# SLOVENSKI STANDARD

# SIST EN 61508-2:2007

januar 2007

**Funkcijska varnost električnih/elektronskih/programirljivih elektronskih varnostnih sistemov - 2. del: Zahteve za električne/elektronske/programirljive elektronske varnostne sisteme (IEC 61508-2:2000)**

**(istoveten EN 61508-2:2001)**

Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems (IEC 61508-2:2000)



ICS 25.040.40

Referenčna številka
SIST EN 61508-2:2007(en)

EUROPEAN STANDARD **EN 61508-2**

NORME EUROPÉENNE

EUROPÄISCHE NORM December 2001

ICS 25.040.40

English version

# Functional safety of electrical/electronic/programmable electronic safety-related systems
# Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems
(IEC 61508-2:2000)

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 61508-2:2000)

Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme
Teil 2: Anforderungen an sicherheitsbezogene elektrische/elektronische/programmierbare elektronische Systeme
(IEC 61508-2:2000)



This European Standard was approved by CENELEC on 2001-07-03. 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, Czech Republic, Denmark, Finland, France, Germany, Greece, Iceland, Ireland, Italy, Luxembourg, Malta, Netherlands, Norway, Portugal, Spain, Sweden, Switzerland and United Kingdom.

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

**Central Secretariat: rue de Stassart 35, B - 1050 Brussels**



Ref. No. EN 61508-2:2001 E

## Foreword

The text of the International Standard IEC 61508-2:2000, prepared by SC 65A, System aspects, of IEC TC 65, Industrial-process measurement and control, was submitted to the Unique Acceptance Procedure and was approved by CENELEC as EN 61508-2 on 2001-07-03 without any modification.

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) 2002-08-01

– latest date by which the national standards conflicting with the EN have to be withdrawn (dow) 2004-08-01

Annexes designated "normative" are part of the body of the standard.
In this standard, annexes A, B, C and ZA are normative.
Annex ZA has been added by CENELEC.

IEC 61508 is a basic safety publication covering the functional safety of electrical, electronic and programmable electronic safety-related systems. The scope states:

"This International Standard covers those aspects to be considered when electrical/electronic/programmable electronic systems (E/E/PESs) are used to carry out safety functions. A major objective of this standard is to facilitate the development of application sector international standards by the technical committees responsible for the application sector. This will allow all the relevant factors associated with the application, to be fully taken into account and thereby meet the specific needs of the application sector. A dual objective of this standard is to enable the development of electrical/electronic/programmable electronic (E/E/PE) safety-related systems where application sector international standards may not exist".



The CENELEC Report R0BT-004, ratified by 103 BT (March 2000) accepts that some IEC standards, which today are either published or under development, are sector implementations of IEC 61508. For example:

- IEC 61511, Functional safety - Safety instrumented systems for the process industry sector;
- IEC 62061, Safety of machinery – Functional safety of electrical, electronic and programmable electronic control systems;
- IEC 61513, Nuclear power plants – Instrumentation and control for systems important to safety – General requirements for systems.

The railways sector has also developed a set of European Standards (EN 50126; EN 50128 and prEN 50129).

NOTE EN 50126 and EN 50128 were based on earlier drafts of IEC 61508. prEN 50129 is based on the principles of the latest version of IEC 61508.

This list does not preclude other sector implementations of IEC 61508 which could be currently under development or published within IEC or CENELEC.

———————

## Endorsement notice

The text of the International Standard IEC 61508-2:2000 was approved by CENELEC as a European Standard without any modification.

In the official version, for Bibliography, the following note has to be added for the standard indicated:

| | | |
|---|---|---|
| IEC 61000-4 | NOTE | Harmonized in the EN 61000-4 series (not modified). |
| IEC 60870-5-1 | NOTE | Harmonized as EN 60870-5-1:1993 (not modified). |

## Annex ZA
(normative)

## Normative references to international publications with their corresponding European publications

This European Standard incorporates by dated or undated reference, provisions from other publications. These normative references are cited at the appropriate places in the text and the publications are listed hereafter. For dated references, subsequent amendments to or revisions of any of these publications apply to this European Standard only when incorporated in it by amendment or revision. For undated references the latest edition of the publication referred to applies (including amendments).

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 |
|---|---|---|---|---|
| IEC 60050-371 | 1984 | International electrotechnical vocabulary (IEV) - Chapter 371: Telecontrol | - | - |
| IEC 60300-3-2 | 1993 | Dependability management<br>Part 3: Application guide<br>Section 2: Collection of dependability data from the field | - | - |
| IEC 61000-1-1 | 1992 | Electromagnetic compatibility (EMC)<br>Part 1: General<br>Section 1: Application and interpretation of fundamental definitions and terms | - | - |
| IEC 61000-2-5 | 1995 | Part 2-5: Environment - Classification of electromagnetic environments - Basic EMC publication | - | - |
| IEC 61508-1<br>+ corr. May | 1998<br>1999 | Functional safety of electrical/electronic/programmable electronic safety-related systems<br>Part 1: General requirements | EN 61508-1 | 2001 |
| IEC 61508-3<br>+ corr. April | 1998<br>1999 | Part 3: Software requirements | EN 61508-3 | 2001 |
| IEC 61508-4<br>+ corr. April | 1998<br>1999 | Part 4: Definitions and abbreviations | EN 61508-4 | 2001 |
| IEC 61508-5<br>+ corr. April | 1998<br>1999 | Part 5: Examples of methods for the determination of safety integrity levels | EN 61508-5 | 2001 |
| IEC 61508-6 | 2000 | Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3 | EN 61508-6 | 2001 |
| IEC 61508-7 | 2000 | Part 7: Overview of techniques and measures | EN 61508-7 | 2001 |
| IEC Guide 104 | 1997 | The preparation of safety publications and the use of basic safety publications and group safety publications | - | - |

| Publication | Year | Title | EN/HD | Year |
|---|---|---|---|---|
| ISO/IEC Guide 51 | 1990 | Guidelines for the inclusion of safety aspects in standards | - | - |
| IEEE 352 | 1987 | IEEE guide for general principles of reliability analysis of nuclear power generating station safety systems | - | - |

# INTERNATIONAL STANDARD

# IEC 61508-2

First edition
2000-05

BASIC SAFETY PUBLICATION

## Functional safety of electrical/electronic/ programmable electronic safety-related systems –

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





International Electrotechnical Commission, 3, rue de Varembé, PO Box 131, CH-1211 Geneva 20, Switzerland
Telephone: +41 22 919 02 11 Telefax: +41 22 919 03 00 E-mail: inmail@iec.ch Web: www.iec.ch

Commission Electrotechnique Internationale
International Electrotechnical Commission
Международная Электротехническая Комиссия

PRICE CODE XB

*For price, see current catalogue*

# CONTENTS

Page

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 IEC (International Electrotechnical Commission) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of the 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, the IEC publishes International Standards. 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. The 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 the 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 National Committees.

3) The documents produced have the form of recommendations for international use and are published in the form of standards, technical specifications, technical reports or guides and they are accepted by the National Committees in that sense.

4) In order to promote international unification, IEC National Committees undertake to apply IEC International Standards transparently to the maximum extent possible in their national and regional standards. Any divergence between the IEC Standard and the corresponding national or regional standard shall be clearly indicated in the latter.

5) The IEC provides no marking procedure to indicate its approval and cannot be rendered responsible for any equipment declared to be in conformity with one of its standards.

6) Attention is drawn to the possibility that some of the elements of this International Standard may be the subject of patent rights. The IEC shall not be held responsible for identifying any or all such patent rights.



International Standard IEC 61508-2 has been prepared by subcommittee 65A: System aspects, of IEC technical committee 65: Industrial-process measurement and control.

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/294/FDIS | 65A/303/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 3.

Annexes A, B, and C form an integral part of this standard.

IEC 61508 consists of the following parts, under the general title *Functional safety of electrical/electronic/programmable electronic safety-related systems*:

– Part 1: General requirements
– Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems
– Part 3: Software requirements
– Part 4: Definitions and abbreviations
– Part 5: Examples of methods for the determination of safety integrity levels
– Part 6: Guidelines on the application of parts 2 and 3
– Part 7: Overview of techniques and measures

The committee has decided that the contents of this publication will remain unchanged until 2006. At this date, the publication will be

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

# INTRODUCTION

Systems comprised of electrical and/or electronic components have been used for many years to perform safety functions in most application sectors. Computer-based systems (generically referred to as programmable electronic systems (PESs)) 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 those 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 components (electrical/electronic/programmable electronic systems (E/E/PESs)) 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 application sector standards.

In most situations, safety is achieved by a number of protective systems which may 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 electrical/electronic/programmable electronic (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 recognised that there is a great variety of E/E/PES applications 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 application sector International Standards.



This International Standard

- considers all relevant overall, E/E/PES and software safety lifecycle phases (for example, from initial concept, through design, implementation, operation and maintenance to decommissioning) when E/E/PESs 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 application sector International Standards, dealing with safety-related E/E/PESs, to be developed; the development of application sector International Standards, within the framework of this International 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;
- uses 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;

– adopts a risk-based approach for the determination of the safety integrity level requirements;

– sets numerical target failure measures for E/E/PE safety-related systems which are linked to the safety integrity levels;

– sets a lower limit on the target failure measures, in a dangerous mode of failure, that can be claimed for 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 failure of $10^{-5}$ to perform its design function on demand,

  – a high demand or continuous mode of operation, the lower limit is set at a probability of a dangerous failure of $10^{-9}$ per hour;

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

– adopts a broad range of principles, techniques and measures to achieve functional safety for E/E/PE safety-related systems, but does not rely on the concept of fail safe which may be of value when the failure modes are well defined and the level of complexity is relatively low. The concept of fail safe was considered inappropriate because of the full range of complexity of E/E/PE safety-related systems that are within the scope of the standard.