



DPC: 25 / 30507501 DC

## BSI Group Headquarters

389 Chiswick High Road London W4 4AL

Tel: +44 (0)20 8996 9000

Fax: +44 (0)20 8996 7400

www.bsigroup.com

Date: 18 February 2025

Origin: International

**Latest date for receipt of comments: 9 April 2025**

Project No. 2025/00123

Responsible committee: GEL/65/1 Systems aspects

Interested committees:

Title: BS EN IEC 61508-5 Functional safety of electrical/electronic/programmable electronic safety-related systems

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

Please notify the secretary if you are aware of any keywords that might assist in classifying or identifying the standard or if the content of this standard

- i) has any issues related to 3rd party IPR, patent or copyright
- ii) affects other national standard(s)
- iii) requires additional national guidance or information

**WARNING: THIS IS A DRAFT AND MUST NOT BE REGARDED OR USED AS A BRITISH STANDARD.  
THIS DRAFT IS NOT CURRENT BEYOND 9 April 2025**

This draft is issued to allow comments from interested parties; all comments will be given consideration prior to publication. No acknowledgement will normally be sent. **See overleaf for information on the submission of comments.**

No copying is allowed, in any form, without prior written permission from BSI except as permitted under the Copyright, Designs and Patent Act 1988 or for circulation within a nominating organization for briefing purposes. Electronic circulation is limited to dissemination by e-mail within such an organization by committee members.

Further copies of this draft may be purchased from BSI Shop <http://shop.bsigroup.com> or from BSI Customer Services, Tel: +44(0) 20 8996 9001 or email [cservices@bsigroup.com](mailto:cservices@bsigroup.com). British, International and foreign standards are also available from BSI Customer Services.

Information on the co-operating organizations represented on the committees referenced above may be obtained from <http://standardsdevelopment.bsigroup.com>

Responsible Committee Secretary: Ms Charmaine Mukherjee (BSI)

Direct tel:

E-mail: [charmaine.mukherjee@bsigroup.com](mailto:charmaine.mukherjee@bsigroup.com)

## Introduction

This draft standard is based on national and international discussions. Your comments on this draft are invited and will assist in the preparation of the consequent standard.

For international standards, comments will be reviewed by the relevant UK national committee before sending the consensus UK vote and comments to the international committee, which will then decide appropriate action. If the international standard is approved, it is usual for the text to be published as a British Standard.

For national standards, comments will be reviewed by the relevant UK national committee and the resulting standards published as a British Standard.

## UK Vote

Please indicate whether you consider the UK should submit a negative (with supporting technical reasons) or positive vote on this draft. Please indicate if you are aware of any reason why this draft standard should not be published as a British Standard.

## Submission of Comments

- **Annotated drafts are not acceptable and will be rejected.**
- All comments should be submitted online at <https://standardsdevelopment.bsigroup.com/>. You will need to register in order to comment.

## Template for comments and secretariat observations

|                  |                        |
|------------------|------------------------|
| Date: xx/xx/20xx | Document: ISO/DIS xxxx |
|------------------|------------------------|

| 1  | 2                                          | (3)                          | 4               | 5                                                                                                                                  | (6)                                                                      | 7                                                  |
|----|--------------------------------------------|------------------------------|-----------------|------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------|----------------------------------------------------|
| MB | Clause No./ Subclause No./Annex (e.g. 3.1) | Paragraph/Figure/ Table/Note | Type of comment | Commend (justification for change) by the MB                                                                                       | Proposed change by the MB                                                | Secretariat observations on each comment submitted |
|    | 3.1                                        | Definition 1                 | ed              | Definition is ambiguous and needs clarifying.                                                                                      | Amend to read '...so that the mains connector to which no connection...' |                                                    |
|    | 6.4                                        | Paragraph 2                  | te              | The use of the UV photometer as an alternative cannot be supported as serious problems have been encountered in its use in the UK. | Delete reference to UV photometer.                                       |                                                    |



# 65A/1167/CDV

COMMITTEE DRAFT FOR VOTE (CDV)

|                                                            |                                               |
|------------------------------------------------------------|-----------------------------------------------|
| PROJECT NUMBER:<br><b>IEC 61508-5 ED3</b>                  |                                               |
| DATE OF CIRCULATION:<br><b>2025-02-14</b>                  | CLOSING DATE FOR VOTING:<br><b>2025-05-09</b> |
| SUPERSEDES DOCUMENTS:<br><b>65A/1060A/CD, 65A/1079A/CC</b> |                                               |

|                                                                                                                                                                                                                                                                                                                                                                                             |                                                                    |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------|
| IEC SC 65A : SYSTEM ASPECTS                                                                                                                                                                                                                                                                                                                                                                 |                                                                    |
| SECRETARIAT:<br>United Kingdom                                                                                                                                                                                                                                                                                                                                                              | SECRETARY:<br>Ms Stephanie Lavy                                    |
| OF INTEREST TO THE FOLLOWING COMMITTEES:<br>TC 8,TC 9,TC 22,TC 31,TC 44,TC 45,TC 56,TC 61,TC 62,TC 65,SC 65B,SC 65C,SC 65E,TC 66,TC 77,TC 80,TC 108,SyC AAL,SyC SM,SC 41                                                                                                                                                                                                                    | HORIZONTAL FUNCTION(S):                                            |
| ASPECTS CONCERNED:<br>Safety                                                                                                                                                                                                                                                                                                                                                                |                                                                    |
| <input checked="" type="checkbox"/> SUBMITTED FOR CENELEC PARALLEL VOTING<br><br><b>Attention IEC-CENELEC parallel voting</b><br><br>The attention of IEC National Committees, members of CENELEC, is drawn to the fact that this Committee Draft for Vote (CDV) is submitted for parallel voting.<br><br>The CENELEC members are invited to vote through the CENELEC online voting system. | <input type="checkbox"/> NOT SUBMITTED FOR CENELEC PARALLEL VOTING |

This document is still under study and subject to change. It should not be used for reference purposes.

Recipients of this document are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

Recipients of this document are invited to submit, with their comments, notification of any relevant "In Some Countries" clauses to be included should this proposal proceed. Recipients are reminded that the CDV stage is the final stage for submitting ISC clauses. (SEE [AC/22/2007](#) OR [NEW GUIDANCE DOC](#)).

|                                                                                                                                                                                           |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| TITLE:<br><b>Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 5: Examples of methods for the determination of safety integrity levels</b> |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|                               |
|-------------------------------|
| PROPOSED STABILITY DATE: 2028 |
|-------------------------------|

|                           |
|---------------------------|
| NOTE FROM TC/SC OFFICERS: |
|---------------------------|

**Copyright © 2025 International Electrotechnical Commission, IEC.** All rights reserved. It is permitted to download this electronic file, to make a copy and to print out the content for the sole purpose of preparing National Committee positions. You may not copy or "mirror" the file or printed version of the document, or any part of it, for any other purpose without permission in writing from IEC.

# CONTENTS

|    |                                                                                              |    |
|----|----------------------------------------------------------------------------------------------|----|
| 1  |                                                                                              |    |
| 2  | FOREWORD.....                                                                                | 5  |
| 3  | INTRODUCTION.....                                                                            | 7  |
| 4  | 1 Scope.....                                                                                 | 9  |
| 5  | 2 Normative references .....                                                                 | 11 |
| 6  | 3 Definitions and abbreviations.....                                                         | 11 |
| 7  | Annex A (informative) Risk and safety integrity – General concepts .....                     | 12 |
| 8  | A.1 General.....                                                                             | 12 |
| 9  | A.2 Necessary risk reduction.....                                                            | 12 |
| 10 | A.2.1 Individual risk .....                                                                  | 13 |
| 11 | A.2.2 Societal risk.....                                                                     | 13 |
| 12 | A.2.3 Continuous improvement .....                                                           | 13 |
| 13 | A.2.4 Risk profile .....                                                                     | 14 |
| 14 | A.3 Role of E/E/PE safety-related systems.....                                               | 14 |
| 15 | A.4 Safety integrity.....                                                                    | 14 |
| 16 | A.5 Modes of operation and SIL determination .....                                           | 15 |
| 17 | A.5.1 Safety integrity and risk reduction for low demand mode applications .....             | 15 |
| 18 | A.5.2 Safety integrity for high demand mode applications .....                               | 16 |
| 19 | A.5.3 Safety integrity for continuous mode applications .....                                | 18 |
| 20 | A.5.4 Common cause and dependency failures.....                                              | 18 |
| 21 | A.5.5 Safety integrity levels when multiple layers of protection are used .....              | 20 |
| 22 | A.5.6 General architecture in this standard .....                                            | 20 |
| 23 | A.6 Risk and safety integrity.....                                                           | 22 |
| 24 | A.7 Safety integrity levels and systematic capability.....                                   | 23 |
| 25 | A.8 Allocation of safety requirements .....                                                  | 23 |
| 26 | A.9 Mitigation systems .....                                                                 | 24 |
| 27 | Annex B (informative) Selection of methods for determining safety integrity level            |    |
| 28 | requirements .....                                                                           | 25 |
| 29 | B.1 General.....                                                                             | 25 |
| 30 | B.2 The ALARP method .....                                                                   | 25 |
| 31 | B.3 Quantitative method of SIL determination .....                                           | 25 |
| 32 | B.4 The risk graph method .....                                                              | 26 |
| 33 | B.5 Layer of protection analysis (LOPA).....                                                 | 26 |
| 34 | B.6 Hazardous event severity matrix .....                                                    | 27 |
| 35 | Annex C (informative) ALARP and tolerable risk concepts .....                                | 28 |
| 36 | C.1 General.....                                                                             | 28 |
| 37 | C.2 ALARP model .....                                                                        | 28 |
| 38 | C.2.1 Introduction .....                                                                     | 28 |
| 39 | C.2.2 Tolerable risk target.....                                                             | 29 |
| 40 | Annex D (informative) Determination of safety integrity levels – A quantitative method ..... | 31 |
| 41 | D.1 General.....                                                                             | 31 |
| 42 | D.2 General method .....                                                                     | 31 |
| 43 | D.3 Example calculation .....                                                                | 32 |
| 44 | Annex E (informative) Determination of safety integrity levels – Risk graph methods .....    | 34 |
| 45 | E.1 General.....                                                                             | 34 |
| 46 | E.2 Risk graph synthesis.....                                                                | 34 |

|    |                                                                                              |                                                                   |    |
|----|----------------------------------------------------------------------------------------------|-------------------------------------------------------------------|----|
| 47 | E.3                                                                                          | Calibration .....                                                 | 35 |
| 48 | E.4                                                                                          | Other possible risk parameters .....                              | 36 |
| 49 | E.5                                                                                          | Risk graph implementation – general scheme .....                  | 36 |
| 50 | E.6                                                                                          | Risk graph example .....                                          | 37 |
| 51 | Annex F (informative)                                                                        | Semi-quantitative method using layer of protection analysis       |    |
| 52 | (LOPA) .....                                                                                 |                                                                   | 42 |
| 53 | F.1                                                                                          | General.....                                                      | 42 |
| 54 | F.1.1                                                                                        | Description .....                                                 | 42 |
| 55 | F.1.2                                                                                        | Annex reference .....                                             | 42 |
| 56 | F.1.3                                                                                        | Method description .....                                          | 42 |
| 57 | F.2                                                                                          | Impact event .....                                                | 42 |
| 58 | F.3                                                                                          | Severity level .....                                              | 42 |
| 59 | F.4                                                                                          | Initiating cause .....                                            | 42 |
| 60 | F.5                                                                                          | Initiation likelihood .....                                       | 43 |
| 61 | F.6                                                                                          | Protection layers (PLs) .....                                     | 46 |
| 62 | F.6.1                                                                                        | General .....                                                     | 46 |
| 63 | F.6.2                                                                                        | Basic control system.....                                         | 46 |
| 64 | F.6.3                                                                                        | Alarms .....                                                      | 46 |
| 65 | F.7                                                                                          | Additional mitigation .....                                       | 47 |
| 66 | F.8                                                                                          | Intermediate event likelihood .....                               | 47 |
| 67 | F.9                                                                                          | Safety integrity levels (SILs) .....                              | 47 |
| 68 | F.10                                                                                         | Tolerable mitigated event likelihood .....                        | 48 |
| 69 | Annex G (informative)                                                                        | Determination of safety integrity levels – A qualitative method – |    |
| 70 | hazardous event severity matrix .....                                                        |                                                                   | 49 |
| 71 | G.1                                                                                          | General.....                                                      | 49 |
| 72 | G.2                                                                                          | Hazardous event severity matrix .....                             | 49 |
| 73 | Bibliography.....                                                                            |                                                                   | 51 |
| 74 |                                                                                              |                                                                   |    |
| 75 | Figure 1 – Overall framework of the IEC 61508 series .....                                   |                                                                   | 10 |
| 76 | Figure A.1 – Risk reduction – general concepts (low demand mode of operation) .....          |                                                                   | 16 |
| 77 | Figure A.2 – Risk and safety integrity concept .....                                         |                                                                   | 16 |
| 78 | Figure A.3 – Risk diagram for high demand applications .....                                 |                                                                   | 17 |
| 79 | Figure A.4 – Risk diagram for continuous mode operation .....                                |                                                                   | 18 |
| 80 | Figure A.5 – Illustration of common cause failures (CCFs) of elements in the EUC             |                                                                   |    |
| 81 | control system and elements in the E/E/PE safety-related system.....                         |                                                                   | 19 |
| 82 | Figure A.6 – Common cause between two E/E/PE safety-related systems .....                    |                                                                   | 20 |
| 83 | Figure A.7 – Architecture where the control functions are not safety functions (EUC          |                                                                   |    |
| 84 | control system is not a designated E/E/PE safety-related system) .....                       |                                                                   | 21 |
| 85 | Figure A.8 – Architecture where the control functions are safety functions (EUC control      |                                                                   |    |
| 86 | system is a designated E/E/PE safety-related system).....                                    |                                                                   | 22 |
| 87 | Figure A.9 – Allocation of safety requirements to the E/E/PE safety-related systems,         |                                                                   |    |
| 88 | and other risk reduction measures .....                                                      |                                                                   | 24 |
| 89 | Figure C.1 – Tolerable risk and ALARP.....                                                   |                                                                   | 29 |
| 90 | Figure D.1 – Safety integrity allocation – example for safety-related protection system..... |                                                                   | 33 |
| 91 | Figure E.1 – Risk Graph: general scheme.....                                                 |                                                                   | 37 |
| 92 | Figure E.2 – Risk graph – example (illustrates general principles only).....                 |                                                                   | 38 |
| 93 | Figure G.1 – Hazardous event severity matrix – example (illustrates general principles       |                                                                   |    |
| 94 | only) .....                                                                                  |                                                                   |    |

|     |                                                                               |
|-----|-------------------------------------------------------------------------------|
| 95  |                                                                               |
| 96  | Table C.1 – Example of risk classification of accidents ..... 30              |
| 97  | Table C.2 – Interpretation of risk classes ..... 30                           |
| 98  | Table E.1 – Example of data relating to risk graph (Figure E.2)..... 38       |
| 99  | Table E.2 – Example of calibration of the general purpose risk graph ..... 40 |
| 100 | Table F.1 – LOPA report ..... 44                                              |
| 101 |                                                                               |
| 102 |                                                                               |

## 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 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) IEC draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). IEC takes no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, IEC had not received notice of (a) patent(s), which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at <https://patents.iec.ch>. IEC shall not be held responsible for identifying any or all such patent rights.

IEC 61508-5 has been prepared by subcommittee 65A: System aspects, of IEC technical committee 65: Industrial-process measurement, control and automation. It is an International Standard.

This third edition cancels and replaces the second edition published in 2010. 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.

This edition includes the following significant technical changes with respect to the previous edition (the following list does refer to this document; other parts do mention specific further details):

- a) Document was upgraded to the 2024 version of the ISO/IEC Directives; this does introduce a significant number of editorial changes, clause renumbering and rewording of the information provided in Notes;
- b) Various minor editorial errors have been corrected, the normative references and the bibliography has been updated.

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

| Draft       | Report on voting |
|-------------|------------------|
| 65A/XX/FDIS | 65A/XX/RVD       |

Full information on the voting for its approval can be found in the report on voting indicated in the above table.

The language used for the development of this document is English.

This document was drafted in accordance with ISO/IEC Directives, Part 2, and developed in accordance with ISO/IEC Directives, Part 1 and ISO/IEC Directives, IEC Supplement, available at [www.iec.ch/members\\_experts/refdocs](http://www.iec.ch/members_experts/refdocs). The main document types developed by IEC are described in greater detail at [www.iec.ch/publications](http://www.iec.ch/publications).

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 document will remain unchanged until the stability date indicated on the IEC website under [webstore.iec.ch](http://webstore.iec.ch) in the data related to the specific document. At this date, the document 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 document 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 should 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 document 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 document, 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;
- 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;

- sets a lower limit on the target failure measures for a safety function carried out by 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 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<sup>-1</sup>];

NOTE 2 A single E/E/PE safety-related system does not necessarily mean a single-channel architecture.

NOTE 3 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 the confidence that its 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 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);
- the criteria in selecting the most appropriate method for determining safety integrity level requirements (see Annex B);
- a number of methods that will enable the safety integrity levels for the E/E/PE safety-related systems to be determined (see Annexes C, D, E, F and G).

The method selected will depend upon the application sector and the specific circumstances under consideration. Annexes C, D, E, F and G 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.

NOTE 1 Those intending to apply the methods indicated in these annexes can consult the source material referenced.

NOTE 2 For more information on the approaches illustrated in Annexes B, and E, see references [5] and [8] in the Bibliography. See also reference [6] in the Bibliography for a description of an additional approach.

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). This document provides further information to complement these basic safety publications.

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.

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

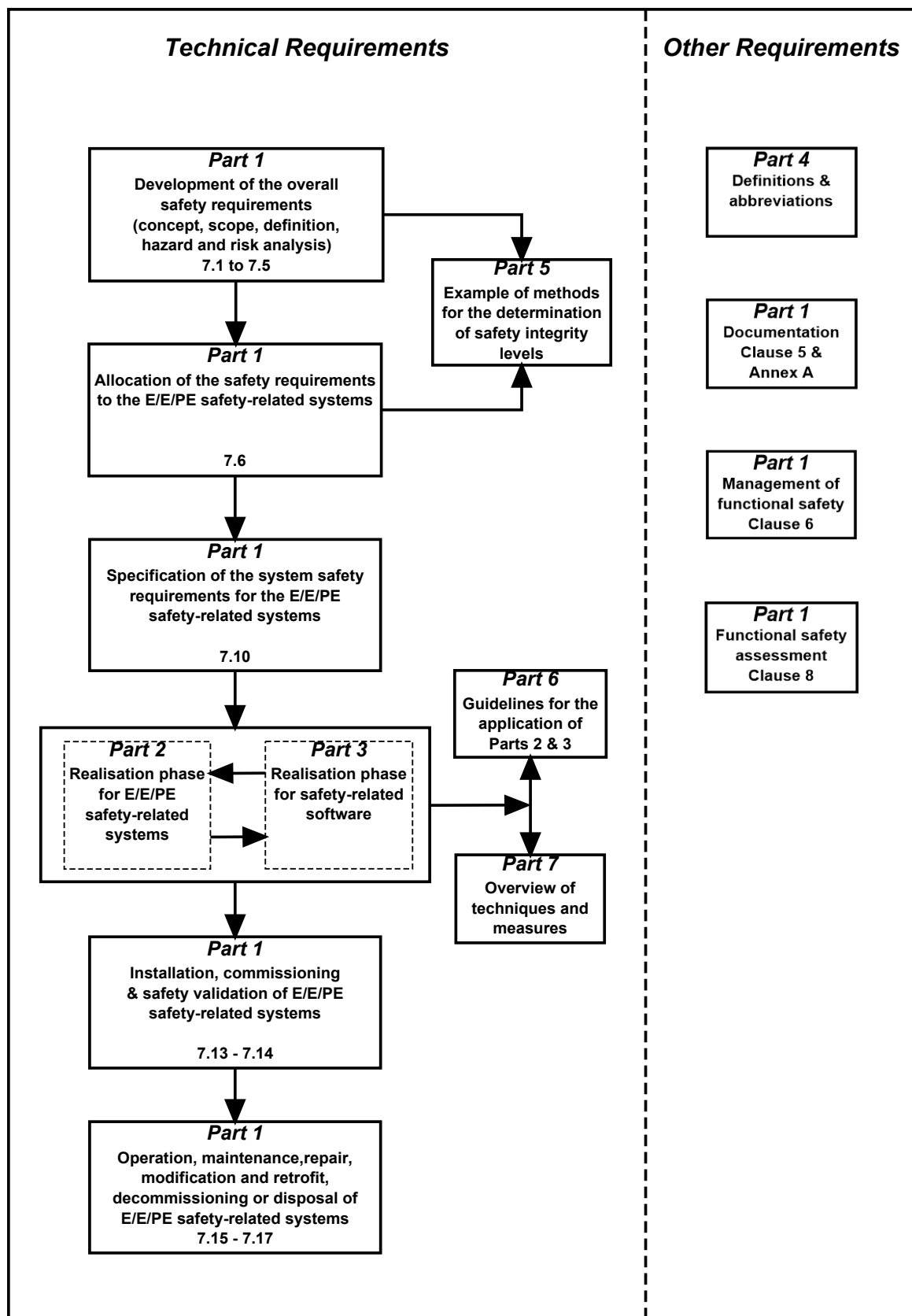


Figure 1 – Overall framework of the IEC 61508 series

## 2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 61508-1:20XX, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements*

IEC 61508-4:20XX, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 4: Definitions and abbreviations*

## 3 Definitions and abbreviations

For the purposes of this document, the definitions and abbreviations given in IEC 61508-4 apply.

## Annex A (informative)

### Risk and safety integrity – General concepts

#### A.1 General

This annex provides information on the underlying concepts of risk and the relationship of risk to safety integrity.

#### A.2 Necessary risk reduction

The necessary risk reduction is the reduction in risk that has to be achieved to meet the tolerable risk for a specific situation (which may be stated either qualitatively<sup>1</sup> or quantitatively<sup>2</sup>). The concept of necessary risk reduction is of fundamental importance in the development of the safety requirements specification for the E/E/PE safety-related systems (in particular, the safety integrity requirements part of the safety requirements specification). The purpose of determining the tolerable risk for a specific hazardous event is to state what is deemed reasonable with respect to both the frequency (or probability) of the hazardous event and its specific consequences. Safety-related systems are designed to reduce the frequency (or probability) of the hazardous event and/or the consequences of the hazardous event.

The tolerable risk will depend on many factors (for example, severity of injury, the number of people exposed to danger, the frequency at which a person or people are exposed to danger and the duration of the exposure). Important factors will be the perception and views of those exposed to the hazardous event. In arriving at what constitutes a tolerable risk for a specific application, a number of inputs are considered. These include:

- legal requirements, both general and those directly relevant to the specific application;
- guidelines from the appropriate safety regulatory authority;
- discussions and agreements with the different parties involved in the application;
- industry standards and guidelines;
- international discussions and agreements; the role of national and international standards is becoming increasingly important in arriving at tolerable risk criteria for specific applications;
- the best independent industrial, expert and scientific advice from advisory bodies.

In determining the safety integrity requirements of the E/E/PE safety-related system(s) and other risk reduction measures, in order to meet the tolerable frequency of a hazardous event, account needs to be taken of the characteristics of the risk that are relevant to the application. The tolerable frequency will depend on the legal requirements in the country of application and on the criteria specified by the user organisation. Issues that may need to be considered together with how they can be applied to E/E/PE safety-related systems are discussed below.

<sup>1</sup> In achieving the tolerable risk, the necessary risk reduction will need to be established. Annexes E and G of this document outline qualitative methods, although in the examples quoted the necessary risk reduction is incorporated implicitly by specification of the SIL requirement rather than stated explicitly by a numeric value of risk reduction required.

<sup>2</sup> For example, that the hazardous event, leading to a specific consequence, can not occur with a frequency greater than one in  $10^8$  h.

### A.2.1 Individual risk

Different targets are usually defined for employees and members of the public. The target for individual risk for employees is applied to the most exposed individual and may be expressed as the total risk per year arising from all work activities. The target is applied to a hypothetical person and therefore needs to take into account the percentage of time that the individual spends at work. The target applies to all risks to the exposed person and the tolerable risk for an individual safety function will need to take account of other risks.

Assurance that the total risk is reduced below a specified target can be done in a number of ways. One method is to consider and sum all risks to the most exposed individual. This may be difficult in cases where a person is exposed to many risks and early decisions are needed for system development. An alternative approach is to allocate a percentage of the overall individual risk target to each safety function under consideration. The percentage allocated can usually be decided from previous experience of the type of facility under consideration.

The target applied to an individual safety function should also take into account the conservatism of the method of risk analysis used. All qualitative methods such as risk graphs involve some evaluation of the critical parameters that contribute to risk. The factors that give rise to risk are the consequence of the hazardous event and its frequency. In determining these factors a number of risk parameters may need to be taken into account such as a vulnerability to the hazardous event, number of people who may be affected by the hazardous event, the probability that a person is present when the hazardous event occurs (i.e. occupancy) and probability of avoiding the hazardous event.

Qualitative methods generally involve deciding if a parameter lies within a certain range. The descriptions of the criteria when using such methods will need to be such that there can be a high level of confidence that the target for risks is not exceeded. This can involve setting range boundaries for all parameters so applications with all parameters at the boundary condition will meet the specified risk criteria for safety. This approach to setting the range boundaries is very conservative because there will be very few applications where all parameters will be at the worst case of the range. If members of the public are to be exposed to risk from failure of a E/E/PE safety-related system, then a lower target will normally apply.

### A.2.2 Societal risk

Societal risk<sup>3</sup> arises where multiple fatalities are likely to arise from single events. Such events are called societal because they are likely to provoke a socio-political response. There can be significant public and organisational aversion to high consequence events and this will need to be taken into consideration in some cases. The criterion for societal risk is often expressed as a maximum accumulated frequency for fatal injuries to a specified number of persons. The criterion is normally specified in the form of one or more lines on an F/N plot where F is the cumulative frequency of hazards and N the number of fatalities arising from the hazards. The relationship is normally a straight line when plotted on logarithmic scales. The slope of the line will depend on the extent to which the organisation is risk averse to higher levels of consequence. The requirement will be to ensure the accumulated frequency for a specified number of fatalities is lower than the accumulated frequency expressed in the F/N plot. (see reference [7] in the Bibliography)

### A.2.3 Continuous improvement

The principles of reducing risk to as low as reasonably practicable are discussed in Annex C.

<sup>3</sup> The question arises what the safe state of the society could be if such risks are mitigated by a safety function and which SIL would be appropriate to mitigate such risks.

#### A.2.4 Risk profile

In deciding risk criteria to be applied for a specific hazard, the risk profile over the life of the asset may need to be considered. Residual risk will vary from low just after a proof test or a repair has been performed to a maximum just prior to proof testing. This may need to be taken into consideration by organisations that specify the risk criteria to be applied. If proof test intervals are significant, then it may be appropriate to specify the maximum hazard probability that can be accepted just prior to proof testing or that the PFD(t) or PFH(t) is lower than the upper SIL boundary more than a specified percentage of the time (e.g. 90 %).

### A.3 Role of E/E/PE safety-related systems

E/E/PE safety-related systems contribute towards providing the necessary risk reduction in order to meet the tolerable risk.

A safety-related system both

- implements the required safety functions necessary to achieve a safe state for the equipment under control or to maintain a safe state for the equipment under control; and
- is intended to achieve, on its own or with other E/E/PE safety-related systems or other risk reduction measures, the necessary safety integrity for the required safety functions.

NOTE 1 The first part of the definition specifies that the safety-related system performs the safety functions which can be specified in the safety functions requirements specification. For example, the safety functions requirements specification can state that when the temperature reaches x, valve y can open to allow water to enter the vessel.

NOTE 2 The second part of the definition specifies that the safety functions can be performed by the safety-related systems with the degree of confidence appropriate to the application, in order that the tolerable risk will be achieved.

A person could be an integral part of an E/E/PE safety-related system. For example, a person could receive information, on the state of the EUC, from a display screen and perform a safety action based on this information.

E/E/PE safety-related systems can operate in a low demand mode of operation or high demand or continuous mode of operation.

### A.4 Safety integrity

Safety integrity is defined as the probability of a safety-related system satisfactorily performing the required safety functions under all the stated conditions within a stated period of time. Safety integrity relates to the performance of the safety-related systems in carrying out the safety functions (the safety functions to be performed will be specified in the safety functions requirements specification).

Safety integrity is considered to be composed of the following two elements.

- Hardware safety integrity; that part of safety integrity relating to random hardware failures in a dangerous mode of failure. The achievement of the specified level of safety-related hardware safety integrity can be estimated to a reasonable level of accuracy, and the requirements can therefore be apportioned between subsystems using the normal rules for the combination of probabilities. It may be necessary to use redundant architectures to achieve adequate hardware safety integrity.