SVENSK STANDARD SS-EN 61508-2

Fastställd	Utgåva	Sida	Ingår i
2002-10-09	1	1 (1+72)	SEK Område 65

Svenska Elektriska Kommissionen, SEK

Funktionssäkerhet hos elektriska, elektroniska och programmerbara elektroniska säkerhetskritiska system – Del 2: Fordringar på elektriska, elektroniska och programmerbara elektroniska säkerhetskritiska system

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

Som svensk standard gäller europastandarden EN 61508-2:2001. Den svenska standarden innehåller den officiella engelska språkversionen av EN 61508-2:2001.

Nationellt förord

Europastandarden EN 61508-2:2001

består av:

- **europastandardens ikraftsättningsdokument,** utarbetat inom CENELEC
- **IEC 61508-2, First edition, 2000 - Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems**

  utarbetad inom International Electrotechnical Commission, IEC.

ICS 25.040.40

Denna standard är fastställd av Svenska Elektriska Kommissionen, SEK,
som också kan lämna upplysningar om **sakinnehållet** i standarden.
Postadress: SEK, Box 1284, 164 29 KISTA
Telefon: 08 - 444 14 00. *Telefax*: 08 - 444 14 30
E-post: sek@sekom.se. *Internet*: www.sekom.se

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 Part 3: Application guide Section 2: Collection of dependability data from the field	-	-
IEC 61000-1-1	1992	Electromagnetic compatibility (EMC) Part 1: General 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 + corr. May	1998 1999	Functional safety of electrical/electronic/programmable electronic safety-related systems Part 1: General requirements	EN 61508-1	2001
IEC 61508-3 + corr. April	1998 1999	Part 3: Software requirements	EN 61508-3	2001
IEC 61508-4 + corr. April	1998 1999	Part 4: Definitions and abbreviations	EN 61508-4	2001
IEC 61508-5 + corr. April	1998 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	-	-

CONTENTS

Page

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 IEC 61508

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, which contains at least one electrical, electronic or programmable electronic based component;

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

d) specifies how to refine the information developed in accordance with IEC 61508-1, concerning the overall safety requirements and their allocation to E/E/PE safety-related systems, and specifies how the overall safety requirements are refined into E/E/PES safety functions requirements and E/E/PES safety integrity requirements;

e) specifies 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/PES safety lifecycle model), except for software, which is dealt with by IEC 61508-3 (see figures 2 and 3) – these requirements include the application of techniques and measures, which 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 3.

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 3.4.4 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 is also intended for use as a stand-alone standard.

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.

NOTE 1 The functional safety of an E/E/PE safety-related system can only be achieved when all related requirements are met. Therefore, it is important that all related requirements are carefully considered and adequately referenced.

NOTE 2 In the USA and Canada, until the proposed sector implementation of IEC 61508 (i.e. IEC 61511) is published as an international standard in the USA and Canada, existing national process safety standards based on IEC 61508 (i.e. ANSI/ISA-S84.01) can be applied to the process sector instead of IEC 61508.

1.3 Figure 1 shows the overall framework for parts 1 to 7 of IEC 61508 and indicates the role that IEC 61508-2 plays in the achievement of functional safety for E/E/PE safety-related systems. Annex A of IEC 61508-6 describes the application of IEC 61508-2 and IEC 61508-3.

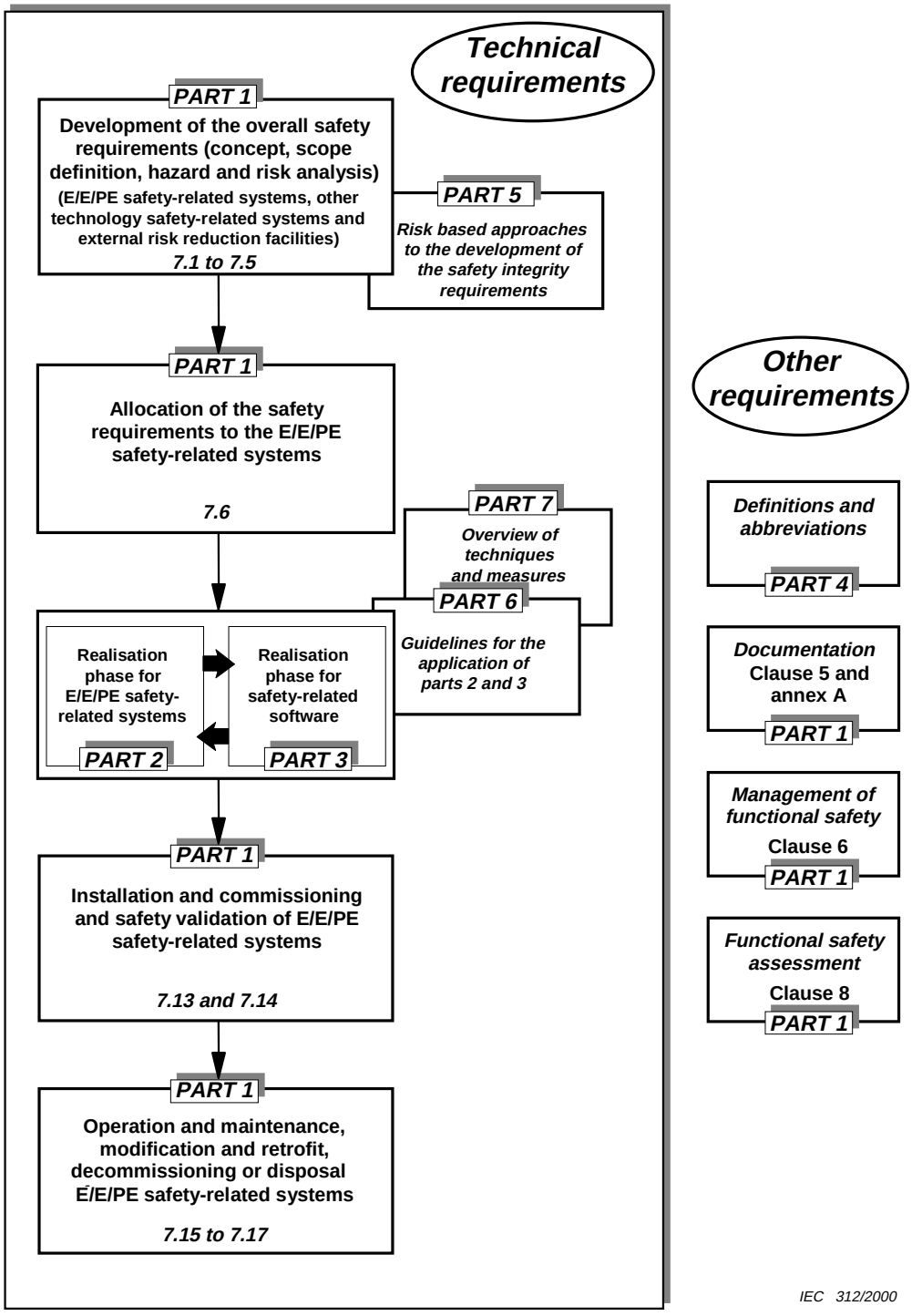

Figure 1 – Overall framework of IEC 61508