

INTERNATIONAL STANDARD

NORME INTERNATIONALE

BASIC SAFETY PUBLICATION

PUBLICATION FONDAMENTALE DE SÉCURITÉ

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

Part 1: General requirements

Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité

Partie 1: Exigences générales



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 It also gives information on projects, withdrawn and replaced publications.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/entry-f.htm

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 toute 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 1: General requirements

Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité

Partie 1: Exigences générales

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

PRICE CODE **XB**
CODE PRIX

ICS 13.110; 25.040; 29.020

ISBN 978-2-88910-524-3

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
5.1 Objectives.....	13
5.2 Requirements.....	13
6 Management of functional safety.....	14
6.1 Objectives.....	14
6.2 Requirements.....	14
7 Overall safety lifecycle requirements.....	17
7.1 General.....	17
7.1.1 Introduction.....	17
7.1.2 Objectives and requirements – general.....	20
7.1.3 Objectives.....	25
7.1.4 Requirements.....	25
7.2 Concept.....	25
7.2.1 Objective.....	25
7.2.2 Requirements.....	26
7.3 Overall scope definition.....	26
7.3.1 Objectives.....	26
7.3.2 Requirements.....	26
7.4 Hazard and risk analysis.....	27
7.4.1 Objectives.....	27
7.4.2 Requirements.....	27
7.5 Overall safety requirements.....	28
7.5.1 Objective.....	29
7.5.2 Requirements.....	29
7.6 Overall safety requirements allocation.....	30
7.6.1 Objectives.....	30
7.6.2 Requirements.....	31
7.7 Overall operation and maintenance planning.....	35
7.7.1 Objective.....	35
7.7.2 Requirements.....	35
7.8 Overall safety validation planning.....	37
7.8.1 Objective.....	37
7.8.2 Requirements.....	37
7.9 Overall installation and commissioning planning.....	38
7.9.1 Objectives.....	38
7.9.2 Requirements.....	38
7.10 E/E/PE system safety requirements specification.....	38
7.10.1 Objective.....	39
7.10.2 Requirements.....	39
7.11 E/E/PE safety-related systems – realisation.....	41

7.11.1 Objective	41
7.11.2 Requirements	41
7.12 Other risk reduction measures – specification and realisation.....	41
7.12.1 Objective	41
7.12.2 Requirements	41
7.13 Overall installation and commissioning.....	41
7.13.1 Objectives	41
7.13.2 Requirements	42
7.14 Overall safety validation.....	42
7.14.1 Objective	42
7.14.2 Requirements	42
7.15 Overall operation, maintenance and repair.....	43
7.15.1 Objective	43
7.15.2 Requirements	43
7.16 Overall modification and retrofit	46
7.16.1 Objective	46
7.16.2 Requirements	47
7.17 Decommissioning or disposal.....	48
7.17.1 Objective	48
7.17.2 Requirements	48
7.18 Verification	49
7.18.1 Objective	49
7.18.2 Requirements	49
8 Functional safety assessment	50
8.1 Objective	50
8.2 Requirements	50
Annex A (informative) Example of a documentation structure.....	54
Bibliography.....	60
Figure 1 – Overall framework of the IEC 61508 series	11
Figure 2 – Overall safety lifecycle	18
Figure 3 – E/E/PE system safety lifecycle (in realisation phase).....	19
Figure 4 – Software safety lifecycle (in realisation phase)	19
Figure 5 – Relationship of overall safety lifecycle to the E/E/PE system and software safety lifecycle	20
Figure 6 – Allocation of overall safety requirements to E/E/PE safety-related systems and other risk reduction measures.....	32
Figure 7 – Example of operations and maintenance activities model	45
Figure 8 – Example of operation and maintenance management model	46
Figure 9 – Example of modification procedure model	48
Figure A.1 – Structuring information into document sets for user groups	59
Table 1 – Overall safety lifecycle – overview.....	21
Table 2 – Safety integrity levels – target failure measures for a safety function operating in low demand mode of operation	33
Table 3 – Safety integrity levels – target failure measures for a safety function operating in high demand mode of operation or continuous mode of operation	34

Table 4 – Minimum levels of independence of those carrying out functional safety assessment (overall safety lifecycle phases 1 to 8 and 12 to 16 inclusive (see Figure 2)) 53

Table 5 – Minimum levels of independence of those carrying out functional safety assessment (overall safety lifecycle phases 9 and 10, including all phases of E/E/PE system and software safety lifecycles (see Figures 2, 3 and 4)) 53

Table A.1 – Example of a documentation structure for information related to the overall safety lifecycle 56

Table A.2 – Example of a documentation structure for information related to the E/E/PE system safety lifecycle..... 57

Table A.3 – Example of a documentation structure for information related to the software safety lifecycle 58

Currently in preview, click buy full version

INTERNATIONAL ELECTROTECHNICAL COMMISSION

**FUNCTIONAL SAFETY OF ELECTRICAL/ELECTRONIC/
PROGRAMMABLE ELECTRONIC SAFETY-RELATED SYSTEMS –****Part 1: General requirements**

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 far 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, accept 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 61508-1 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 1998. 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.