are graded against the safety integrity level, for the avoidance of, and control of, faults and failures;

f) specifies the information necessary for carrying out the installation, commissioning and final safety validation of the E/E/PE safety-related systems;

g) does not apply to the operation and maintenance phase of the E/E/PE safety-related systems – this is dealt with in IEC 61508-1 – however, IEC 61508-2 does provide requirements for the preparation of information and procedures needed by the user for the operation and maintenance of the E/E/PE safety-related systems;

h) specifies requirements to be met by the organisation carrying out any modification of the E/E/PE safety-related systems;

NOTE 1 This part of IEC 61508 is mainly directed at suppliers and/or in-company engineering departments, hence the inclusion of requirements for modification.

NOTE 2 The relationship between IEC 61508-2 and IEC 61508-3 is illustrated in Figure 4.

i) does not apply for medical equipment in compliance with the IEC 60601 series.

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). As basic safety publications, they are intended for use by technical committees in the preparation of standards in accordance with the principles contained in IEC Guide 104 and ISO/IEC Guide 51. IEC 61508-1, IEC 61508-2, IEC 61508-3 and IEC 61508-4 are also intended for use as stand-alone standards. The horizontal safety function of this international standard does not apply to medical equipment in compliance with the IEC 60601 series.

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST EN 61508-2:2011
https://standards.iteh.ai/catalog/standards/sist/37ac1149-e181-4a42-8979-98c4b876cb2d/sist-en-61508-2-2011