

# INTERNATIONAL STANDARD

# NORME INTERNATIONALE

BASIC SAFETY PUBLICATION

PUBLICATION FONDAMENTALE DE SÉCURITÉ

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

**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**



## THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2000 IEC, Geneva, Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester.

If you have any questions about IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

Droits de reproduction réservés. Sauf indication contraire, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et les microfilms, sans l'accord écrit de la CEI ou du Comité national de la CEI du pays du demandeur.

Si vous avez des questions sur le copyright de la CEI ou si vous désirez obtenir des droits supplémentaires sur cette publication, utilisez les coordonnées ci-après ou contactez le Comité national de la CEI de votre pays de résidence.

IEC Central Office  
3, rue de Varembe  
CH-1211 Geneva 20  
Switzerland  
Email: [inmail@iec.ch](mailto:inmail@iec.ch)  
Web: [www.iec.ch](http://www.iec.ch)

### About the IEC

The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

### About IEC publications

The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigenda or an amendment might have been published.

- Catalogue of IEC publications: [www.iec.ch/searchpub](http://www.iec.ch/searchpub)

The IEC on-line Catalogue enables you to search by a variety of criteria (reference number, text, technical committee,...). It also gives information on projects, withdrawn and replaced publications.

- IEC Just Published: [www.iec.ch/online\\_news/justpub](http://www.iec.ch/online_news/justpub)

Stay up to date on all new IEC publications. Just Published details twice a month all new publications released. Available on-line and also by email.

- Electropedia: [www.electropedia.org](http://www.electropedia.org)

The world's leading online dictionary of electronic and electrical terms containing more than 20 000 terms and definitions in English and French, with equivalent terms in additional languages. Also known as the International Electrotechnical Vocabulary online.

- Customer Service Centre: [www.iec.ch/webstore/custserv](http://www.iec.ch/webstore/custserv)

If you wish to give us your feedback on this publication or need further assistance, please visit the Customer Service Centre FAQ or contact us:

Email: [csc@iec.ch](mailto:csc@iec.ch)

Tel.: +41 22 919 02 11

Fax: +41 22 919 03 00

### A propos de la CEI

La Commission Electrotechnique internationale (CEI) est la première organisation mondiale qui élabore et publie des normes internationales pour tout ce qui a trait à l'électricité, à l'électronique et aux technologies apparentées.

### A propos des publications CEI

Le contenu technique des publications de la CEI est constamment revu. Veuillez vous assurer que vous possédez l'édition la plus récente, un corrigendum ou amendement peut avoir été publié.

- Catalogue des publications de la CEI: [www.iec.ch/searchpub/cur\\_fut-f.htm](http://www.iec.ch/searchpub/cur_fut-f.htm)

Le Catalogue en-ligne de la CEI vous permet d'effectuer des recherches en utilisant différents critères (numéro de référence, texte, comité d'études,...). Il donne aussi des informations sur les projets et les publications retirées ou remplacées.

- Just Published CEI: [www.iec.ch/online\\_news/justpub](http://www.iec.ch/online_news/justpub)

Restez informé sur les nouvelles publications de la CEI. Just Published détaille deux fois par mois les nouvelles publications parues. Disponible en-ligne et aussi par email.

- Electropedia: [www.electropedia.org](http://www.electropedia.org)

Le premier dictionnaire en ligne au monde de termes électroniques et électriques. Il contient plus de 20 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans les langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International en ligne.

- Service Clients: [www.iec.ch/webstore/custserv/custserv\\_entry-f.htm](http://www.iec.ch/webstore/custserv/custserv_entry-f.htm)

Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions, visitez le FAQ du Service clients ou contactez-nous:

Email: [csc@iec.ch](mailto:csc@iec.ch)

Tél.: +41 22 919 02 11

Fax: +41 22 919 03 00

# INTERNATIONAL STANDARD

# NORME INTERNATIONALE

BASIC SAFETY PUBLICATION  
PUBLICATION FONDAMENTALE DE SÉCURITÉ

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

**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**

INTERNATIONAL  
ELECTROTECHNICAL  
COMMISSION

COMMISSION  
ELECTROTECHNIQUE  
INTERNATIONALE

PRICE CODE  
CODE PRIX

**XB**

## CONTENTS

	Page
FOREWORD .....	4
INTRODUCTION .....	6
Clause	
1 Scope .....	8
2 Normative references .....	11
3 Definitions and abbreviations .....	12
4 Conformance to this standard .....	12
5 Documentation .....	12
6 Management of functional safety .....	12
7 E/E/PES safety lifecycle requirements .....	12
7.1 General .....	12
7.2 E/E/PES safety requirements specification .....	16
7.3 E/E/PES safety validation planning .....	18
7.4 E/E/PES design and development .....	19
7.5 E/E/PES integration .....	36
7.6 E/E/PES operation and maintenance procedures .....	37
7.7 E/E/PES safety validation .....	39
7.8 E/E/PES modification .....	40
7.9 E/E/PES verification .....	40
8 Functional safety assessment .....	42
Annex A (normative) Techniques and measures for E/E/PE safety-related systems: control of failures during operation .....	43
A.1 General .....	43
A.2 Hardware safety integrity .....	44
A.3 Systematic safety integrity .....	53
Annex B (normative) Techniques and measures for E/E/PE safety-related systems: avoidance of systematic failures during the different phases of the lifecycle .....	59
Annex C (normative) Diagnostic coverage and safe failure fraction .....	69
C.1 Calculation of diagnostic coverage and safe failure fraction of a subsystem .....	69
C.2 Determination of diagnostic coverage factors .....	70
Bibliography .....	72

	Page
Figure 1 – Overall framework of IEC 61508 .....	1 0
Figure 2 – E/E/PES safety lifecycle (in realisation phase).....	1 3
Figure 3 – Relationship and scope for IEC 61508-2 and IEC 61508-3.....	1 4
Figure 4 – Relationship between the hardware and software architectures of programmable electronics .....	2 0
Figure 5 – Example limitation on hardware safety integrity for a single-channel safety function.....	2 5
Figure 6 – Example limitation on hardware safety integrity for a multiple-channel safety function.....	2 7
Table 1 – Overview – Realisation phase of the E/E/PES safety lifecycle.....	1 5
Table 2 – Hardware safety integrity: architectural constraints on type A safety-related subsystems .....	2 4
Table 3 – Hardware safety integrity: architectural constraints on type B safety-related subsystems .....	2 4
Table A.1 – Faults or failures to be detected during operation or to be analysed in the derivation of safe failure fraction.....	4 5
Table A.2 – Electrical subsystems .....	4 6
Table A.3 – Electronic subsystems .....	4 7
Table A.4 – Processing units .....	4 7
Table A.5 – Invariable memory ranges .....	4 8
Table A.6 – Variable memory ranges.....	4 8
Table A.7 – I/O units and interface (external communication).....	4 9
Table A.8 – Data paths (internal communication) .....	4 9
Table A.9 – Power supply.....	5 0
Table A.10 – Program sequence (watch-dog).....	5 0
Table A.11 – Ventilation and heating system (if necessary) .....	5 1
Table A.12 – Clock.....	5 1
Table A.13 – Communication and mass-storage .....	5 2
Table A.14 – Sensors.....	5 2
Table A.15 – Final elements (actuators).....	5 3
Table A.16 – Techniques and measures to control systematic failures caused by hardware and software design.....	5 5
Table A.17 – Techniques and measures to control systematic failures caused by environmental stress or influences .....	5 6
Table A.18 – Techniques and measures to control systematic operational failures .....	5 7
Table A.19 – Effectiveness of techniques and measures to control systematic failures.....	5 8
Table B.1 – Recommendations to avoid mistakes during specification of E/E/PES requirements (see 7.2) .....	6 1
Table B.2 – Recommendations to avoid introducing faults during E/E/PES design and development (see 7.4).....	6 2
Table B.3 – Recommendations to avoid faults during E/E/PES integration (see 7.5).....	6 3
Table B.4 – Recommendations to avoid faults and failures during E/E/PES operation and maintenance procedures (see 7.6).....	6 4
Table B.5 – Recommendations to avoid faults during E/E/PES safety validation (see 7.7) .....	6 5
Table B.6 – Effectiveness of techniques and measures to avoid systematic failures .....	6 6

INTERNATIONAL ELECTROTECHNICAL COMMISSION

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

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

FOREWORD

- 1) The IEC (International Electrotechnical Commission) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of the IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, the IEC publishes International Standards. Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. The IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
- 2) The formal decisions or agreements of the IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested National Committees.
- 3) The documents produced have the form of recommendations for international use and are published in the form of standards, technical specifications, technical reports or guides and they are accepted by the National Committees in that sense.
- 4) In order to promote international unification, IEC National Committees undertake to apply IEC International Standards transparently to the maximum extent possible in their national and regional standards. Any divergence between the IEC Standard and the corresponding national or regional standard shall be clearly indicated in the latter.
- 5) The IEC provides no marking procedure to indicate its approval and cannot be rendered responsible for any equipment declared to be in conformity with one of its standards.
- 6) Attention is drawn to the possibility that some of the elements of this International Standard may be the subject of patent rights. The IEC shall not be held responsible for identifying any or all such patent rights.

International Standard IEC 61508-2 has been prepared by subcommittee 65A: System aspects, of IEC technical committee 65: Industrial-process measurement and control.

It has the status of a basic safety publication according to IEC Guide 104.

The text of this standard is based on the following documents:

FDIS	Report on voting
65A/294/FDIS	65A/303/RVD

Full information on the voting for the approval of this standard can be found in the report on voting indicated in the above table.

This publication has been drafted in accordance with the ISO/IEC Directives, Part 3.

Annexes A, B, and C form an integral part of this standard.

IEC 61508 consists of the following parts, under the general title *Functional safety of electrical/electronic/programmable electronic safety-related systems*:

- Part 1: General requirements
- Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems
- Part 3: Software requirements
- Part 4: Definitions and abbreviations
- Part 5: Examples of methods for the determination of safety integrity levels
- Part 6: Guidelines on the application of parts 2 and 3
- Part 7: Overview of techniques and measures

The committee has decided that the contents of this publication will remain unchanged until 2006. At this date, the publication will be

- reconfirmed;
- withdrawn;
- replaced by a revised edition, or
- amended.

iTech Standards  
(<https://standards.itih.ai>)  
Document Preview

IEC 61508-2:2000

<https://standards.itih.ai/standards/iec/61508-2-2000>

## INTRODUCTION

Systems comprised of electrical and/or electronic components have been used for many years to perform safety functions in most application sectors. Computer-based systems (generically referred to as programmable electronic systems (PESs)) 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 those 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 components (electrical/electronic/programmable electronic systems (E/E/PESs)) 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 application sector standards.

In most situations, safety is achieved by a number of protective systems which may 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 electrical/electronic/programmable electronic (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 recognised that there is a great variety of E/E/PES applications 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 application sector International Standards.

This International Standard

- considers all relevant overall, E/E/PES and software safety lifecycle phases (for example, from initial concept, through design, implementation, operation and maintenance to decommissioning) when E/E/PESs 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 application sector International Standards, dealing with safety-related E/E/PESs, to be developed; the development of application sector International Standards, within the framework of this International 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;
- uses 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;



- adopts a risk-based approach for the determination of the safety integrity level requirements;
- sets numerical target failure measures for E/E/PE safety-related systems which are linked to the safety integrity levels;
- sets a lower limit on the target failure measures, in a dangerous mode of failure, that can be claimed for 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 failure of  $10^{-5}$  to perform its design function on demand,
  - a high demand or continuous mode of operation, the lower limit is set at a probability of a dangerous failure of  $10^{-9}$  per hour;

NOTE A single E/E/PE safety-related system does not necessarily mean a single-channel architecture.

- adopts a broad range of principles, techniques and measures to achieve functional safety for E/E/PE safety-related systems, but does not rely on the concept of fail safe which may be of value when the failure modes are well defined and the level of complexity is relatively low. The concept of fail safe was considered inappropriate because of the full range of complexity of E/E/PE safety-related systems that are within the scope of the standard.

WITHDRAWN

iTeh Standards  
(<https://standards.iteh.ai>)  
Document Preview

IEC 61508-2:2000

<https://standards.iteh.ai/catalog/standards/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

### 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.

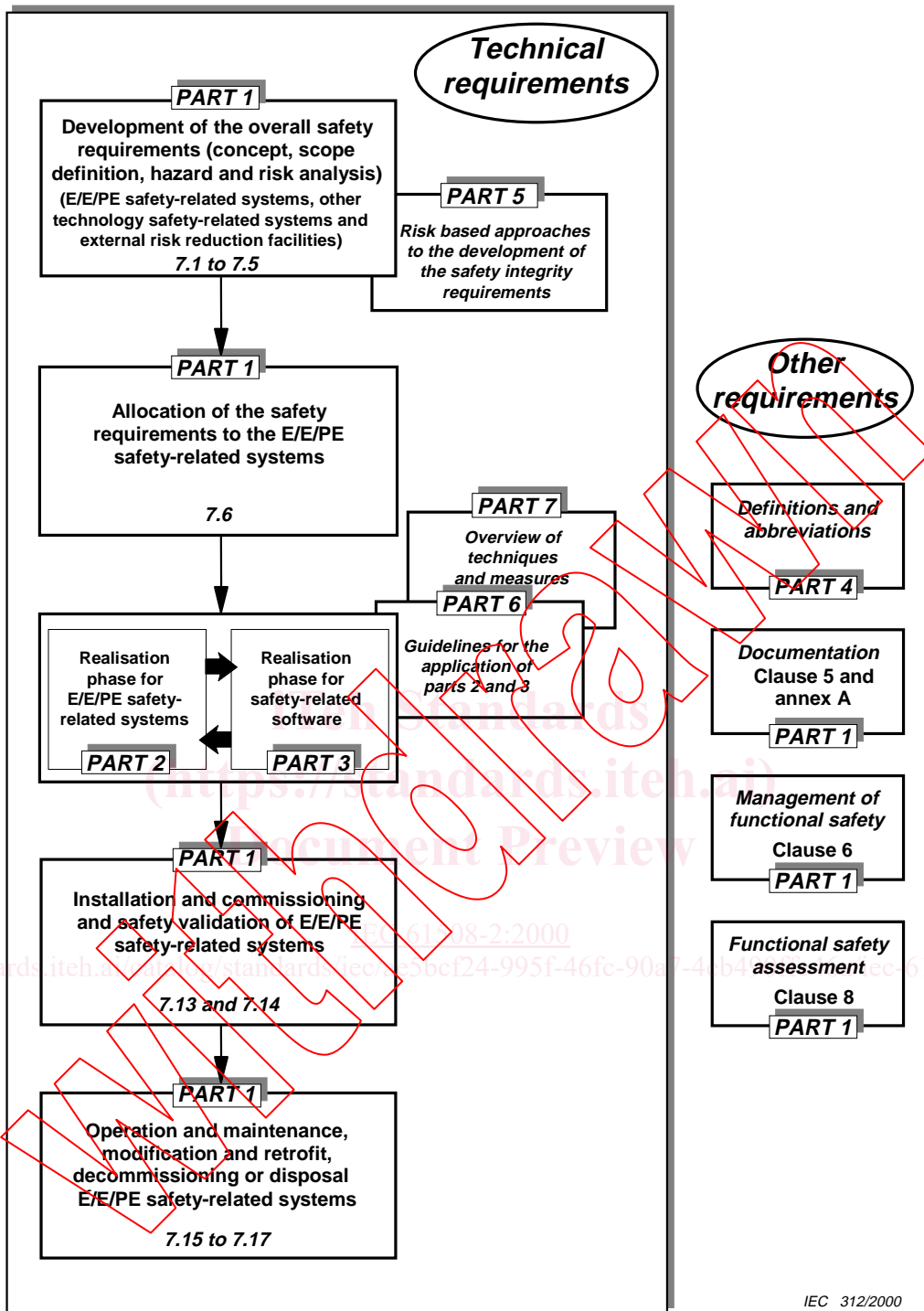
NOTE 2 In the USA and Canada, until the proposed sector implementation of IEC 61508 (i.e. IEC 61511) is published as an international standard in the USA and Canada, existing national process safety standards based on IEC 61508 (i.e. ANSI/ISA-S84.01) can be applied to the process sector instead of IEC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

iTech Standards  
(<https://standards.itih.ai>)  
Document Preview

IEC 61508-2:2000

<https://standards.itih.ai/standards/iec/61508-2-2000>



IEC 312/2000

Figure 1 – Overall framework of IEC 61508

## 2 Normative references

The following normative documents contain provisions which, through reference in this text, constitute provisions of this part of IEC 61508. For dated references, subsequent amendments to, or revisions of, any of these publications do not apply. However, parties to agreements based on this part of IEC 61508 are encouraged to investigate the possibility of applying the most recent editions of the normative documents indicated below. For undated references, the latest edition of the normative document referred to applies. Members of IEC and ISO maintain registers of currently valid International Standards.

IEC 60050(371):1984, *International Electrotechnical Vocabulary – 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, *Electromagnetic compatibility (EMC) – Part 2: Environment – Section 5: Classification of electromagnetic environments – Basic EMC publication*

IEC 61508-1:1998, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements*

IEC 61508-3:1998, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 3: Software requirements*

IEC 61508-4:1998, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 4: Definitions and abbreviations*

IEC 61508-5:1998, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 5: Examples of methods for the determination of safety integrity levels*

IEC 61508-6, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 6: Guidelines on the application of parts 2 and 3<sup>1)</sup>*

IEC 61508-7:2000, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 7: Overview of techniques and measures*

IEC Guide 104:1997, *The preparation of safety publications and the use of basic safety publications and group safety publications*

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*

---

1) To be published.

### 3 Definitions and abbreviations

For the purposes of this part of IEC 61508, the definitions and abbreviations given in IEC 61508-4 apply.

### 4 Conformance to this standard

The requirements for conformance to this standard are as detailed in clause 4 of IEC 61508-1.

### 5 Documentation

The requirements for documentation are as detailed in clause 5 of IEC 61508-1.

### 6 Management of functional safety

The requirements for management of functional safety are as detailed in clause 6 of IEC 61508-1.

### 7 E/E/PES safety lifecycle requirements

#### 7.1 General

##### 7.1.1 Objectives and requirements: General

7.1.1.1 This subclause sets out the objectives and requirements for the E/E/PES safety lifecycle phases.

NOTE The objectives and requirements for the overall safety lifecycle, together with a general introduction to the structure of the standard, are given in IEC 61508-1.

7.1.1.2 For all phases of the E/E/PES safety lifecycle, table 1 indicates

- the objectives to be achieved;
- the scope of the phase;
- a reference to the subclause containing the requirements;
- the required inputs to the phase;
- the outputs required to comply with the subclause.

##### 7.1.2 Objectives

7.1.2.1 The first objective of the requirements of this subclause is to structure, in a systematic manner, the phases in the E/E/PES safety lifecycle that shall be considered in order to achieve the required functional safety of the E/E/PE safety-related systems.

7.1.2.2 The second objective of the requirements of this subclause is to document all information relevant to the functional safety of the E/E/PE safety-related systems throughout the E/E/PES safety lifecycle.