

© Copyright SEK. Reproduction in any form without permission is prohibited.

## **Säkerhetsfordringar på elektriska, elektroniska och programmerbara elektroniska säkerhetskritiska systems funktion – Del 4: Definitioner och förkortningar**

*Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 4: Definitions and abbreviations*

Som svensk standard gäller europastandarden EN 61508-4:2010. Den svenska standarden innehåller den officiella engelska språkversionen av EN 61508-4:2010.

### **Nationellt förord**

Europastandarden EN 61508-4:2010

består av:

- **europastandardens ikraftsättningsdokument**, utarbetat inom CENELEC
- **IEC 61508-4, Second edition, 2010 - Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 4: Definitions and abbreviations**

utarbetad inom International Electrotechnical Commission, IEC.

Tidigare fastställd svensk standard SS-EN 61508-4, utgåva 1, 2002, gäller ej fr o m 2013-05-01.

### *Standarder underlättar utvecklingen och höjer elsäkerheten*

Det finns många fördelar med att ha gemensamma tekniska regler för bl a säkerhet, prestanda, dokumentation, utförande och skötsel av elprodukter, elanläggningar och metoder. Genom att utforma sådana standarder blir säkerhetskraven tydliga och utvecklingskostnaderna rimliga samtidigt som marknadens acceptans för produkten eller tjänsten ökar.

Många standarder inom elområdet beskriver tekniska lösningar och metoder som åstadkommer den elsäkerhet som föreskrivs av svenska myndigheter och av EU.

### *SEK är Sveriges röst i standardiseringsarbetet inom elområdet*

SEK Svensk Elstandard svarar för standardiseringen inom elområdet i Sverige och samordnar svensk medverkan i internationell och europeisk standardisering. SEK är en ideell organisation med frivilligt deltagande från svenska myndigheter, företag och organisationer som vill medverka till och påverka utformningen av tekniska regler inom elektrotekniken.

SEK samordnar svenska intressenters medverkan i SEKs tekniska kommittéer och stödjer svenska experters medverkan i internationella och europeiska projekt.

### *Stora delar av arbetet sker internationellt*

Utformningen av standarder sker i allt väsentligt i internationellt och europeiskt samarbete. SEK är svensk nationalkommitté av International Electrotechnical Commission (IEC) och Comité Européen de Normalisation Electrotechnique (CENELEC).

Standardiseringsarbetet inom SEK är organiserat i referensgrupper bestående av ett antal tekniska kommittéer som speglar hur arbetet inom IEC och CENELEC är organiserat.

Arbetet i de tekniska kommittéerna är öppet för alla svenska organisationer, företag, institutioner, myndigheter och statliga verk. Den årliga avgiften för deltagandet och intäkter från försäljning finansierar SEKs standardiseringsverksamhet och medlemsavgift till IEC och CENELEC.

### *Var med och påverka!*

Den som deltar i SEKs tekniska kommittéarbete har möjlighet att påverka framtida standarder och får tidig tillgång till information och dokumentation om utvecklingen inom sitt teknikområde. Arbetet och kontakterna med kollegor, kunder och konkurrenter kan gynnsamt påverka enskilda företags affärsutveckling och bidrar till deltagarnas egen kompetensutveckling.

Du som vill dra nytta av dessa möjligheter är välkommen att kontakta SEKs kansli för mer information.

### **SEK Svensk Elstandard**

Box 1284  
164 29 Kista  
Tel 08-444 14 00  
[www.elstandard.se](http://www.elstandard.se)

**Functional safety of electrical/electronic/programmable electronic safety-related systems -  
Part 4: Definitions and abbreviations  
(IEC 61508-4:2010)**

Sécurité fonctionnelle des systèmes  
électriques/électroniques/électroniques  
programmables relatifs à la sécurité -  
Partie 4: Définitions et abréviations  
(CEI 61508-4:2010)

Funktionale Sicherheit sicherheitsbezogener  
elektrischer/elektronischer/programmierbarer  
elektronischer Systeme -  
Teil 4: Begriffe und Abkürzungen  
(IEC 61508-4:2010)

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**

## Foreword

The text of document 65A/551/FDIS, future edition 2 of IEC 61508-4, 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 61508-4 on 2010-05-01.

This European Standard supersedes EN 61508-4:2001.

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.

---

## Endorsement notice

The text of the International Standard IEC 61508-4:2010 was approved by CENELEC as a European Standard without any modification.

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

[1] IEC 61511 series	NOTE Harmonized in EN 61511 series (not modified).
[2] IEC 62061:2005	NOTE Harmonized as EN 62061:2005 (not modified).
[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 61508-7:2010	NOTE Harmonized as EN 61508-7:2010 (not modified).
[8] IEC 61131-3:2003	NOTE Harmonized as EN 61131-3:2003 (not modified).
[10] ISO 8402:1994	NOTE Harmonized as EN ISO 8402:1995 (not modified).
[11] IEC 60601 series	NOTE Harmonized in EN 60601 series (partially modified).
[14] IEC 61508-1:2010	NOTE Harmonized as EN 61508-1:2010 (not modified).
[15] IEC 61508-2:2010	NOTE Harmonized as EN 61508-2:2010 (not modified).
[16] IEC 61508-3:2010	NOTE Harmonized as EN 61508-3:2010 (not modified).
[18] ISO 9000:2005	NOTE Harmonized as EN ISO 9000:2005 (not modified).

## **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.

<u>Publication</u>	<u>Year</u>	<u>Title</u>	<u>EN/HD</u>	<u>Year</u>
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	-	-

## CONTENTS

INTRODUCTION.....	5
1 Scope.....	7
2 Normative references.....	9
3 Definitions and abbreviations .....	9
3.1 Safety terms .....	10
3.2 Equipment and devices .....	12
3.3 Systems – general aspects .....	15
3.4 Systems – safety-related aspects.....	17
3.5 Safety functions and safety integrity .....	19
3.6 Fault, failure and error (see Figure 4).....	22
3.7 Lifecycle activities.....	27
3.8 Confirmation of safety measures.....	28
Bibliography .....	32
Index .....	33
Figure 1 – Overall framework of the IEC 61508 series .....	8
Figure 2 – Programmable electronic system .....	16
Figure 3 – Electrical/electronic/programmable electronic system (E/E/PE system) – structure and terminology .....	16
Figure 4 – Failure model .....	23
Table 1 – Abbreviations used in this standard.....	9

## 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.

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, through 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.

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



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

## **Part 4: Definitions and abbreviations**

### **1 Scope**

**1.1** This part of IEC 61508 contains the definitions and explanation of terms that are used in parts 1 to 7 of the IEC 61508 series of standards.

**1.2** The definitions are grouped under general headings so that related terms can be understood within the context of each other. However, it should be noted that these headings are not intended to add meaning to the definitions.

**1.3** 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 publications. The horizontal safety function of this international standard does not apply to medical equipment in compliance with the IEC 60601 series.

**1.4** 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.

**1.5** Figure 1 shows the overall framework of the IEC 61508 series and indicates the role that IEC 61508-4 plays in the achievement of functional safety for E/E/PE safety-related systems.

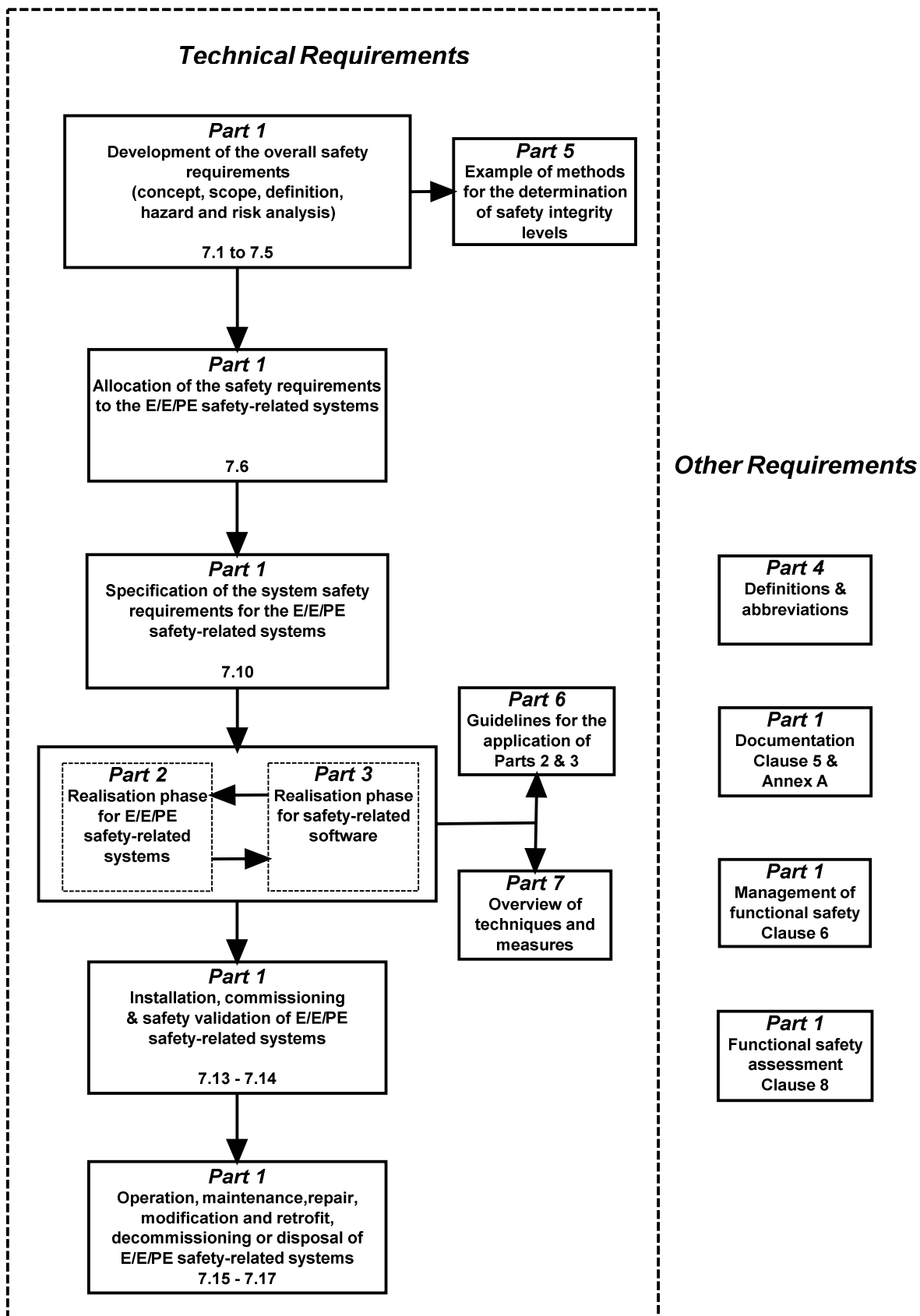


Figure 1 – Overall framework of the IEC 61508 series

## 2 Normative references

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.

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*