

This is a preview of "BS EN 61508-7:2010". [Click here to purchase the full version from the ANSI store.](#)

BS EN 61508-7:2010



BSI Standards Publication

Functional safety of electrical/ electronic/programmable electronic safety related systems

Part 7: Overview of techniques and measures

NO COPYING WITHOUT BSI PERMISSION EXCEPT AS PERMITTED BY COPYRIGHT LAW

raising standards worldwide™



This is a preview of "BS EN 61508-7:2010". [Click here to purchase the full version from the ANSI store.](#)

This British Standard is the UK implementation of EN 61508-7:2010. It is identical to IEC 61508-7:2010. It supersedes BS EN 61508-7:2002 which is withdrawn.

The UK participation in its preparation was entrusted by Technical Committee GEL/65, Measurement and control, to Subcommittee GEL/65/1, System considerations.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© BSI 2010

ISBN 978 0 580 65450 3

ICS 13.260; 25.040.40; 29.020

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 30 June 2010.

Amendments issued since publication

Amd. No.	Date	Text affected
-----------------	-------------	----------------------

This is a preview of "BS EN 61508-7:2010". [Click here to purchase the full version from the ANSI store.](#)

NORME EUROPÉENNE
EUROPÄISCHE NORM

May 2010

ICS 25.040.40; 35.240.50

Supersedes EN 61508-7:2001

English version

**Functional safety of electrical/electronic/programmable electronic safety-related systems -
Part 7: Overview of techniques and measures
(IEC 61508-7:2010)**

Sécurité fonctionnelle des systèmes
électriques/électroniques/électroniques
programmables relatifs à la sécurité -
Partie 7: Présentation de techniques
et mesures
(CEI 61508-7:2010)

Funktionale Sicherheit sicherheitsbezogener
elektrischer/elektronischer/programmierbarer
elektronischer Systeme -
Teil 7: Überblick über Verfahren
und Maßnahmen
(IEC 61508-7:2010)

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

This is a preview of "BS EN 61508-7:2010". [Click here to purchase the full version from the ANSI store.](#)

Foreword

The text of document 65A/554/FDIS, future edition 2 of IEC 61508-7, 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 61508-7 on 2010-05-01.

This European Standard supersedes EN 61508-7:2001.

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 61508-7:2010 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 60068-1:1988 | NOTE | Harmonized as EN 60068-1:1994 (not modified). |
| [2] IEC 60529:1989 | NOTE | Harmonized as EN 60529:1991 (not modified). |
| [3] IEC 60812:2006 | NOTE | Harmonized as EN 60812:2006 (not modified). |
| [4] IEC 60880:2006 | NOTE | Harmonized as EN 60880:2009 (not modified). |
| [5] IEC 61000-4-1:2006 | NOTE | Harmonized as EN 61000-4-1:2007 (not modified). |
| [6] IEC 61000-4-5:2005 | NOTE | Harmonized as EN 61000-4-5:2006 (not modified). |
| [8] IEC 61025:2006 | NOTE | Harmonized as EN 61025:2007 (not modified). |
| [9] IEC 61069-5:1994 | NOTE | Harmonized as EN 61069-5:1995 (not modified). |
| [10] IEC 61078:2006 | NOTE | Harmonized as EN 61078:2006 (not modified). |
| [11] IEC 61131-3:2003 | NOTE | Harmonized as EN 61131-3:2003 (not modified). |
| [12] IEC 61160:2005 | NOTE | Harmonized as EN 61160:2005 (not modified). |
| [13] IEC 61163-1:2006 | NOTE | Harmonized as EN 61163-1:2006 (not modified). |
| [14] IEC 61164:2004 | NOTE | Harmonized as EN 61164:2004 (not modified). |
| [15] IEC 61165:2006 | NOTE | Harmonized as EN 61165:2006 (not modified). |
| [16] IEC 61326-3-1:2008 | NOTE | Harmonized as EN 61326-3-1:2008 (not modified). |
| [17] IEC 61326-3-2:2008 | NOTE | Harmonized as EN 61326-3-2:2008 (not modified). |
| [18] IEC 81346-1:2009 | NOTE | Harmonized as EN 81346-1:2009 (not modified). |

This is a preview of "BS EN 61508-7:2010". [Click here to purchase the full version from the ANSI store.](#)

[22] IEC 62061:2005	NOTE	Harmonized as EN 62061:2005 (not modified).
[23] IEC 62308:2006	NOTE	Harmonized as EN 62308:2006 (not modified).
[37] IEC 61800-5-2	NOTE	Harmonized as EN 61800-5-2.
[38] IEC 60601 series	NOTE	Harmonized in EN 60601 series (partially modified).
[39] IEC 60068-2-1	NOTE	Harmonized as EN 60068-2-1.
[40] IEC 60068-2-2	NOTE	Harmonized as EN 60068-2-2.
[41] ISO 9000	NOTE	Harmonized as EN ISO 9000.
[42] IEC 61508-1:2010	NOTE	Harmonized as EN 61508-1:2010 (not modified).
[43] IEC 61508-2:2010	NOTE	Harmonized as EN 61508-2:2010 (not modified).
[44] IEC 61508-3:2010	NOTE	Harmonized as EN 61508-3:2010 (not modified).
[45] IEC 61508-6:2010	NOTE	Harmonized as EN 61508-6:2010 (not modified).

This is a preview of "BS EN 61508-7:2010". [Click here to purchase the full version from the ANSI store.](#)

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 61508-4	2010	Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 4: Definitions and abbreviations	EN 61508-4	2010

This is a preview of "BS EN 61508-7:2010". [Click here to purchase the full version from the ANSI store.](#)

CONTENTS

INTRODUCTION.....	5
1 Scope.....	7
2 Normative references	9
3 Definitions and abbreviations.....	9
Annex A (informative) Overview of techniques and measures for E/E/PE safety-related systems: control of random hardware failures (see IEC 61508-2).....	10
Annex B (informative) Overview of techniques and measures for E/E/PE safety related systems: avoidance of systematic failures (see IEC 61508-2 and IEC 61508-3).....	27
Annex C (informative) Overview of techniques and measures for achieving software safety integrity (see IEC 61508-3).....	54
Annex D (informative) A probabilistic approach to determining software safety integrity for pre-developed software	107
Annex E (informative) Overview of techniques and measures for design of ASICs	112
Annex F (informative) Definitions of properties of software lifecycle phases.....	126
Annex G (informative) Guidance for the development of safety-related object oriented software.....	132
Bibliography.....	134
Index	137
Figure 1 – Overall framework of IEC 61508.....	8
Table C.1 – Recommendations for specific programming languages	86
Table D.1 – Necessary history for confidence to safety integrity levels	107
Table D.2 – Probabilities of failure for low demand mode of operation	108
Table D.3 – Mean distances of two test points	109
Table D.4 – Probabilities of failure for high demand or continuous mode of operation.....	110
Table D.5 – Probability of testing all program properties	111
Table F.1 – Software Safety Requirements Specification	126
Table F.2 – Software design and development: software architecture design	127
Table F.3 – Software design and development: support tools and programming language.....	128
Table F.4 – Software design and development: detailed design	128
Table F.5 – Software design and development: software module testing and integration.....	129
Table F.6 – Programmable electronics integration (hardware and software).....	129
Table F.7 – Software aspects of system safety validation	130
Table F.8 – Software modification.....	130
Table F.9 – Software verification.....	131
Table F.10 – Functional safety assessment	131
Table G.1 – Object Oriented Software Architecture.....	132
Table G.2 – Object Oriented Detailed Design.....	133
Table G.3 – Some Oriented Detailed terms.....	133