

INTERNATIONAL STANDARD

IEC
61508-5

First edition
1998-12

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

*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 61508-5:1998(E)

INTERNATIONAL STANDARD

IEC 61508-5

First edition
1998-12

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

© 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

U

For price, see current catalogue

CONTENTS

	Page
FOREWORD	5
INTRODUCTION	9
Clause	
1 Scope	13
2 Normative references	17
3 Definitions and abbreviations.....	17
Annexes	
A Risk and safety integrity – General concepts.....	19
B ALARP and tolerable risk concepts.....	31
C Determination of safety integrity levels: a quantitative method.....	37
D Determination of safety integrity levels – A qualitative method: risk graph	43
E Determination of safety integrity levels – A qualitative method: hazardous event severity matrix	53
F Bibliography	57
Figures	
1 Overall framework of this standard.....	15
A.1 Risk reduction: general concepts	25
A.2 Risk and safety integrity concepts.....	25
A.3 Allocation of safety requirements to the E/E/PE safety-related systems, other technology safety-related systems and external risk reduction facilities	29
B.1 Tolerable risk and ALARP.....	33
C.1 Safety integrity allocation: example for safety-related protection system	41
D.1 Risk graph: general scheme	47
D.2 Risk graph: example (illustrates general principles only)	49
E.1 Hazardous event severity matrix: example (illustrates general principles only).....	55
Tables	
B.1 Risk classification of accidents	35
B.2 Interpretation of risk classes.....	35
D.1 Example data relating to example risk graph (figure D.2)	51

INTERNATIONAL ELECTROTECHNICAL COMMISSION

**FUNCTIONAL SAFETY OF ELECTRICAL/ELECTRONIC/PROGRAMMABLE
ELECTRONIC SAFETY-RELATED SYSTEMS –****Part 5: Examples of methods for the determination
of safety integrity levels**

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 61508-5 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/266/FDIS	65A/276/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, C, D, E and F are for information only.

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

This part 5 shall be read in conjunction with part 1.

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

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

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 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 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 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.

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

Part 5: Examples of methods for the determination of safety integrity levels

1 Scope

1.1 This part of IEC 61508 provides information on

- the underlying concepts of risk and the relationship of risk to safety integrity (see annex A);
- a number of methods that will enable the safety integrity levels for the E/E/PE safety-related systems, other technology safety-related systems and external risk reduction facilities to be determined (see annexes B, C, D and E).

1.2 The method selected will depend upon the application sector and the specific circumstances under consideration. Annexes B, C, D and E illustrate quantitative and qualitative approaches and have been simplified in order to illustrate the underlying principles. These annexes have been included to illustrate the general principles of a number of methods but do not provide a definitive account. Those intending to apply the methods indicated in these annexes should consult the source material referenced.

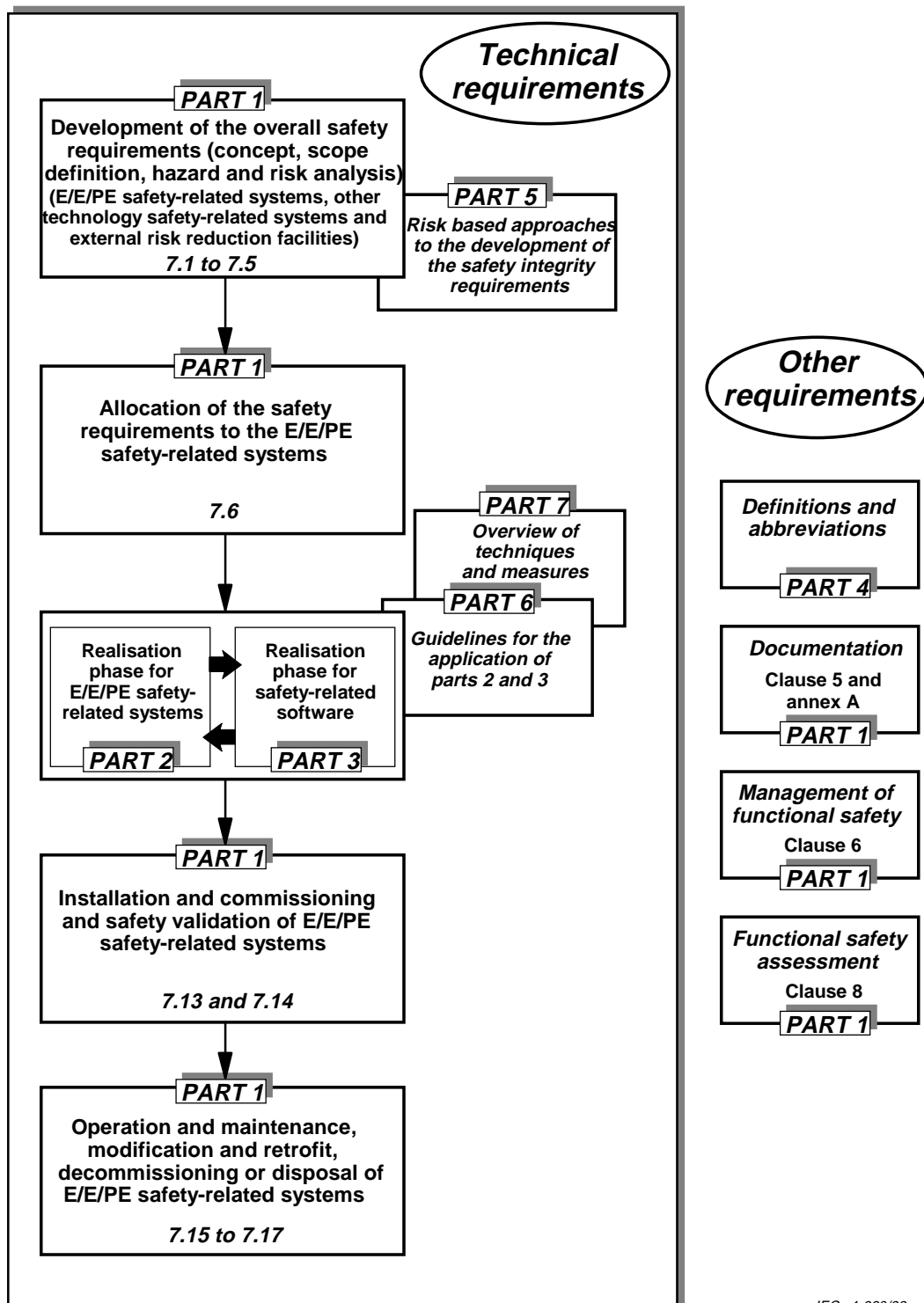
NOTE – For more information on the approaches illustrated in annexes B, D and E, see references [4], [2] and [3] respectively in annex F. See also reference [5] in annex F for a description of an additional approach.

1.3 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 (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 S84.01-1996) can be applied to the process sector instead of IEC 61508.

1.4 Figure 1 shows the overall framework for parts 1 to 7 of IEC 61508 and indicates the role that IEC 61508-5 plays in the achievement of functional safety for E/E/PE safety-related systems.



IEC 1 660/98

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 International Standard. At the time of publication, the editions indicated were valid. All normative documents are subject to revision, and parties to agreements based on this International Standard are encouraged to investigate the possibility of applying the most recent editions of the normative documents indicated below. Members of IEC and ISO maintain registers of currently valid International Standards.

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

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 of terms*

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* ¹⁾

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*

¹⁾ To be published.