This is a preview - click here to buy the full publication

INTERNATIONAL STANDARD

IEC 61508-2

First edition
2000-05

BASIC SAFETY PUBLICATION

withdrawn

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

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

*This **English-language** version is derived from the original **bilingual** publication by leaving out all French-language pages. Missing page numbers correspond to the French-language pages.*

Reference number
IEC 61508-2:2000(E)

This is a preview - click here to buy the full publication

INTERNATIONAL STANDARD

IEC 61508-2

First edition
2000-05

BASIC SAFETY PUBLICATION

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

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

withdrawn

© IEC 2000 Copyright - all rights reserved

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 the publisher.

International Electrotechnical Commission, 3, rue de Varembé, PO Box 131, CH-1211 Geneva 20, Switzerland
Telephone: +41 22 919 02 11 Telefax: +41 22 919 03 00 E-mail: inmail@iec.ch Web: www.iec.ch

Commission Electrotechnique Internationale
International Electrotechnical Commission
Международная Электротехническая Комиссия

PRICE CODE XB

For price, see current catalogue

This is a preview - click here to buy the full publication

CONTENTS

Page

FOREWORD 7
INTRODUCTION 11

Clause

1 Scope 15
2 Normative references 21
3 Definitions and abbreviations 23
4 Conformance to this standard 23
5 Documentation 23
6 Management of functional safety 23
7 E/E/PES safety lifecycle requirements 23
7.1 General 23
7.2 E/E/PES safety requirements specification 31
7.3 E/E/PES safety validation planning 35
7.4 E/E/PES design and development 37
7.5 E/E/PES integration 71
7.6 E/E/PES operation and maintenance procedures 73
7.7 E/E/PES safety validation 77
7.8 E/E/PES modification 79
7.9 E/E/PES verification 79
8 Functional safety assessment 83

Annex A (normative) Techniques and measures for E/E/PE safety-related systems: control of failures during operation 85
A.1 General 85
A.2 Hardware safety integrity 87
A.3 Systematic safety integrity 105
Annex B (normative) Techniques and measures for E/E/PE safety-related systems: avoidance of systematic failures during the different phases of the lifecycle 117
Annex C (normative) Diagnostic coverage and safe failure fraction 137
C.1 Calculation of diagnostic coverage and safe failure fraction of a subsystem 137
C.2 Determination of diagnostic coverage factors 139

Bibliography 143

Withdrawn

This is a preview - click here to buy the full publication

Page

Figure 1 – Overall framework of IEC 61508 19
Figure 2 – E/E/PES safety lifecycle (in realisation phase) 25
Figure 3 – Relationship and scope for IEC 61508-2 and IEC 61508-3 27
Figure 4 – Relationship between the hardware and software architectures of programmable electronics 39
Figure 5 – Example limitation on hardware safety integrity for a single-channel safety function 49
Figure 6 – Example limitation on hardware safety integrity for a multiple-channel safety function 53

Table 1 – Overview – Realisation phase of the E/E/PES safety lifecycle 29
Table 2 – Hardware safety integrity: architectural constraints on type A safety-related subsystems 47
Table 3 – Hardware safety integrity: architectural constraints on type B safety-related subsystems 47
Table A.1 – Faults or failures to be detected during operation or to be analysed in the derivation of safe failure fraction 89
Table A.2 – Electrical subsystems 91
Table A.3 – Electronic subsystems 93
Table A.4 – Processing units 93
Table A.5 – Invariable memory ranges 95
Table A.6 – Variable memory ranges 95
Table A.7 – I/O units and interface (external communication) 97
Table A.8 – Data paths (internal communication) 97
Table A.9 – Power supply 99
Table A.10 – Program sequence (watch-dog) 99
Table A.11 – Ventilation and heating system (if necessary) 101
Table A.12 – Clock 101
Table A.13 – Communication and mass-storage 103
Table A.14 – Sensors 103
Table A.15 – Final elements (actuators) 105
Table A.16 – Techniques and measures to control systematic failures caused by hardware and software design 109
Table A.17 – Techniques and measures to control systematic failures caused by environmental stress or influences 111
Table A.18 – Techniques and measures to control systematic operational failures 113
Table A.19 – Effectiveness of techniques and measures to control systematic failures 115
Table B.1 – Recommendations to avoid mistakes during specification of E/E/PES requirements (see 7.2) 121
Table B.2 – Recommendations to avoid introducing faults during E/E/PES design and development (see 7.4) 123
Table B.3 – Recommendations to avoid faults during E/E/PES integration (see 7.5) 125
Table B.4 – Recommendations to avoid faults and failures during E/E/PES operation and maintenance procedures (see 7.6) 127
Table B.5 – Recommendations to avoid faults during E/E/PES safety validation (see 7.7) 129
Table B.6 – Effectiveness of techniques and measures to avoid systematic failures 131

Withdrawn

This is a preview - click here to buy the full publication

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.

Withdrawn

This is a preview - click here to buy the full publication

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.

withdrawn

This is a preview - click here to buy the full publication

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;

Withdrawn

This is a preview - click here to buy the full publication

- 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

This is a preview - click here to buy the full publication

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

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

Withdrawn

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.

This is a preview - click here to buy the full publication

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.

withdrawn

This is a preview - click here to buy the full publication

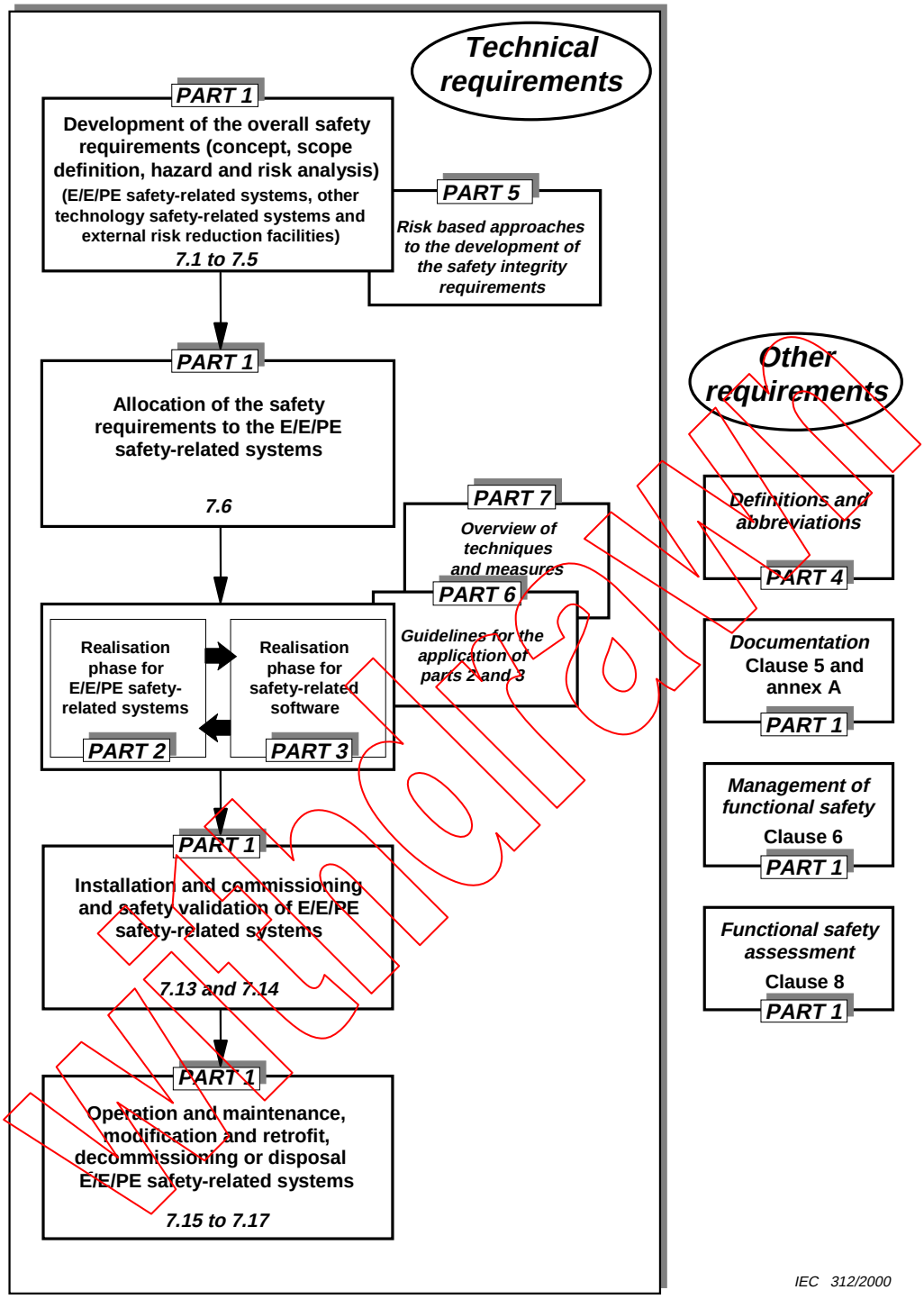

Figure 1 – Overall framework of IEC 61508

This is a preview - click here to buy the full publication

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* [1)]

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*

Withdrawn

---

1) To be published.