SEK

SVENSK STANDARD SS-EN 61508-3

Svenska Elektriska Kommissionen, SEK

Fastställd	Utgåva	Sida	Ingår i
2002-10-09	1	1 (1+49)	SEK Område 65

Funktionssäkerhet hos elektriska, elektroniska och programmerbara elektroniska säkerhetskritiska system – Del 3: Fordringar på programvara

Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 3: Software requirements

Som svensk standard gäller europastandarden EN 61508-3:2001. Den svenska standarden innehåller den officiella engelska språkversionen av EN 61508-3:2001.

Nationellt förord

Europastandarden EN 61508-3:2001

består av:

- **europastandardens ikraftsättningsdokument,** utarbetat inom CENELEC
- **IEC 61508-3**[*]**, First edition, 1998 - Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 3: Software requirements**

utarbetad inom International Electrotechnical Commission, IEC.

[*] Se även bifogat Corrigendum, april 1999, till IEC 61508-3:1998.

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 61508-3**

NORME EUROPÉENNE

EUROPÄISCHE NORM December 2001

ICS 25.040.40

English version

Functional safety of electrical/electronic/programmable electronic safety-related systems
Part 3: Software requirements
(IEC 61508-3:1998 + corrigendum 1999)

Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité
Partie 3: Prescriptions concernant les logiciels
(CEI 61508-3:1998 + corrigendum 1999)

Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme
Teil 3: Anforderungen an Software
(IEC 61508-3:1998 + 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

Foreword

The text of the International Standard IEC 61508-3:1998 including its corrigendum April 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 61508-3 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, annexes A, B and ZA are normative and annex C is 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 61508-3:1998 including its corrigendum April 1999 was approved by CENELEC as a European Standard without any modification.

____

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 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 61508-2	2000	Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems	EN 61508-2	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
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	-	-

CONTENTS

Page

Clause

Tables

Table Page

Figures

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

Part 3: Software requirements

1 Scope

1.1 This part of IEC 61508

a) is intended to be utilised only after a thorough understanding of IEC 61508-1 and IEC 61508-2;

b) applies to any software forming part of a safety-related system or used to develop a safety-related system within the scope of IEC 61508-1 and IEC 61508-2. Such software is termed safety-related software.

- Safety-related software includes operating systems, system software, software in communication networks, human-computer interface functions, support tools and firmware as well as application programs.
- Application programs include high level programs, low level programs and special purpose programs in limited variability languages (see 3.2.7 of IEC 61508-4).

c) requires that the software safety functions and software safety integrity levels are specified.

NOTE 1 – If this has already been done as part of the specification of the E/E/PE safety-related systems (see 7.2 of IEC 61508-2), then it does not have to be repeated in this part.

NOTE 2 – Specifying the software safety functions and software safety integrity levels is an iterative procedure; see figures 2 and 6.

NOTE 3 – See clause 5 and annex A of IEC 61508-1 for documentation structure. The documentation structure may take account of company procedures, and of the working practices of specific application sectors.

d) establishes requirements for safety lifecycle phases and activities which shall be applied during the design and development of the safety-related software (the software safety lifecycle model). These requirements include the application of measures and techniques, which are graded against the safety integrity level, for the avoidance of and control of faults and failures in the software.

e) provides requirements for information relating to the software safety validation to be passed to the organisation carrying out the E/E/PES integration.

f) provides requirements for the preparation of information and procedures concerning software needed by the user for the operation and maintenance of the E/E/PE safety-related system.

g) provides requirements to be met by the organisation carrying out modifications to safety-related software.

h) provides, in conjunction with IEC 61508-1 and IEC 61508-2, requirements for support tools such as development and design tools, language translators, testing and debugging tools, configuration management tools.

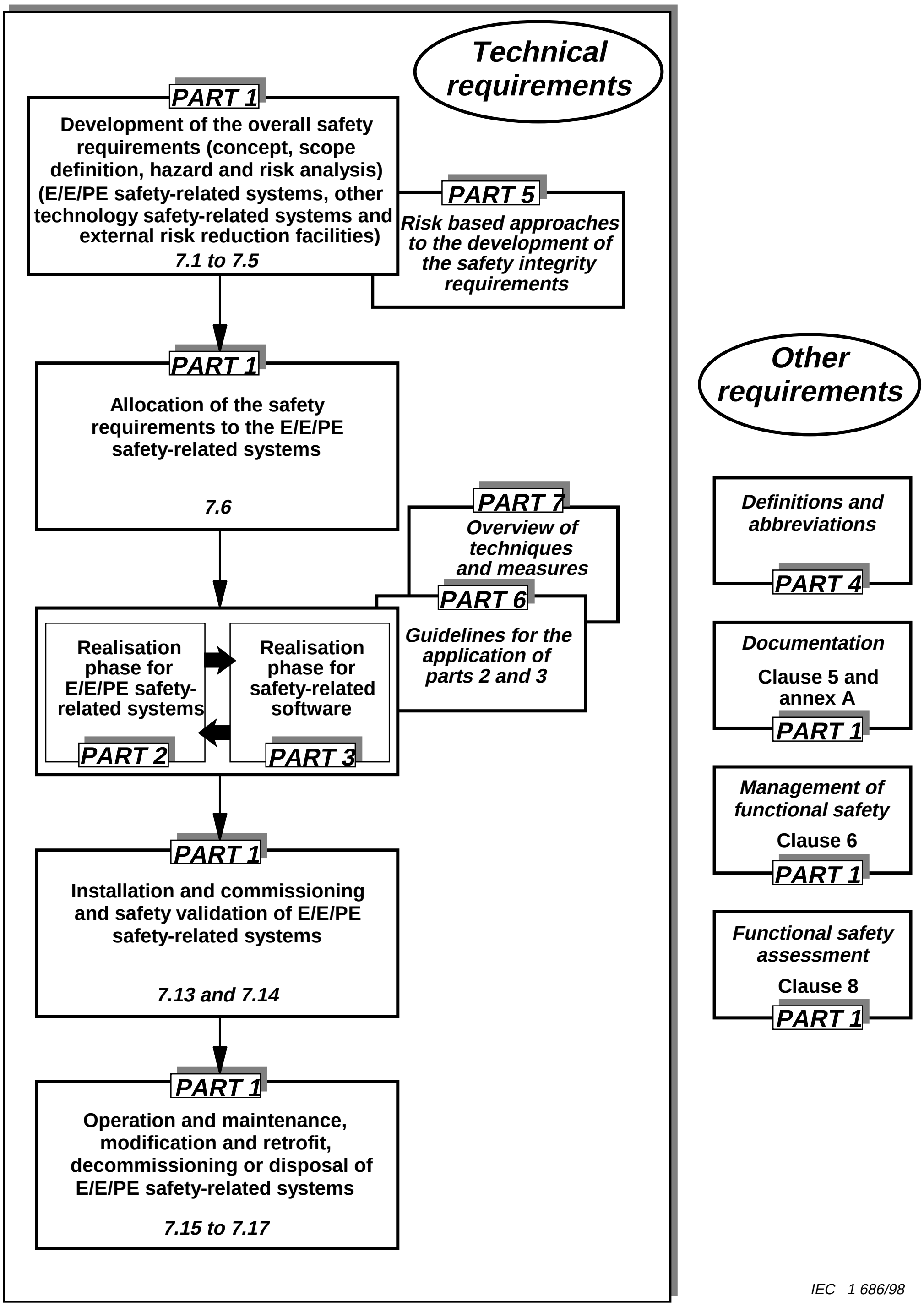
NOTE 4 – Figures 4 and 6 show the relationship between IEC 61508-2 and IEC 61508-3.

1.2 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 (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 S84.01-1996) can be applied to the process sector instead of IEC 61508.

1.3 Figure 1 shows the overall framework of parts 1 to 7 IEC 61508, and indicates the role that IEC 61508-3 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.


Technical requirements
PART 1
Development of the overall safety requirements (concept, scope definition, hazard and risk analysis) (E/E/PE safety-related systems, other technology safety-related systems and external risk reduction facilities)
7.1 to 7.5
PART 5
Risk based approaches to the development of the safety integrity requirements
PART 1
Allocation of the safety requirements to the E/E/PE safety-related systems
7.6
PART 7
Overview of techniques and measures
PART 6
Guidelines for the application of parts 2 and 3
Realisation phase for E/E/PE safety-related systems
PART 2
Realisation phase for safety-related software
PART 3
PART 1
Installation and commissioning and safety validation of E/E/PE safety-related systems
7.13 and 7.14
PART 1
Operation and maintenance, modification and retrofit, decommissioning or disposal of E/E/PE safety-related systems
7.15 to 7.17
Other requirements
Definitions and abbreviations
PART 4
Documentation
Clause 5 and annex A
PART 1
Management of functional safety
Clause 6
PART 1
Functional safety assessment
Clause 8
PART 1

IEC 1 686/98

Figure 1 – Overall framework of this standard