

SS IEC 61508-6 : 2019
IEC 61508-6:2010, IDT
(ICS 25.040.40)

SINGAPORE STANDARD

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

– Part 6 : Guidelines on the application of SS IEC 61508-2
and SS IEC 61508-3

SS IEC 61508-6 : 2019
IEC 61508-6:2010, IDT
(ICS 25.040.40)

SINGAPORE STANDARD

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

– Part 6 : Guidelines on the application of SS IEC 61508-2 and SS IEC 61508-3

Published by Enterprise Singapore

All rights reserved. Unless otherwise specified, no part of this Singapore Standard may be reproduced or utilised in any form or by any means, electronic or mechanical, including photocopying and microfilming, without permission in writing from Enterprise Singapore. Request for permission can be sent to: standards@enterprisesg.gov.sg.

© IEC 2010 – All rights reserved
© Enterprise Singapore 2019

ISBN 978-981-48-9418-0

SS IEC 61508-6 : 2019

The content of this Singapore Standard was approved on 17 October 2019 by the Manufacturing Standards Committee (MSC) under the purview of the Singapore Standards Council.

First published, 2019

MSC consists of the following members:

	Name	Representation
Chairman	: Dr John Yong	<i>Individual Capacity</i>
Deputy Chairman	: Mr Brandon Lee	<i>Individual Capacity</i>
Secretary	: Mr Lee Wei Guo	<i>Singapore Manufacturing Federation – Standards Development Organisation</i>
Members	: Dr Karen Chong	<i>Science Engineering Research Council</i>
	Ms Fong Pin Fen	<i>Economic Development Board</i>
	Mr Goh Wee Hong	<i>TÜV SÜD PSB Pte Ltd</i>
	Mr Ho Chi Bao	<i>Enterprise Singapore</i>
	Mr Steven Koh	<i>Singapore Precision Engineering Technology Association</i>
	Ms Lee Wan Sie	<i>Infocomm Media Development Authority</i>
	Dr Jim Li Hui Hong	<i>Individual Capacity</i>
	Dr Lim Ee Meng	<i>National Metrology Centre</i>
	Er. Prof Seeram Ramakrishna	<i>The Institution of Engineers, Singapore</i>
	Mr Sze Thiam Siong	<i>Setsco Services Pte Ltd</i>

MSC sets up the Technical Committee on Smart Manufacturing to oversee the preparation of this standard. The Technical Committee consists of the following members:

	Name	Representation
Co-Chairmen	: Mr Yeoh Pit Wee	<i>Individual Capacity</i>
	Dr Tan Puay Siew	<i>Individual Capacity</i>
Secretary	: Mr Louis Lauw	<i>Singapore Manufacturing Federation – Standards Development Organisation</i>
Members	: Mr Ang Wee Seng	<i>Singapore Semiconductor Industry Association</i>
	Dr Ian Chan Hian Leng	<i>Singapore Institute of Manufacturing Technology</i>
	Mr Cheong Siah Chong	<i>Singapore Industrial Automation Association</i>
	Mr David Chia	<i>Beckhoff Automation Pte Ltd</i>
	Dr Andreas Hauser	<i>TÜV SÜD Asia Pacific Pte Ltd</i>
	Mr Sunny Khoo	<i>Toshiba TEC Singapore Pte Ltd</i>
	Mr Brandon Lee	<i>Singapore Manufacturing Federation</i>
	Prof Lee Loo Hay	<i>National University of Singapore</i>
	Mr Zach Lee	<i>Siemens Industry Software Pte Ltd</i>
	Mr Gerry Ong	<i>SMT Technology Pte Ltd</i>
	Prof John Pang	<i>Nanyang Technological University</i>

Members	:	Er. Prof Seeram Ramakrishna	<i>The Institution of Engineers, Singapore</i>
		Mr Sim Bak Chor	<i>Infocomm Media Development Authority</i>
		Mr Tian Boon Quey	<i>TRUMPF Pte Ltd</i>
		Mr Toh Hong Wee	<i>PBA Systems Pte Ltd</i>
		Dr Carlos Toro	<i>Advanced Remanufacturing Technology Centre</i>

The Technical Committee sets up the Working Group on Smart Manufacturing Readiness Level to prepare this standard. The Working Group consists of the following experts who contribute in their *individual capacity*:

	Name
Co-Convenors	: Mr Brandon Lee Mr Shridhar Ravikumar
Secretary	: Mr Louis Lauw
Members	: Dr Ian Chan Hian Leng Mr Cheong Siah Chong Mr David Chia Dr Andreas Hauser Mr Michael Leong Dr Lin Wei Dr Gary Ng Prof John Pang Dr Tan Puay Siew Mr Yeoh Pit Wee

The organisations in which the experts of the Working Group are involved are:

Advanced Remanufacturing Technology Centre
Beckhoff Automation Pte Ltd
INTECH Process Automation Pte Ltd
Nanyang Technological University
Rockwell Automation Southeast Asia Pte Ltd
SESTO Robotics Pte Ltd
Singapore Industrial Automation Association
Singapore Institute of Manufacturing Technology
TÜV SÜD Asia Pacific Pte Ltd

(blank page)

CONTENTS

NATIONAL FOREWORD	9
FOREWORD	10
INTRODUCTION	12
1 Scope	14
2 Normative references	16
3 Definitions and abbreviations	16
Annex A (informative) Application of IEC 61508-2 and of IEC 61508-3	17
Annex B (informative) Example of technique for evaluating probabilities of hardware failure	25
Annex C (informative) Calculation of diagnostic coverage and safe failure fraction – worked example	79
Annex D (informative) A methodology for quantifying the effect of hardware-related common cause failures in E/E/PE systems	83
Annex E (informative) Example applications of software safety integrity tables of IEC 61508-3	97
Bibliography	112
Figure 1 – Overall framework of the IEC 61508 series	15
Figure A.1 – Application of IEC 61508-2	21
Figure A.2 – Application of IEC 61508-2 (Figure A.1 <i>continued</i>)	22
Figure A.3 – Application of IEC 61508-3	24
Figure B.1 – Reliability Block Diagram of a whole safety loop	26
Figure B.2 – Example configuration for two sensor channels	30
Figure B.3 – Subsystem structure	33
Figure B.4 – 1oo1 physical block diagram	34
Figure B.5 – 1oo1 reliability block diagram	34
Figure B.6 – 1oo2 physical block diagram	35
Figure B.7 – 1oo2 reliability block diagram	36
Figure B.8 – 2oo2 physical block diagram	36
Figure B.9 – 2oo2 reliability block diagram	36
Figure B.10 – 1oo2D physical block diagram	37
Figure B.11 – 1oo2D reliability block diagram	37
Figure B.12 – 2oo3 physical block diagram	38
Figure B.13 – 2oo3 reliability block diagram	38
Figure B.14 – Architecture of an example for low demand mode of operation	44
Figure B.15 – Architecture of an example for high demand or continuous mode of operation	53
Figure B.16 – Reliability block diagram of a simple whole loop with sensors organised into 2oo3 logic	55
Figure B.17 – Simple fault tree equivalent to the reliability block diagram presented on Figure B.1	56

Figure B.18 – Equivalence fault tree / reliability block diagram 56

Figure B.19 – Instantaneous unavailability $U(t)$ of single periodically tested components 58

Figure B.20 – Principle of $PF_{D_{avg}}$ calculations when using fault trees 59

Figure B.21 – Effect of staggering the tests 60

Figure B.22 – Example of complex testing pattern 60

Figure B.23 – Markov graph modelling the behaviour of a two component system 62

Figure B.24 – Principle of the multiphase Markovian modelling 63

Figure B.25 – Saw-tooth curve obtained by multiphase Markovian approach 64

Figure B.26 – Approximated Markovian model 64

Figure B.27 – Impact of failures due to the demand itself 65

Figure B.28 – Modelling of the impact of test duration 65

Figure B.29 – Multiphase Markovian model with both DD and DU failures 66

Figure B.30 – Changing logic (2oo3 to 1oo2) instead of repairing first failure 67

Figure B.31 – "Reliability" Markov graphs with an absorbing state 67

Figure B.32 – "Availability" Markov graphs without absorbing states 69

Figure B.33 – Petri net for modelling a single periodically tested component 70

Figure B.34 – Petri net to model common cause failure and repair resources 73

Figure B.35 – Using reliability block diagrams to build Petri net and auxiliary Petri net for PF_{D} and PF_{H} calculations 74

Figure B.36 – Simple Petri net for a single component with revealed failures and repairs 75

Figure B.37 – Example of functional and dysfunctional modelling with a formal language 76

Figure B.38 – Uncertainty propagation principle 77

Figure D.1 – Relationship of common cause failures to the failures of individual channels ... 85

Figure D.2 – Implementing shock model with fault trees 95

Table B.1 – Terms and their ranges used in this annex (applies to 1oo1, 1oo2, 2oo2, 1oo2D, 1oo3 and 2oo3) 31

Table B.2 – Average probability of failure on demand for a proof test interval of six months and a mean time to restoration of 8 h 39

Table B.3 – Average probability of failure on demand for a proof test interval of one year and mean time to restoration of 8 h 41

Table B.4 – Average probability of failure on demand for a proof test interval of two years and a mean time to restoration of 8 h 42

Table B.5 – Average probability of failure on demand for a proof test interval of ten years and a mean time to restoration of 8 h 43

Table B.6 – Average probability of failure on demand for the sensor subsystem in the example for low demand mode of operation (one year proof test interval and 8 h $MTTR$).... 44

Table B.7 – Average probability of failure on demand for the logic subsystem in the example for low demand mode of operation (one year proof test interval and 8 h $MTTR$).... 45

Table B.8 – Average probability of failure on demand for the final element subsystem in the example for low demand mode of operation (one year proof test interval and 8 h $MTTR$).... 45

Table B.9 – Example for a non-perfect proof test 47

Table B.10 – Average frequency of a dangerous failure (in high demand or continuous mode of operation) for a proof test interval of one month and a mean time to restoration of 8 h	49
Table B.11 – Average frequency of a dangerous failure (in high demand or continuous mode of operation) for a proof test interval of three month and a mean time to restoration of 8 h	50
Table B.12 – Average frequency of a dangerous failure (in high demand or continuous mode of operation) for a proof test interval of six month and a mean time to restoration of 8 h	51
Table B.13 – Average frequency of a dangerous failure (in high demand or continuous mode of operation) for a proof test interval of one year and a mean time to restoration of 8 h	52
Table B.14 – Average frequency of a dangerous failure for the sensor subsystem in the example for high demand or continuous mode of operation (six month proof test interval and 8 h <i>MTTR</i>)	53
Table B.15 – Average frequency of a dangerous failure for the logic subsystem in the example for high demand or continuous mode of operation (six month proof test interval and 8 h <i>MTTR</i>)	54
Table B.16 – Average frequency of a dangerous failure for the final element subsystem in the example for high demand or continuous mode of operation (six month proof test interval and 8 h <i>MTTR</i>)	54
Table C.1 – Example calculations for diagnostic coverage and safe failure fraction	81
Table C.2 – Diagnostic coverage and effectiveness for different elements	82
Table D.1 – Scoring programmable electronics or sensors/final elements	90
Table D.2 – Value of <i>Z</i> – programmable electronics	91
Table D.3 – Value of <i>Z</i> – sensors or final elements	91
Table D.4 – Calculation of β_{int} or $\beta_{D int}$	92
Table D.5 – Calculation of β for systems with levels of redundancy greater than 1oo2	93
Table D.6 – Example values for programmable electronics	94
Table E.1 – Software safety requirements specification	98
Table E.2 – Software design and development – software architecture design	99
Table E.3 – Software design and development – support tools and programming language	100
Table E.4 – Software design and development – detailed design	101
Table E.5 – Software design and development – software module testing and integration ..	102
Table E.6 – Programmable electronics integration (hardware and software)	102
Table E.7 – Software aspects of system safety validation	103
Table E.8 – Software modification	103
Table E.9 – Software verification	104
Table E.10 – Functional safety assessment	104
Table E.11 – Software safety requirements specification	106
Table E.12 – Software design and development – software architecture design	106
Table E.13 – Software design and development – support tools and programming language	107
Table E.14 – Software design and development – detailed design	108

Table E.15 – Software design and development – software module testing and integration	108
Table E.16 – Programmable electronics integration (hardware and software)	109
Table E.17 – Software aspects of system safety validation	110
Table E.18 – Modification	110
Table E.19 – Software verification	111
Table E.20 – Functional safety assessment	111

National Foreword

This Singapore Standard was prepared by the Working Group on Smart Manufacturing Readiness Level set up by the Technical Committee on Smart Manufacturing under the purview of MSC.

This standard is identical with IEC 61508-6:2010, “Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3”, published by the International Electrotechnical Commission.

NOTE 1 – Where appropriate, the words “International Standard” are read as “Singapore Standard”.

NOTE 2 – Reference to International Standards are replaced by applicable Singapore Standards and Technical References.

NOTE 3 – Where numerical values are expressed as decimals, the comma is read as a full point.

This standard is expected to be used by system integrators, government agencies, testing, inspection and certification bodies, professional institutions, institutes of higher learning and training providers.

Attention is drawn to the possibility that some of the elements of this Singapore Standard may be the subject of patent rights. Enterprise Singapore shall not be held responsible for identifying any or all of such patent rights.

NOTE

- 1. Singapore Standards (SSs) and Technical References (TRs) are reviewed periodically to keep abreast of technical changes, technological developments and industry practices. The changes are documented through the issue of either amendments or revisions. Where SSs are deemed to be stable, i.e. no foreseeable changes in them, they will be classified as “Mature Standards”. Mature Standards will not be subject to further review, unless there are requests to review such standards.*
- 2. An SS or TR is voluntary in nature except when it is made mandatory by a regulatory authority. It can also be cited in contracts making its application a business necessity. Users are advised to assess and determine whether the SS or TR is suitable for their intended use or purpose. If required, they should refer to the relevant professionals or experts for advice on the use of the document. Enterprise Singapore and the Singapore Standards Council shall not be liable for any damages whether directly or indirectly suffered by anyone or any organisation as a result of the use of any SS or TR. Although care has been taken to draft this standard, users are also advised to ensure that they apply the information after due diligence.*
- 3. Compliance with a SS or TR does not exempt users from any legal obligations.*

INTERNATIONAL ELECTROTECHNICAL COMMISSION

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

**Part 6: Guidelines on the application
of IEC 61508-2 and IEC 61508-3**

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.

International Standard IEC 61508-6 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 2000. 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.

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

FDIS	Report on voting
65A/553/FDIS	65A/577/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.

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.

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.

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.

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

**Part 6: Guidelines on the application
of IEC 61508-2 and IEC 61508-3**

1 Scope

1.1 This part of IEC 61508 contains information and guidelines on IEC 61508-2 and IEC 61508-3.

- Annex A gives a brief overview of the requirements of IEC 61508-2 and IEC 61508-3 and sets out the functional steps in their application.
- Annex B gives an example technique for calculating the probabilities of hardware failure and should be read in conjunction with 7.4.3 and Annex C of IEC 61508-2 and Annex D.
- Annex C gives a worked example of calculating diagnostic coverage and should be read in conjunction with Annex C of IEC 61508-2.
- Annex D gives a methodology for quantifying the effect of hardware-related common cause failures on the probability of failure.
- Annex E gives worked examples of the application of the software safety integrity tables specified in Annex A of IEC 61508-3 for safety integrity levels 2 and 3.

1.2 IEC 61508-1, IEC 61508-2, IEC 61508-3 and IEC 61508-4 are basic safety publications, although this status does not apply in the context of low complexity E/E/PE safety-related systems (see 3.4.3 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 61508-6 plays in the achievement of functional safety for E/E/PE safety-related systems.

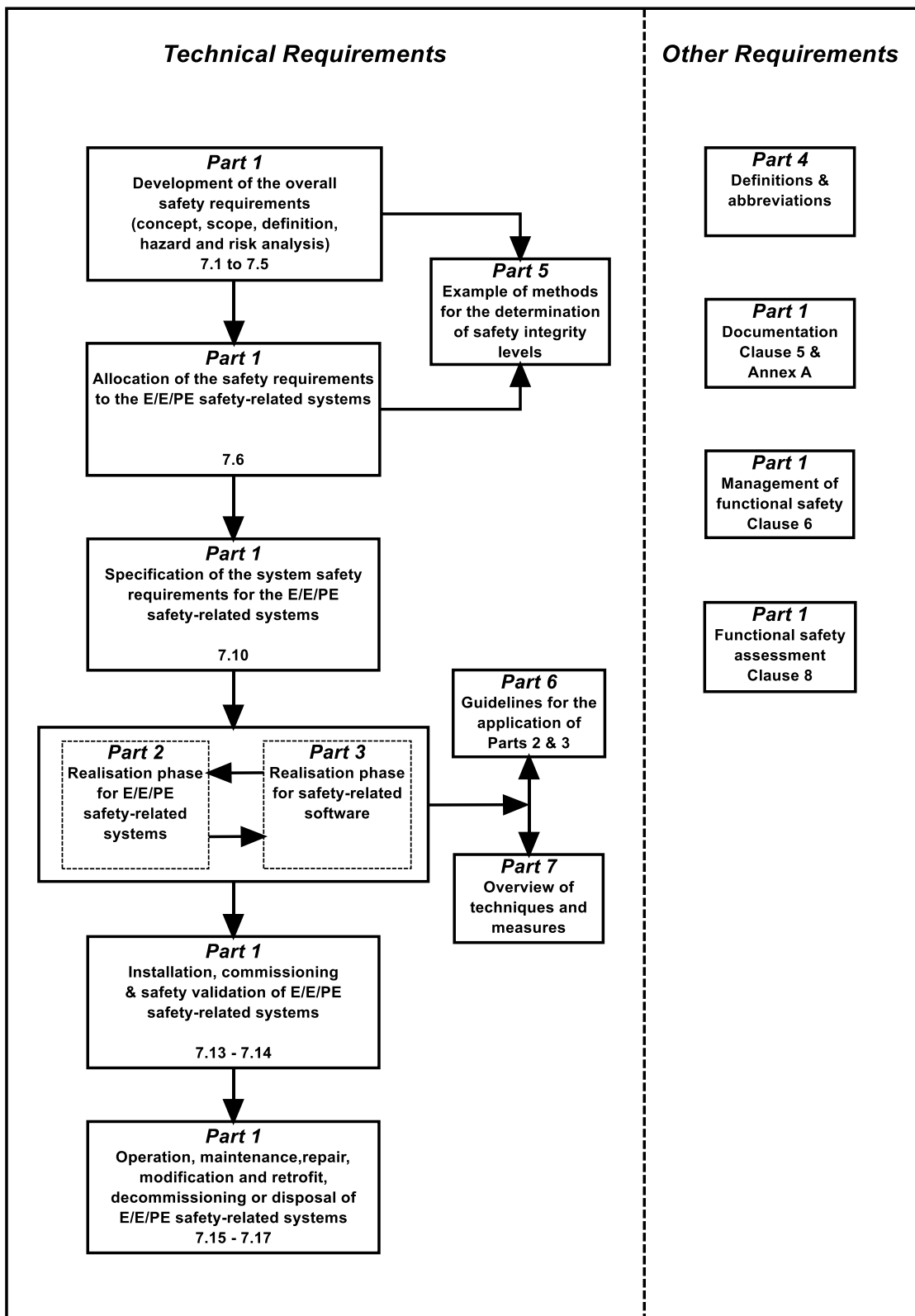


Figure 1 – Overall framework of the IEC 61508 series

2 Normative references

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

IEC 61508-3:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 3: Software requirements*

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