

INTERNATIONAL STANDARD

IEC 61508-1

First edition
1998-12

BASIC SAFETY PUBLICATION

Functional safety of electrical/electronic/ programmable electronic safety-related systems – Part 1: General requirements

*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 61508-1:1998(E)

INTERNATIONAL STANDARD

IEC 61508-1

First edition
1998-12

BASIC SAFETY PUBLICATION

Functional safety of electrical/electronic/ programmable electronic safety-related systems – Part 1: General requirements

© IEC 1998 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 Varembe, 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 **XA**

For price, see current catalogue

CONTENTS

	Page
FOREWORD	7
INTRODUCTION	11
Clause	
1 Scope	15
2 Normative references	21
3 Definitions and abbreviations.....	21
4 Conformance to this standard.....	23
5 Documentation.....	23
5.1 Objectives.....	23
5.2 Requirements	25
6 Management of functional safety	27
6.1 Objectives.....	27
6.2 Requirements	27
7 Overall safety lifecycle requirements	31
7.1 General.....	31
7.2 Concept	49
7.3 Overall scope definition.....	49
7.4 Hazard and risk analysis	51
7.5 Overall safety requirements.....	55
7.6 Safety requirements allocation	57
7.7 Overall operation and maintenance planning	69
7.8 Overall safety validation planning	71
7.9 Overall installation and commissioning planning	73
7.10 Realisation: E/E/PES.....	75
7.11 Realisation: other technology	75
7.12 Realisation: external risk reduction facilities	75
7.13 Overall installation and commissioning	77
7.14 Overall safety validation	77
7.15 Overall operation, maintenance and repair.....	79
7.16 Overall modification and retrofit.....	85
7.17 Decommissioning or disposal	89
7.18 Verification.....	91
8 Functional safety assessment.....	93
8.1 Objective	93
8.2 Requirements	93

Annexes

Annex A (informative) Example documentation structure	99
A.1 General	99
A.2 Safety lifecycle document structure	101
A.3 Physical document structure	107
A.4 List of documents.....	111
Annex B (informative) Competence of persons.....	113
B.1 Objective	113
B.2 General considerations	113
Annex C (informative) Bibliography	115

Tables

1 Overall safety lifecycle: overview	39
2 Safety integrity levels: target failure measures for a safety function, allocated to an E/E/PE safety-related system operating in low demand mode of operation	65
3 Safety integrity levels: target failure measures for a safety function, allocated to an E/E/PE safety-related system operating in high demand or continuous mode of operation.....	65
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))	97
5 Minimum levels of independence of those carrying out functional safety assessment (overall safety lifecycle phase 9 - includes all phases of E/E/PES and software safety lifecycles (see figures 2, 3 and 4))	97
A.1 Example documentation structure for information related to the overall safety lifecycle	103
A.2 Example documentation structure for information related to the E/E/PES safety lifecycle	105
A.3 Example documentation structure for information related to the software safety lifecycle	107

Figures

1 Overall framework of this standard	19
2 Overall safety lifecycle.....	33
3 E/E/PES safety lifecycle (in realisation phase)	35
4 Software safety lifecycle (in realisation phase).....	35
5 Relationship of overall safety lifecycle to E/E/PES and software safety lifecycles.....	37
6 Allocation of safety requirements to the E/E/PE safety-related systems, other technology safety-related systems and external risk reduction facilities	63
7 Example operations and maintenance activities model.....	83
8 Example operation and maintenance management model.....	85
9 Example modification procedure model	89
A.1 Structuring information into document sets for user groups.....	109
A.2 Structuring information for large complex systems and small low complexity systems	109

INTERNATIONAL ELECTROTECHNICAL COMMISSION

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

Part 1: General requirements

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 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 61508-1 has been prepared by subcommittee 65A: System aspects, of IEC technical committee 65: Industrial-process measurement and control.

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

FDIS	Report on voting
65A/264/FDIS	65A/274/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.

Annexes A, B and C are for information only.

It has the status of a basic safety publication in accordance with IEC Guide 104.

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 IEC 61508-2 and IEC 61508-3
- Part 7: Overview of techniques and measures

The contents of the corrigendum of April 1999 have been included in this copy.

Withdrawn

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 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 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 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 recognized 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 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 use 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

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

Part 1: General requirements

1 Scope

1.1 This International Standard covers those aspects to be considered when electrical/electronic/programmable electronic systems (E/E/PESs) are used to carry out safety functions. A major objective of this standard is to facilitate the development of application sector international standards by the technical committees responsible for the application sector. This will allow all the relevant factors, associated with the application, to be fully taken into account and thereby meet the specific needs of the application sector. A dual objective of this standard is to enable the development of electrical/electronic/programmable electronic (E/E/PE) safety-related systems where application sector international standards may not exist.

1.2 In particular, this standard

a) applies to safety-related systems when one or more of such systems incorporates electrical/electronic/programmable electronic devices;

NOTE 1 – In the context of low complexity E/E/PE safety-related systems, certain requirements specified in this standard may be unnecessary, and exemption from compliance with such requirements is possible (see 4.2, and the definition of a low complexity E/E/PE safety-related system in 3.4.4 of IEC 61508-4).

NOTE 2 – Although a person can form part of a safety-related system (see 3.4.1 of IEC 61508-4), human factor requirements related to the design of E/E/PE safety-related systems are not considered in detail in this standard.

b) is generically-based and applicable to all E/E/PE safety-related systems irrespective of the application;

c) covers possible hazards caused by failures of the safety functions to be performed by E/E/PE safety-related systems, as distinct from hazards arising from the E/E/PE equipment itself (for example electric shock etc);

d) does not cover E/E/PE systems where

- a single E/E/PE system is capable of providing the necessary risk reduction, and
- the required safety integrity of the E/E/PE system is less than that specified for safety integrity level 1 (the lowest safety integrity level in this standard).

e) is mainly concerned with the E/E/PE safety-related systems whose failure could have an impact on the safety of persons and/or the environment; however, it is recognized that the consequences of failure could also have serious economic implications and in such cases this standard could be used to specify any E/E/PE system used for the protection of equipment or product;

NOTE – See 3.1.1 and 7.3.1.2 of IEC 61508-4.

- f) considers E/E/PE safety-related systems, other technology safety-related systems and external risk reduction facilities in order that the safety requirements specification for the E/E/PE safety-related systems can be determined in a systematic, risk-based manner;
- g) uses an overall safety lifecycle model as the technical framework for dealing systematically with the activities necessary for ensuring the functional safety of the E/E/PE safety-related systems;

NOTE 3 – The early phases of the overall safety lifecycle include, of necessity, consideration of other technology (as well as the E/E/PE safety-related systems) and external risk reduction facilities, in order that the safety requirements specification for the E/E/PE safety-related systems can be developed in a systematic, risk-based manner.

NOTE 4 – Although the overall safety lifecycle is primarily concerned with E/E/PE safety-related systems, it could also provide a technical framework for the consideration of any safety-related system irrespective of the technology of that system (for example mechanical, hydraulic or pneumatic).

- h) does not specify the safety integrity levels required for sector applications (which must be based on detailed information and knowledge of the sector application). The technical committees responsible for the specific application sectors shall specify, where appropriate, the safety integrity levels in the application sector standards;
- i) provides general requirements for E/E/PE safety-related systems where no application sector standards exist;
- j) does not cover the precautions that may be necessary to prevent unauthorized persons damaging, and/or otherwise adversely affecting, the functional safety of E/E/PE safety-related systems.

1.3 This part of IEC 61508 specifies the general requirements that are applicable to all parts. Other parts of IEC 61508 concentrate on more specific topics:

- parts 2 and 3 provide additional and specific requirements for E/E/PE safety-related systems (for hardware and software);
- part 4 gives definitions and abbreviations that are used throughout this standard;
- part 5 provides guidelines on the application of part 1 in determining safety integrity levels, by showing example methods;
- part 6 provides guidelines on the application of parts 2 and 3;
- part 7 contains an overview of techniques and measures.

1.4 Parts 1, 2, 3 and 4 of this standard 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 part 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*. Parts 1, 2, 3, and 4 are also intended for use as stand-alone publications.

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 – In the USA and Canada, until the proposed process sector implementation of IEC 61508 is published as an international standard in the USA and Canada, existing national process safety standards based on IEC 61508 (i.e. ANSI/ISA S84.01-1996) (see reference [8] in annex C) can be applied to the process sector instead of IEC 61508.

1.5 Figure 1 shows the overall framework for parts 1 to 7 of IEC 61508 and indicates the role that IEC 61508-1 plays in the achievement of functional safety for E/E/PE safety-related systems.

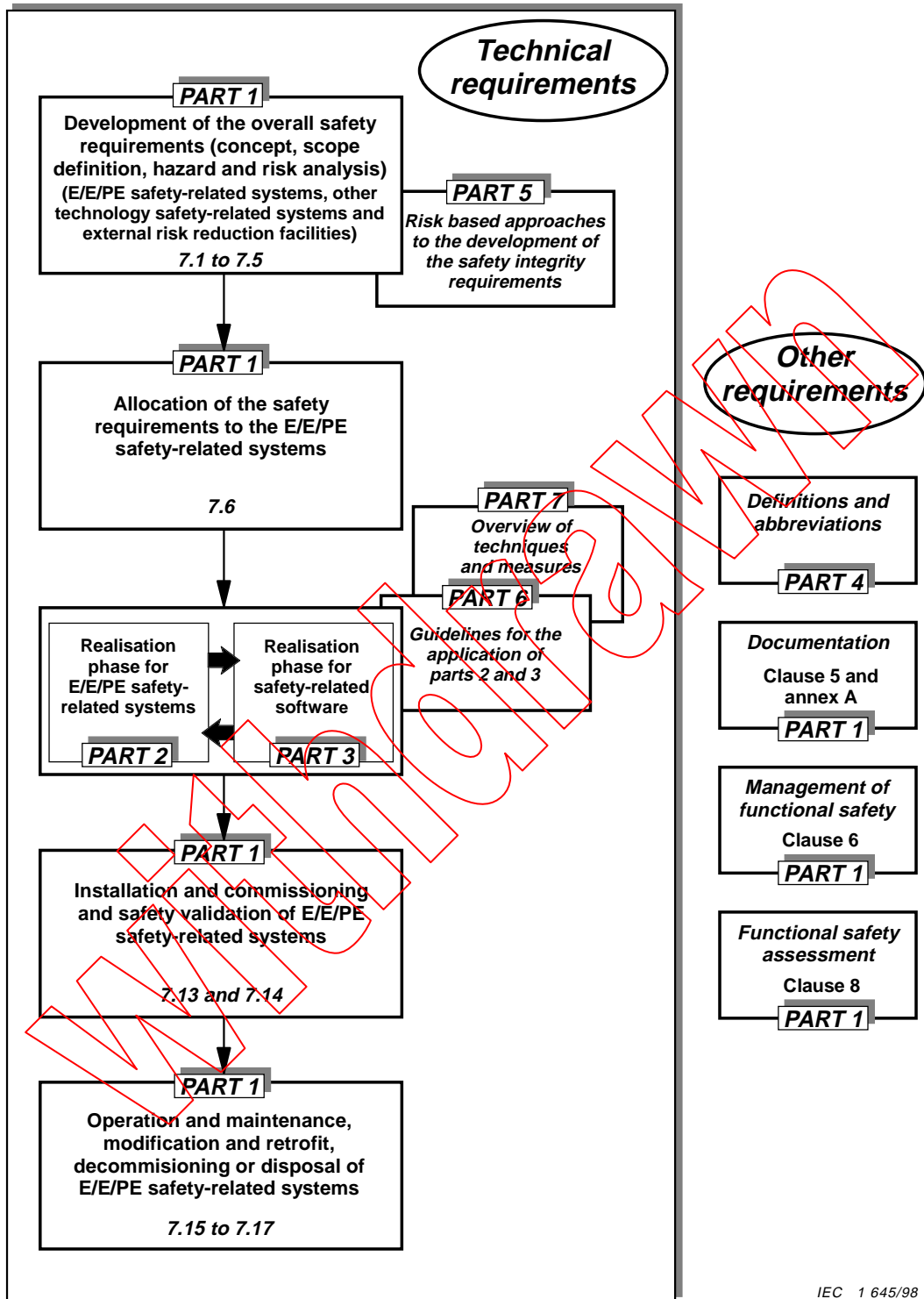


Figure 1 – Overall framework of this standard

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.

ISO/IEC Guide 51:1990, *Guidelines for the inclusion of safety aspects in standards*

IEC Guide 104:1997, *Guide to the drafting of safety standards, and the role of Committees with safety pilot functions and safety group functions*

IEC 61508-2, — *Functional safety of electrical/electrical/programmable electronic safety-related systems – Part 2: Requirements for electrical/electrical/programmable electronic safety-related systems* ¹⁾

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

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

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

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

IEC 61508-7, — *Functional safety of electrical/electrical/programmable electronic safety-related systems – Part 7: Overview of techniques and measures* ²⁾

²⁾ To be published.