

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: Exigences pour les systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité



THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2010 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
Web: 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

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 It also gives information on projects, withdrawn and replaced publications.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

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

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

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
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

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

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

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

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
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: Exigences pour les systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

PRICE CODE
CODE PRIX

XD

ICS 25.040.40

ISBN 978-2-88910-525-0

CONTENTS

FOREWORD.....	5
INTRODUCTION.....	7
1 Scope.....	9
2 Normative references	12
3 Definitions and abbreviations.....	12
4 Conformance to this standard	12
5 Documentation	13
6 Management of functional safety	13
7 E/E/PE system safety lifecycle requirements	13
7.1 General.....	13
7.1.1 Objectives and requirements – general.....	13
7.1.2 Objectives	13
7.1.3 Requirements	13
7.2 E/E/PE system design requirements specification	17
7.2.1 Objective	17
7.2.2 General	17
7.2.3 E/E/PE system design requirements specification.....	18
7.3 E/E/PE system safety validation planning	19
7.3.1 Objective	19
7.3.2 Requirements	19
7.4 E/E/PE system design and development.....	19
7.4.1 Objective	20
7.4.2 General requirements	20
7.4.3 Synthesis of elements to achieve the required systematic capability.....	22
7.4.4 Hardware safety integrity architectural constraints.....	23
7.4.5 Requirements for quantifying the effect of random hardware failures	32
7.4.6 Requirements for the avoidance of systematic faults	34
7.4.7 Requirements for the control of systematic faults.....	35
7.4.8 Requirements for system behaviour on detection of a fault	35
7.4.9 Requirements for E/E/PE system implementation	36
7.4.10 Requirements for proven in use elements.....	38
7.4.11 Additional requirements for data communications	39
7.5 E/E/PE system integration	40
7.5.1 Objective	40
7.5.2 Requirements	40
7.6 E/E/PE system operation and maintenance procedures	41
7.6.1 Objective	41
7.6.2 Requirements	41
7.7 E/E/PE system safety validation	42
7.7.1 Objective	42
7.7.2 Requirements	42
7.8 E/E/PE system modification.....	43
7.8.1 Objective	43
7.8.2 Requirements	43
7.9 E/E/PE system verification	44
7.9.1 Objective	44

7.9.2 Requirements	44
8 Functional safety assessment.....	46
Annex A (normative) Techniques and measures for E/E/PE safety-related systems – control of failures during operation.....	47
Annex B (normative) Techniques and measures for E/E/PE safety-related systems – avoidance of systematic failures during the different phases of the lifecycle	62
Annex C (normative) Diagnostic coverage and safe failure fraction.....	71
Annex D (normative) Safety manual for compliant items	74
Annex E (normative) Special architecture requirements for integrated circuits (ICs) with on-chip redundancy	76
Annex F (informative) Techniques and measures for ASICs – avoidance of systematic failures	81
Bibliography.....	89
Figure 1 – Overall framework of the IEC 61508 series	11
Figure 2 – E/E/PE system safety lifecycle (in realisation phase).....	14
Figure 3 – ASIC development lifecycle (the V-Model).....	15
Figure 4 – Relationship between and scope of IEC 61508-2 and IEC 61508-3	15
Figure 5 – Determination of the maximum SIL for specified architecture (E/E/PE safety-related subsystem comprising a number of series elements, see 7.4.4.2.3)	28
Figure 6 – Determination of the maximum SIL for specified architecture (E/E/PE safety-related subsystem comprised of two subsystems X & Y, see 7.4.4.2.4).....	30
Figure 7 – Architectures for data communication.....	40
Table 1 – Overview – realisation phase of the E/E/PE system safety lifecycle.....	16
Table 2 – Maximum allowable safety integrity level for a safety function carried out by a type A safety-related element or subsystem.....	26
Table 3 – Maximum allowable safety integrity level for a safety function carried out by a type B safety-related element or subsystem.....	27
Table A.1 – Faults or failures to be assumed when quantifying the effect of random hardware failures or to be taken into account in the derivation of safe failure fraction	49
Table A.2 – Electrical components	51
Table A.3 – Electronic components	51
Table A.4 – Processing units	52
Table A.5 – Invariable memory ranges	52
Table A.6 – Variable memory ranges	53
Table A.7 – I/O units and interface (external communication).....	53
Table A.8 – Data paths (internal communication)	54
Table A.9 – Power supply	54
Table A.10 – Program sequence (watch-dog).....	55
Table A.11 – Clock	55
Table A.12 – Communication and mass-storage	55
Table A.13 – Sensors	56
Table A.14 – Final elements (actuators).....	56
Table A.15 – Techniques and measures to control systematic failures caused by hardware design	58

Table A.16 – Techniques and measures to control systematic failures caused by environmental stress or influences	59
Table A.17 – Techniques and measures to control systematic operational failures.....	60
Table A.18 – Effectiveness of techniques and measures to control systematic failures	61
Table B.1 – Techniques and measures to avoid mistakes during specification of E/E/PE system design requirements (see 7.2)	63
Table B.2 – Techniques and measures to avoid introducing faults during E/E/PE system design and development (see 7.4)	64
Table B.3 – Techniques and measures to avoid faults during E/E/PE system integration (see 7.5).....	65
Table B.4 – Techniques and measures to avoid faults and failures during E/E/PE system operation and maintenance procedures (see 7.6).....	66
Table B.5 – Techniques and measures to avoid faults during E/E/PE system safety validation (see 7.7)	67
Table B.6 – Effectiveness of techniques and measures to avoid systematic failures.....	68
Table E.1 – Techniques and measures that increase β_{B-IC}	79
Table E.2 – Techniques and measures that decrease β_{B-IC}	80
Table F.1 – Techniques and measures to avoid introducing faults during ASIC’s design and development – full and semi-custom digital ASICs (see 7.4.6.7).....	83
Table F.2 – Techniques and measures to avoid introducing faults during ASIC design and development: User programmable ICs (FPGA/PLD/CPLD) (see 7.4.6.7)	86

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 International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of 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, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as “IEC Publication(s)”). 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. 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 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 IEC National Committees.
- 3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
- 4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
- 5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
- 6) All users should ensure that they have the latest edition of this publication.
- 7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
- 8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
- 9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. 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, control and automation.

This second edition cancels and replaces the first edition published in 2000. This edition constitutes a technical revision.

This edition has been subject to a thorough review and incorporates many comments received at the various revision stages.

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/549/FDIS	65A/573/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 2

A list of all parts of the IEC 61508 series, published under the general title *Functional safety of electrical / electronic / programmable electronic safety-related systems*, can be found on the IEC website.

The committee has decided that the contents of this publication will remain unchanged until the maintenance result date indicated on the IEC web site under "<http://webstore.iec.ch>" in the data related to the specific publication. At this date, the publication will be

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

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

1 Scope

1.1 This part of the IEC 61508 series

- 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, that contains at least one electrical, electronic or programmable electronic element;
- c) applies to all elements within an E/E/PE safety-related system (including sensors, actuators and the operator interface);
- d) specifies how to refine the E/E/PE system safety requirements specification, developed in accordance with IEC 61508-1 (comprising the E/E/PE system safety functions requirements specification and the E/E/PE system safety integrity requirements specification), into the E/E/PE system design requirements specification;
- e) specifies the 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/PE system safety lifecycle model) except software, which is dealt with in IEC 61508-3 (see Figures 2 to 4). These requirements include the application of techniques and measures that 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 4.

- i) does not apply for medical equipment in compliance with the IEC 60601 series.

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

1.3 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 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.

1.4 Figure 1 shows the overall framework of the IEC 61508 series 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.