IEC 61508-3

Edition 2.0 2010-04

INTERNATIONAL STANDARD

NORME INTERNATIONALE

BASIC SAFETY PUBLICATION

PUBLICATION FONDAMENTALE DE SÉCURITÉ

Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 3: Software requirements

iTeh STANDARD PREVIEW
(standards.iteh.ai)
IEC 61508-3:2010
https://standards.iteh.ai/catalog/standards/sist/f6570ef4-4785-4a0c-bc75-
5e8c4dc7dfb/iec-61508-3-2010

Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 3: Exigences concernant les logiciels

IEC 61508-3:2010

THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2010 IEC, Geneva, Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester.
If you have any questions about IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

Droits de reproduction réservés. Sauf indication contraire, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et les microfilms, sans l'accord écrit de la CEI ou du Comité national de la CEI du pays du demandeur.
Si vous avez des questions sur le copyright de la CEI ou si vous désirez obtenir des droits supplémentaires sur cette publication, utilisez les coordonnées ci-après ou contactez le Comité national de la CEI de votre pays de résidence.

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland
Email: inmail@iec.ch
Web: www.iec.ch

About the IEC

The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications

The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigenda or an amendment might have been published.

- Catalogue of IEC publications: www.iec.ch/searchpub

The IEC on-line Catalogue enables you to search by a variety of criteria (reference number, text, technical committee,…). It also gives information on projects, withdrawn and replaced publications.

- IEC Just Published: www.iec.ch/online_news/justpub

Stay up to date on all new IEC publications. Just Published details twice a month all new publications released. Available on-line and also by email.

- Electropedia: www.electropedia.org

The world's leading online dictionary of electronic and electrical terms containing more than 20 000 terms and definitions in English and French, with equivalent terms in additional languages. Also known as the International Electrotechnical Vocabulary online.

- Customer Service Centre: www.iec.ch/webstore/custserv

If you wish to give us your feedback on this publication or need further assistance, please visit the Customer Service Centre FAQ or contact us:
Email: csc@iec.ch
Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00

iTeh STANDARD PREVIEW
(standards.iteh.ai)
IEC 61508-3:2010
https://standards.iteh.ai/catalog/standards/sist/f6570ef4-4785-4a0c-bc73-35d31a657df6/iec-61508-3-2010

A propos de la CEI

La Commission Electrotechnique Internationale (CEI) est la première organisation mondiale qui élabore et publie des normes internationales pour tout ce qui a trait à l'électricité, à l'électronique et aux technologies apparentées.

A propos des publications CEI

Le contenu technique des publications de la CEI est constamment revu. Veuillez vous assurer que vous possédez l'édition la plus récente, un corrigendum ou amendement peut avoir été publié.

- Catalogue des publications de la CEI: www.iec.ch/searchpub/cur_fut-f.htm

Le Catalogue en-ligne de la CEI vous permet d'effectuer des recherches en utilisant différents critères (numéro de référence, texte, comité d'études,…). Il donne aussi des informations sur les projets et les publications retirées ou remplacées.

- Just Published CEI: www.iec.ch/online_news/justpub

Restez informé sur les nouvelles publications de la CEI. Just Published détaille deux fois par mois les nouvelles publications parues. Disponible en-ligne et aussi par email.

- Electropedia: www.electropedia.org

Le premier dictionnaire en ligne au monde de termes électroniques et électriques. Il contient plus de 20 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans les langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International en ligne.

- Service Clients: www.iec.ch/webstore/custserv/custserv_entry-f.htm

Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions, visitez le FAQ du Service clients ou contactez-nous:
Email: csc@iec.ch
Tél.: +41 22 919 02 11
Fax: +41 22 919 03 00

IEC 61508-3

Edition 2.0 2010-04

INTERNATIONAL STANDARD

NORME INTERNATIONALE

BASIC SAFETY PUBLICATION

PUBLICATION FONDAMENTALE DE SÉCURITÉ

iTeh STANDARD PREVIEW
(standards.iteh.ai)

Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 3: Software requirements

IEC 61508-3:2010
https://standards.iteh.ai/catalog/standards/sist/...-iec-61508-3-2010

Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 3: Exigences concernant les logiciels

INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMISSION ELECTROTECHNIQUE INTERNATIONALE

PRICE CODE
CODE PRIX XE

ICS 25.040.40

ISBN 978-2-88910-526-7

® Registered trademark of the International Electrotechnical Commission
Marque déposée de la Commission Electrotechnique Internationale

CONTENTS

FOREWORD 5
INTRODUCTION 7
1 Scope 9
2 Normative references 12
3 Definitions and abbreviations 13
4 Conformance to this standard 13
5 Documentation 13
6 Additional requirements for management of safety-related software 13
6.1 Objectives 13
6.2 Requirements 13
7 Software safety lifecycle requirements 14
7.1 General 14
7.1.1 Objective 14
7.1.2 Requirements 14
7.2 Software safety requirements specification 21
7.2.1 Objectives 21
7.2.2 Requirements 21
7.3 Validation plan for software aspects of system safety 24
7.3.1 Objective 24
7.3.2 Requirements 24
7.4 Software design and development 25
7.4.1 Objectives 25
7.4.2 General requirements 26
7.4.3 Requirements for software architecture design 29
7.4.4 Requirements for support tools, including programming languages 30
7.4.5 Requirements for detailed design and development – software system design 33
7.4.6 Requirements for code implementation 34
7.4.7 Requirements for software module testing 35
7.4.8 Requirements for software integration testing 35
7.5 Programmable electronics integration (hardware and software) 36
7.5.1 Objectives 36
7.5.2 Requirements 36
7.6 Software operation and modification procedures 37
7.6.1 Objective 37
7.6.2 Requirements 37
7.7 Software aspects of system safety validation 37
7.7.1 Objective 37
7.7.2 Requirements 38
7.8 Software modification 39
7.8.1 Objective 39
7.8.2 Requirements 39
7.9 Software verification 41
7.9.1 Objective 41
7.9.2 Requirements 41
8 Functional safety assessment 44

iTeh STANDARD PREVIEW
(standards.iteh.ai)
IEC 61508-3:2010
https://standards.iteh.ai/catalog/standards/sist/f6570ef1-4785-4a0e-bc73-35f5a657dfb/iec-61508-3-2010

Annex A (normative) Guide to the selection of techniques and measures 46
Annex B (informative) Detailed tables 55
Annex C (informative) Properties for software systematic capability 60
Annex D (normative) Safety manual for compliant items – additional requirements for software elements 97
Annex E (informative) Relationships between IEC 61508-2 and IEC 61508-3 100
Annex F (informative) Techniques for achieving non-interference between software elements on a single computer 102
Annex G (informative) Guidance for tailoring lifecycles associated with data driven systems 107
Bibliography 111

Figure 1 – Overall framework of the IEC 61508 series 11
Figure 2 – Overall safety lifecycle 12
Figure 3 – E/E/PE system safety lifecycle (in realisation phase) 16
Figure 4 – Software safety lifecycle (in realisation phase) 16
Figure 5 – Relationship and scope for IEC 61508-2 and IEC 61508-3 17
Figure 6 – Software systematic capability and the development lifecycle (the V-model) 17
Figure G.1 – Variability in complexity of data driven systems 108

Table 1 – Software safety lifecycle – overview 18
Table A.1 – Software safety requirements specification 47
Table A.2 – Software design and development – software architecture design 48
Table A.3 – Software design and development – support tools and programming language 49
Table A.4 – Software design and development – detailed design 50
Table A.5 – Software design and development – software module testing and integration 51
Table A.6 – Programmable electronics integration (hardware and software) 51
Table A.7 – Software aspects of system safety validation 52
Table A.8 – Modification 52
Table A.9 – Software verification 53
Table A.10 – Functional safety assessment 54
Table B.1 – Design and coding standards 55
Table B.2 – Dynamic analysis and testing 56
Table B.3 – Functional and black-box testing 56
Table B.4 – Failure analysis 57
Table B.5 – Modelling 57
Table B.6 – Performance testing 58
Table B.7 – Semi-formal methods 58
Table B.8 – Static analysis 59
Table B.9 – Modular approach 59
Table C.1 – Properties for systematic safety integrity – Software safety requirements specification 64

iTeh STANDARD PREVIEW
(standards.iteh.ai)
IEC 61508-3:2010
https://standards.iteh.ai/catalog/standards/sist/f6570ef4-4785-4a0c-bc73-[illegible]-iec-61508-3-2010

Table C.2 – Properties for systematic safety integrity – Software design and development – software Architecture Design 67
Table C.3 – Properties for systematic safety integrity – Software design and development – support tools and programming language 76
Table C.4 – Properties for systematic safety integrity – Software design and development – detailed design (includes software system design, software module design and coding) 77
Table C.5 – Properties for systematic safety integrity – Software design and development – software module testing and integration 79
Table C.6 – Properties for systematic safety integrity – Programmable electronics integration (hardware and software) 81
Table C.7 – Properties for systematic safety integrity – Software aspects of system safety validation 82
Table C.8 – Properties for systematic safety integrity – Software modification 83
Table C.9 – Properties for systematic safety integrity – Software verification 85
Table C.10 – Properties for systematic safety integrity – Functional safety assessment 86
Table C.11 – Detailed properties – Design and coding standards 87
Table C.12 – Detailed properties – Dynamic analysis and testing 89
Table C.13 – Detailed properties – Functional and black-box testing 90
Table C.14 – Detailed properties – Failure analysis 91
Table C.15 – Detailed properties – Modelling 92
Table C.16 – Detailed properties – Performance testing 93
Table C.17 – Detailed properties – Semi-formal methods 94
Table C.18 – Properties for systematic safety integrity – Static analysis 95
Table C.19 – Detailed properties – Modular approach 96
Table E.1 – Categories of IEC 61508-2 requirements 100
Table E.2 – Requirements of IEC 61508-2 for software and their typical relevance to certain types of software 100
Table F.1 – Module coupling – definition of terms 104
Table F.2 – Types of module coupling 105

iTeh STANDARD PREVIEW
(standards.iteh.ai)
IEC 61508-3:2010
https://standards.iteh.ai/catalog/standards/sist/f6570ef4-4785-4a0c-bc73-35d51ab57dfb/iec-61508-3-2010

INTERNATIONAL ELECTROTECHNICAL COMMISSION

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

Part 3: Software requirements

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
2) The formal decisions or agreements of IEC on technical matters express, as 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) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
IEC 61508-3:2010
https://standards.iteh.ai/catalog/standards/sist/f6570ef4-4785-4a0c-bc73-35d31a657dfb/iec-61508-3-2010

International Standard IEC 61508-3 has been prepared by subcommittee 65A: System aspects, of IEC technical committee 65: Industrial-process measurement, control and automation.

This second edition cancels and replaces the first edition published in 1998. This edition constitutes a technical revision.

This edition has been subject to a thorough review and incorporates many comments received at the various revision stages.

It has the status of a basic safety publication according to IEC Guide 104.

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

FDIS	Report on voting
65A/550/FDIS	65A/574/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 2.

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 publication will remain unchanged until the stability date indicated on the IEC web site under "http://webstore.iec.ch" in the data related to the specific publication. At this date, the publication will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
IEC 61508-3:2010
https://standards.iteh.ai/catalog/standards/sist/f6570ef4-4785-4a0c-bc73-35d31a657dfb/iec-61508-3-2010

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 International Standard 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 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 E/E/PE safety-related systems, it may also provide a framework within which safety-related systems based on other technologies may be considered.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
IEC 61508-3:2010
https://standards.iteh.ai/catalog/standards/sist/b570e4d-d5b5-4d0c-bc75-15431a6574f8/iec-61508-3-2010

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 International Standard, 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;

NOTE 2 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^{-1}];

NOTE 3 A single E/E/PE safety-related system does not necessarily mean a single-channel architecture.

NOTE 4 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 its confidence that the 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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
IEC 61508-3:2010
https://standards.iteh.ai/catalog/standards/sist/f6570ef4-4785-4a0c-bc73-35d31a657dfb/iec-61508-3-2010

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

Part 3: Software requirements

1 Scope

1.1 This part of the IEC 61508 series

a) is intended to be utilized only after a thorough understanding of IEC 61508-1 and IEC 61508-2;

b) applies to any software forming part of a safety-related system or used to develop a safety-related system within the scope of IEC 61508-1 and IEC 61508-2. Such software is termed safety-related software (including operating systems, system software, software in communication networks, human-computer interface functions, and firmware as well as application software);

c) provides specific requirements applicable to support tools used to develop and configure a safety-related system within the scope of IEC 61508-1 and IEC 61508-2;

d) requires that the software safety functions and software systematic capability are specified;

iTeh STANDARD PREVIEW
(standards.iteh.ai)

NOTE 1 If this has already been done as part of the specification of the E/E/PE safety-related systems (see 7.2 of IEC 61508-2), then it does not have to be repeated in this part.

NOTE 2 Specifying the software safety functions and software systematic capability is an iterative procedure; see Figures 3 and 6.

IEC 61508-3:2010
https://standards.iteh.ai/catalog/standards/sist/f6570ef4-4785-4a0c-bc73-35d5fab57dfb/iec-61508-3-2010

NOTE 3 See Clause 5 and Annex A of IEC 61508-1 for documentation structure. The documentation structure may take account of company procedures, and of the working practices of specific application sectors.

NOTE 4 Note: See 3.5.9 of IEC 61508-4 for definition of the term "systematic capability".

e) establishes requirements for safety lifecycle phases and activities which shall be applied during the design and development of the safety-related software (the software safety lifecycle model). These requirements include the application of measures and techniques, which are graded against the required systematic capability, for the avoidance of and control of faults and failures in the software;

f) provides requirements for information relating to the software aspects of system safety validation to be passed to the organisation carrying out the E/E/PE system integration;

g) provides requirements for the preparation of information and procedures concerning software needed by the user for the operation and maintenance of the E/E/PE safety-related system;

h) provides requirements to be met by the organisation carrying out modifications to safety-related software;

i) provides, in conjunction with IEC 61508-1 and IEC 61508-2, requirements for support tools such as development and design tools, language translators, testing and debugging tools, configuration management tools;

NOTE 4 Figure 5 shows the relationship between IEC 61508-2 and IEC 61508-3.

j) Does not apply for medical equipment in compliance with the IEC 60601 series.

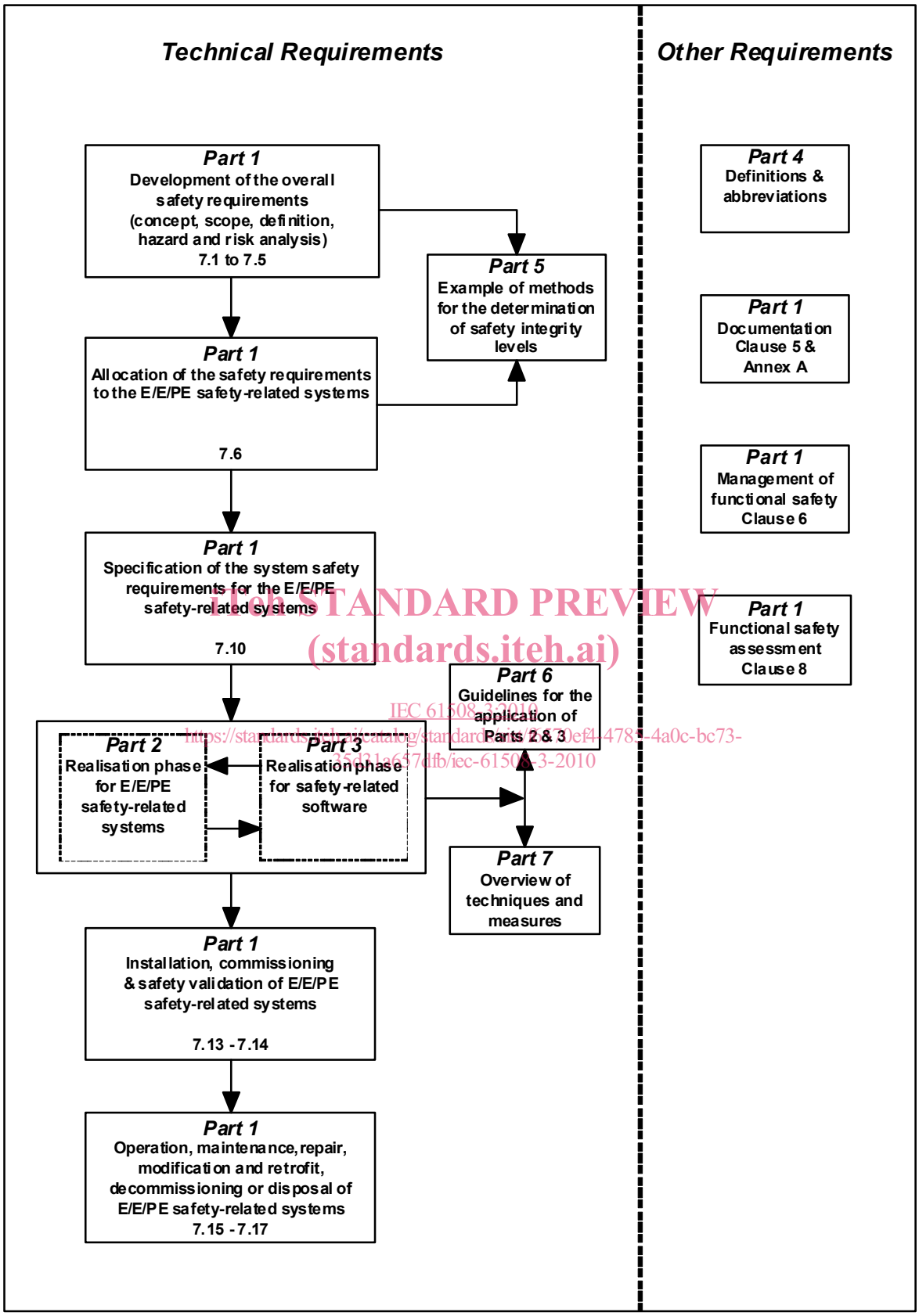
1.2 IEC 61508-1, IEC 61598-2, IEC 61508-3 and IEC 61508-4 are basic safety publications, although this status does not apply in the context of low complexity E/E/PE safety-related systems (see 3.4.3 of IEC 61508-4). As basic safety publications, they are intended for use by technical committees in the preparation of standards in accordance with the principles contained in IEC Guide 104 and ISO/IEC Guide 51. IEC 61508-1, IEC 61508-2, IEC 61508-3 and IEC 61508-4 are also intended for use as stand-alone publications. The horizontal safety

function of this international standard does not apply to medical equipment in compliance with the IEC 60601 series.

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.

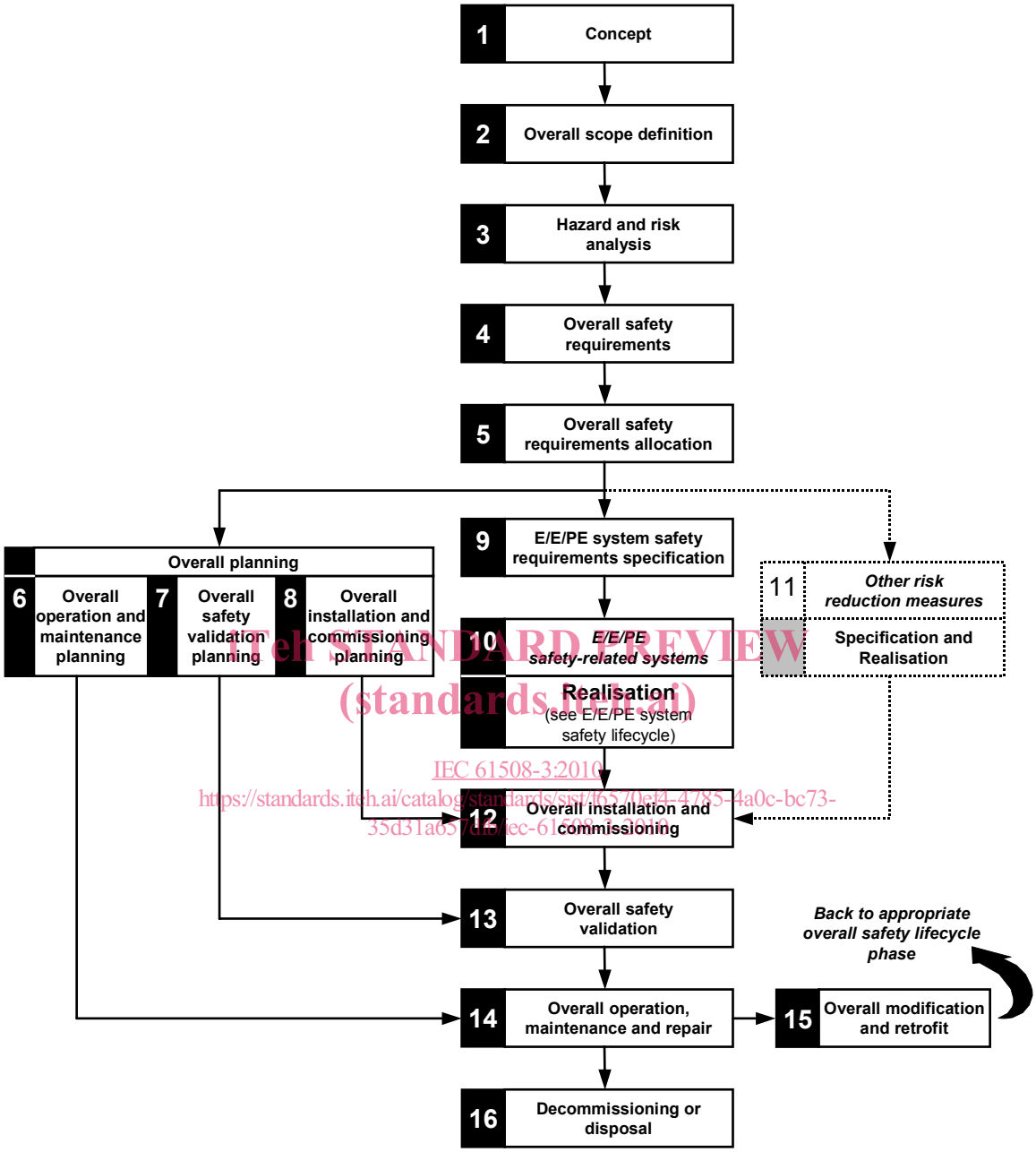
1.4 Figure 1 shows the overall framework of the IEC 61508 series and indicates the role that IEC 61508-3 plays in the achievement of functional safety for E/E/PE safety-related systems.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
IEC 61508-3:2010
https://standards.iteh.ai/catalog/standards/sist/f6570ef4-4785-4a0c-bc73-35d31a657dfb/iec-61508-3-2010



iTeh STANDARD PREVIEW
(standards.iteh.ai)
IEC 61508-3:2010
https://standards.iteh.ai/catalog/standards/sist/70ef4-4785-4a0c-bc73-35431a657dfb/iec-61508-3-2010

Figure 1 – Overall framework of the IEC 61508 series



iTeh STANDARD PREVIEW
(standards.iteh.ai)
IEC 61508-3:2010
https://standards.iteh.ai/catalog/standards/sist/f65706f4-4785-4a0c-bc73-35d31a657db8/iec-61508-3-2010

Figure 2 – Overall safety lifecycle

2 Normative references

The following referenced documents are indispensable for the application 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: 2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements*

IEC 61508-2: 2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems*

IEC 61508-4: 2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 4: Definitions and abbreviations*

IEC Guide 104:1997, *The preparation of safety publications and the use of basic safety publications and group safety publications*

IEC/ISO Guide 51:1999, *Safety aspects – Guidelines for their inclusion in standards*

3 Definitions and abbreviations

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

4 Conformance to this standard

The requirements for conformance to this standard are given in Clause 4 of IEC 61508-1.

5 Documentation

iTeh STANDARD PREVIEW
(standards.iteh.ai)

The objectives and requirements for documentation are given in Clause 5 of IEC 61508-1.

IEC 61508-3:2010
https://standards.iteh.ai/catalog/standards/sist/f6570ef4-4785-4a0c-bc73-35d31a657dfb/iec-61508-3-2010

6 Additional requirements for management of safety-related software

6.1 Objectives

The objectives are as detailed in 6.1 of IEC 61508-1.

6.2 Requirements

6.2.1 The requirements are as detailed in 6.2 of IEC 61508-1, with the following additional requirements.

6.2.2 The functional safety planning shall define the strategy for software procurement, development, integration, verification, validation and modification to the extent required by the safety integrity level of the safety functions implemented by the E/E/PE safety-related system.

NOTE The philosophy of this approach is to use the functional safety planning as an opportunity to customize this standard to take account of the required safety integrity for each safety function implemented by the E/E/PE safety-related system.

6.2.3 Software configuration management shall:

a) apply administrative and technical controls throughout the software safety lifecycle, in order to manage software changes and thus ensure that the specified requirements for safety-related software continue to be satisfied;

b) guarantee that all necessary operations have been carried out to demonstrate that the required software systematic capability has been achieved;

c) maintain accurately and with unique identification all configuration items which are necessary to meet the safety integrity requirements of the E/E/PE safety-related system. Configuration items include at least the following: safety analysis and requirements; software specification and design documents; software source code modules; test plans