SVENSK STANDARD SS-EN 61508-1

Fastställd	Utgåva	Sida	Ingår i
2002-10-09	1	1 (1+60)	SEK Område 65

Svenska Elektriska Kommissionen, SEK

Funktionssäkerhet hos elektriska, elektroniska och programmerbara elektroniska säkerhetskritiska system – Del 1: Allmänna fordringar

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

Som svensk standard gäller europastandarden EN 61508-1:2001. Den svenska standarden innehåller den officiella engelska språkversionen av EN 61508-1:2001.

Nationellt förord

Europastandarden EN 61508-1:2001

består av:

– **europastandardens ikraftsättningsdokument,** utarbetat inom CENELEC
– **IEC 61508-1[*)], First edition, 1998 - Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 1: General requirements**

utarbetad inom International Electrotechnical Commission, IEC.

[*)] Se även bifogat Corrigendum, maj 1999, till IEC 61508-1:1998.

ICS 13.110; 25.040; 29.020; 35.240.50

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 61508-1**

NORME EUROPÉENNE

EUROPÄISCHE NORM December 2001

ICS 13.110;25.040;29.020;35.240.50

English version

Functional safety of electrical/electronic/programmable electronic safety-related systems
Part 1: General requirements
(IEC 61508-1:1998 + corrigendum 1999)

Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité
Partie 1: Prescriptions générales
(CEI 61508-1:1998 + corrigendum 1999)

Funktionale Sicherheit sicherheitsbezogener elektrischer/ elektronischer/programmierbarer elektronischer Systeme
Teil 1: Allgemeine Anforderungen
(IEC 61508-1:1998 + Corrigendum 1999)

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 61508-1:2001 E

Foreword

The text of the International Standard IEC 61508-1:1998 including its corrigendum May 1999, 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 61508-1 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.
Annexes designated "informative" are given for information only.
In this standard, annex ZA is normative and annexes A, B and C are informative.
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 61508-1:1998 including its corrigendum May 1999 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 61355:1997 NOTE Harmonized as EN 61355:1997 (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
ISO/IEC Guide 51	1990	Guidelines for the inclusion of safety aspects in standards	-	-
IEC Guide 104	1997	The preparation of safety publications and the use of basic safety publications and group safety publications	-	-
IEC 61508-2	2000	Functional safety of electrical/electronic/programmable electronic safety-related systems Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems	EN 61508-2	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

CONTENTS

Page

Clause

Annexes

Tables

Figures

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 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.

1.2 In particular, this standard

a) applies to safety-related systems when one or more of such systems incorporates electrical/electronic/programmable electronic devices;

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 3.4.4 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 possible hazards caused by failures of the safety functions to be performed by E/E/PE safety-related systems, as distinct from hazards arising from the E/E/PE equipment itself (for example electric shock etc);

d) does not cover E/E/PE systems where

   – a single E/E/PE system is capable of providing the necessary risk reduction, and

   – the required safety integrity of the E/E/PE system is less than that specified for safety integrity level 1 (the lowest safety integrity level in this standard).

e) 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 – See 3.1.1 and 7.3.1.2 of IEC 61508-4.

f) considers E/E/PE safety-related systems, other technology safety-related systems and external risk reduction facilities in order that the safety requirements specification for the E/E/PE safety-related systems can be determined in a systematic, risk-based manner;

g) 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;

NOTE 3 – The early phases of the overall safety lifecycle include, of necessity, consideration of other technology (as well as the E/E/PE safety-related systems) and external risk reduction facilities, in order that the safety requirements specification for the E/E/PE safety-related systems can be developed in a systematic, risk-based manner.

NOTE 4 – Although the overall safety lifecycle is primarily concerned with E/E/PE safety-related systems, it could also provide a technical framework for the consideration of any safety-related system irrespective of the technology of that system (for example mechanical, hydraulic or pneumatic).

h) does not specify the safety integrity levels required for sector applications (which must be based on detailed information and knowledge of the sector application). The technical committees responsible for the specific application sectors shall specify, where appropriate, the safety integrity levels in the application sector standards;

i) provides general requirements for E/E/PE safety-related systems where no application sector standards exist;

j) does not cover the precautions that may be necessary to prevent unauthorized persons damaging, and/or otherwise adversely affecting, the functional safety of E/E/PE safety-related systems.

1.3 This part of IEC 61508 specifies the general requirements that are applicable to all parts. Other parts of IEC 61508 concentrate on more specific topics:

– parts 2 and 3 provide additional and specific requirements for E/E/PE safety-related systems (for hardware and software);

– part 4 gives definitions and abbreviations that are used throughout this standard;

– part 5 provides guidelines on the application of part 1 in determining safety integrity levels, by showing example methods;

– part 6 provides guidelines on the application of parts 2 and 3;

– part 7 contains an overview of techniques and measures.

1.4 Parts 1, 2, 3 and 4 of this standard 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 part 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*. Parts 1, 2, 3, and 4 are also intended for use as stand-alone publications.

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 – In the USA and Canada, until the proposed process sector implementation of IEC 61508 is published as an international standard in the USA and Canada, existing national process safety standards based on IEC 61508 (i.e. ANSI/ISA S84.01-1996) (see reference [8] in annex C) can be applied to the process sector instead of IEC 61508.

1.5 Figure 1 shows the overall framework for parts 1 to 7 of IEC 61508 and indicates the role that IEC 61508-1 plays in the achievement of functional safety for E/E/PE safety-related systems.

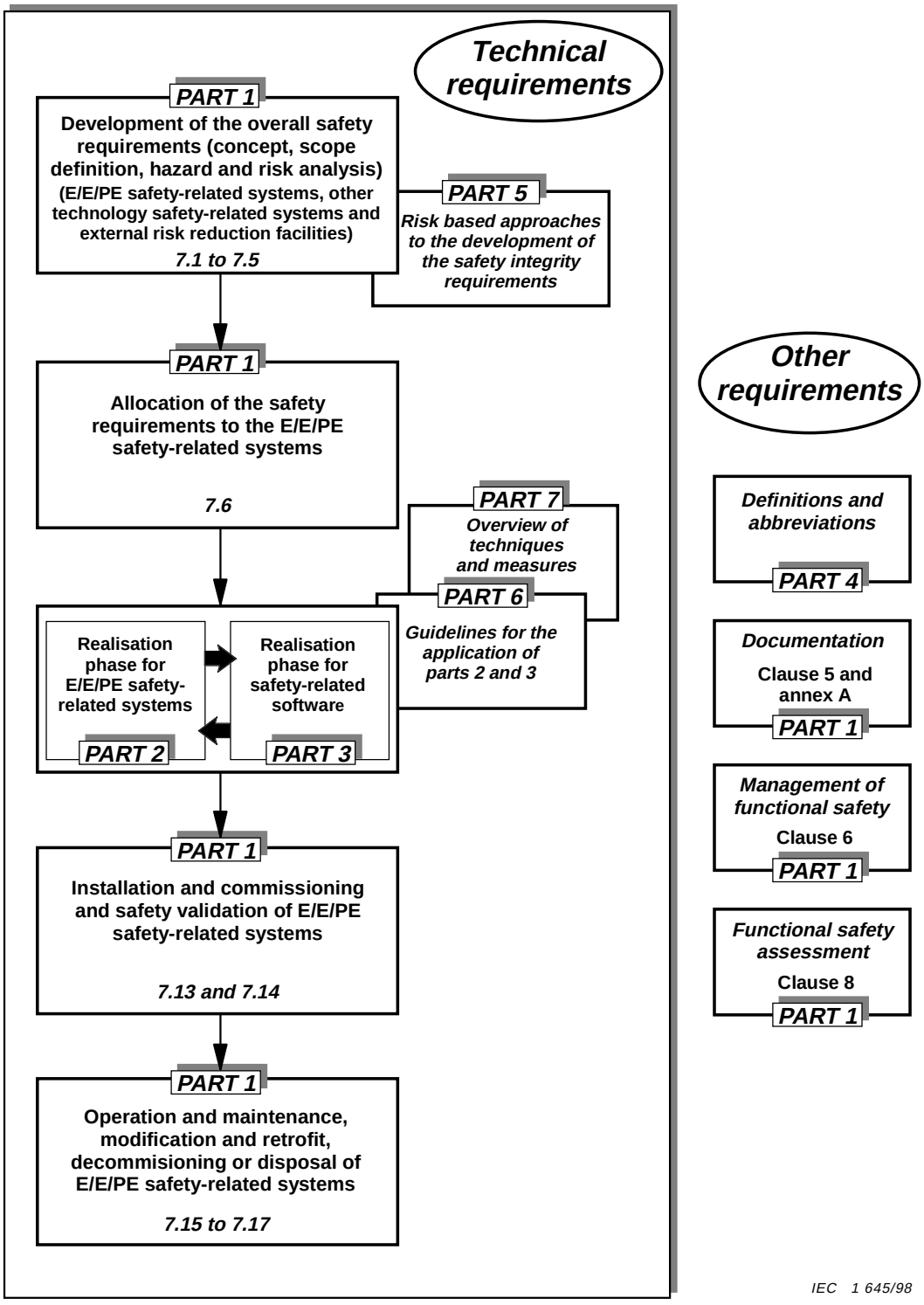

Figure 1 – Overall framework of this standard