

INTERNATIONAL STANDARD

NORME INTERNATIONALE

**Functional safety of electrical/electronic/programmable electronic
safety-related systems –
Part 7: Overview of techniques and measures**

**Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques
programmables relatifs à la sécurité –
Partie 7: Présentation de techniques et mesures**

<https://standards.iteh.ai/en/standards/iec/4d69740-ca18-40f7-8f62-52f6d6ef7719/iec-61508-7-2000>

WATERM



THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2000 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 Varembe
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 It also gives information on projects, withdrawn and replaced publications.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

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

INTERNATIONAL STANDARD

NORME INTERNATIONALE

**Functional safety of electrical/electronic/programmable electronic
safety-related systems –
Part 7: Overview of techniques and measures**

**Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques
programmables relatifs à la sécurité –
Partie 7: Présentation de techniques et mesures**

<https://standards.iteh.ai/en/standards/iec/4d69740-ca18-40f7-8f62-52f6d6ef7719/iec-61508-7-2000>

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

PRICE CODE
CODE PRIX

XE

CONTENTS

	Page
FOREWORD.....	8
INTRODUCTION.....	10
Clause	
1 Scope.....	12
2 Normative references.....	14
3 Definitions and abbreviations.....	14
Annex A (informative) Overview of techniques and measures for E/E/PES: control of random hardware failures (see IEC 61508-2).....	15
A.1 Electrical.....	15
A.1.1 Failure detection by on-line monitoring.....	15
A.1.2 Monitoring of relay contacts.....	15
A.1.3 Comparator.....	15
A.1.4 Majority voter.....	16
A.1.5 Idle current principle (de-energised to trip).....	16
A.2 Electronic.....	16
A.2.1 Tests by redundant hardware.....	16
A.2.2 Dynamic principles.....	17
A.2.3 Standard test access port and boundary-scan architecture.....	17
A.2.4 Fail-safe hardware.....	17
A.2.5 Monitored redundancy.....	18
A.2.6 Electrical/electronic components with automatic check.....	18
A.2.7 Analogue signal monitoring.....	18
A.2.8 De-rating.....	19
A.3 Processing units.....	19
A.3.1 Self-test by software: limited number of patterns (one-channel).....	19
A.3.2 Self-test by software: walking bit (one-channel).....	19
A.3.3 Self-test supported by hardware (one-channel).....	19
A.3.4 Coded processing (one-channel).....	20
A.3.5 Reciprocal comparison by software.....	20
A.4 Invariable memory ranges.....	20
A.4.1 Word-saving multi-bit redundancy (for example ROM monitoring with a modified Hamming code).....	20
A.4.2 Modified checksum.....	21
A.4.3 Signature of one word (8-bit).....	21
A.4.4 Signature of a double word (16-bit).....	21
A.4.5 Block replication (for example double ROM with hardware or software comparison).....	22
A.5 Variable memory ranges.....	22
A.5.1 RAM test "checkerboard" or "march".....	22
A.5.2 RAM test "walkpath".....	23
A.5.3 RAM test "galpat" or "transparent galpat".....	23
A.5.4 RAM test "Abraham".....	24
A.5.5 One-bit redundancy (for example RAM monitoring with a parity bit).....	24
A.5.6 RAM monitoring with a modified Hamming code, or detection of data failures with error-detection-correction codes (EDC).....	24
A.5.7 Double RAM with hardware or software comparison and read/write test.....	25

Clause	Page
A.6 I/O-units and interfaces (external communication)	25
A.6.1 Test pattern.....	25
A.6.2 Code protection.....	25
A.6.3 Multi-channel parallel output	26
A.6.4 Monitored outputs	26
A.6.5 Input comparison/voting	27
A.7 Data paths (internal communication)	27
A.7.1 One-bit hardware redundancy.....	27
A.7.2 Multi-bit hardware redundancy	27
A.7.3 Complete hardware redundancy	27
A.7.4 Inspection using test patterns	28
A.7.5 Transmission redundancy	28
A.7.6 Information redundancy	28
A.8 Power supply.....	28
A.8.1 Overvoltage protection with safety shut-off	28
A.8.2 Voltage control (secondary)	29
A.8.3 Power-down with safety shut-off	29
A.9 Temporal and logical program sequence monitoring.....	29
A.9.1 Watch-dog with separate time base without time-window	29
A.9.2 Watch-dog with separate time base and time-window.....	30
A.9.3 Logical monitoring of program sequence	30
A.9.4 Combination of temporal and logical monitoring of program sequences	30
A.9.5 Temporal monitoring with on-line check.....	30
A.10 Ventilation and heating.....	31
A.10.1 Temperature sensor.....	31
A.10.2 Fan control.....	31
A.10.3 Actuation of the safety shut-off via thermal fuse.....	31
A.10.4 Staggered message from thermo-sensors and conditional alarm.....	31
A.10.5 Connection of forced-air cooling and status indication	31
A.11 Communication and mass-storage	32
A.11.1 Separation of electrical energy lines from information lines	32
A.11.2 Spatial separation of multiple lines.....	32
A.11.3 Increase of interference immunity	32
A.11.4 Antivalent signal transmission	33
A.12 Sensors.....	33
A.12.1 Reference sensor.....	33
A.12.2 Positive-activated switch	33
A.13 Final elements (actuators).....	33
A.13.1 Monitoring	33
A.13.2 Cross-monitoring of multiple actuators.....	34
A.14 Measures against the physical environment.....	34
Annex B (informative) Overview of techniques and measures for E/E/PES: avoidance of systematic failures (see IEC 61508-2 and IEC 61508-3).....	35
B.1 General measures and techniques.....	35
B.1.1 Project management.....	35
B.1.2 Documentation.....	36
B.1.3 Separation of safety-related systems from non-safety-related systems	37
B.1.4 Diverse hardware	37

Clause	Page
B.2 E/E/PES safety requirements specification	38
B.2.1 Structured specification.....	38
B.2.2 Formal methods	38
B.2.3 Semi-formal methods	39
B.2.3.1 General	39
B.2.3.2 Finite state machines/state transition diagrams.....	39
B.2.3.3 Time Petri nets	40
B.2.4 Computer-aided specification tools	40
B.2.4.1 General	40
B.2.4.2 Tools oriented towards no specific method	41
B.2.4.3 Model orientated procedure with hierarchical analysis	41
B.2.4.4 Entity models.....	41
B.2.4.5 Incentive and answer	42
B.2.5 Checklists	42
B.2.6 Inspection of the specification	43
B.3 E/E/PES design and development.....	43
B.3.1 Observance of guidelines and standards	43
B.3.2 Structured design.....	44
B.3.3 Use of well-tried components	45
B.3.4 Modularisation.....	45
B.3.5 Computer-aided design tools	46
B.3.6 Simulation	46
B.3.7 Inspection (reviews and analysis)	46
B.3.8 Walk-through.....	47
B.4 E/E/PES operation and maintenance procedures	47
B.4.1 Operation and maintenance instructions	47
B.4.2 User friendliness	48
B.4.3 Maintenance friendliness	48
B.4.4 Limited operation possibilities	48
B.4.5 Operation only by skilled operators	49
B.4.6 Protection against operator mistakes	49
B.4.7 (Not used)	49
B.4.8 Modification protection	49
B.4.9 Input acknowledgement	49
B.5 E/E/PES integration.....	50
B.5.1 Functional testing.....	50
B.5.2 Black-box testing.....	50
B.5.3 Statistical testing	51
B.5.4 Field experience.....	51
B.6 E/E/PES safety validation.....	52
B.6.1 Functional testing under environmental conditions.....	52
B.6.2 Interference surge immunity testing	53
B.6.3 (Not used)	53
B.6.4 Static analysis	53
B.6.5 Dynamic analysis	54

Clause	Page
B.6.6 Failure analysis	54
B.6.6.1 Failure modes and effects analysis	54
B.6.6.2 Cause consequence diagrams	55
B.6.6.3 Event tree analysis	55
B.6.6.4 Failure modes, effects and criticality analysis.....	55
B.6.6.5 Fault tree analysis	56
B.6.7 Worst-case analysis.....	56
B.6.8 Expanded functional testing	56
B.6.9 Worst-case testing	57
B.6.10 Fault insertion testing.....	57
Annex C (informative) Overview of techniques and measures for achieving software safety integrity (see IEC 61508-3)	58
C.1 General	58
C.2 Requirements and detailed design	58
C.2.1 Structured methods.....	58
C.2.1.1 General	58
C.2.1.2 CORE – Controlled Requirements Expression.....	59
C.2.1.3 JSD – Jackson System Development.....	59
C.2.1.4 MASCOT – Modular Approach to Software Construction, Operation and Test.....	60
C.2.1.5 Real-time Yourdon.....	60
C.2.1.6 SADT – Structured Analysis and Design Technique.....	61
C.2.2 Data flow diagrams	62
C.2.3 Structure diagrams.....	63
C.2.4 Formal methods.....	63
C.2.4.1 General	63
C.2.4.2 CCS – Calculus of Communicating Systems.....	64
C.2.4.3 CSP – Communicating Sequential Processes.....	64
C.2.4.4 HOL – Higher Order Logic.....	65
C.2.4.5 LOTOS.....	65
C.2.4.6 OBJ.....	65
C.2.4.7 Temporal logic.....	66
C.2.4.8 VDM, VDM++ – Vienna Development Method.....	67
C.2.4.9 Z.....	68
C.2.5 Defensive programming	69
C.2.6 Design and coding standards.....	70
C.2.6.1 General	70
C.2.6.2 Coding standards	70
C.2.6.3 No dynamic variables or dynamic objects	71
C.2.6.4 On-line checking during creation of dynamic variables or dynamic objects	71
C.2.6.5 Limited use of interrupts	71
C.2.6.6 Limited use of pointers	72
C.2.6.7 Limited use of recursion	72
C.2.7 Structured programming	72
C.2.8 Information hiding/encapsulation.....	73
C.2.9 Modular approach	74
C.2.10 Use of trusted/verified software modules and components	74

Clause	Page	
C.3	Architecture design.....	75
C.3.1	Fault detection and diagnosis	75
C.3.2	Error detecting and correcting codes	76
C.3.3	Failure assertion programming.....	76
C.3.4	Safety bag.....	77
C.3.5	Software diversity (diverse programming)	77
C.3.6	Recovery block	78
C.3.7	Backward recovery.....	79
C.3.8	Forward recovery	79
C.3.9	Re-try fault recovery mechanisms.....	79
C.3.10	Memorising executed cases.....	80
C.3.11	Graceful degradation.....	80
C.3.12	Artificial intelligence fault correction	81
C.3.13	Dynamic reconfiguration	81
C.4	Development tools and programming languages.....	82
C.4.1	Strongly typed programming languages.....	82
C.4.2	Language subsets.....	82
C.4.3	Certified tools and certified translators.....	83
C.4.4	Tools and translators: increased confidence from use	83
C.4.4.1	Comparison of source program and executable code	84
C.4.5	Library of trusted/verified software modules and components.....	84
C.4.6	Suitable programming languages.....	85
C.5	Verification and modification.....	88
C.5.1	Probabilistic testing.....	88
C.5.2	Data recording and analysis.....	89
C.5.3	Interface testing	89
C.5.4	Boundary value analysis.....	89
C.5.5	Error guessing.....	90
C.5.6	Error seeding	90
C.5.7	Equivalence classes and input partition testing.....	91
C.5.8	Structure-based testing.....	91
C.5.9	Control flow analysis.....	92
C.5.10	Data flow analysis.....	93
C.5.11	Sneak circuit analysis.....	93
C.5.12	Symbolic execution	94
C.5.13	Formal proof.....	94
C.5.14	Complexity metrics.....	95
C.5.15	Fagan inspections.....	95
C.5.16	Walk-throughs/design reviews	96
C.5.17	Prototyping/animation	96
C.5.18	Process simulation.....	97
C.5.19	Performance requirements.....	97
C.5.20	Performance modelling	98
C.5.21	Avalanche/stress testing.....	98
C.5.22	Response timing and memory constraints	99
C.5.23	Impact analysis	99
C.5.24	Software configuration management.....	100

Clause	Page
C.6 Functional safety assessment	100
C.6.1 Decision tables (truth tables).....	100
C.6.2 Hazard and Operability Study (HAZOP).....	100
C.6.3 Common cause failure analysis	102
C.6.4 Markov models.....	102
C.6.5 Reliability block diagrams.....	103
C.6.6 Monte-Carlo simulation	104
Annex D (informative) A probabilistic approach to determining software safety integrity for pre-developed software.....	105
D.1 General	105
D.2 Statistical testing formulae and examples of their use.....	106
D.2.1 Simple statistical test for low demand mode of operation.....	106
D.2.1.1 Prerequisites	106
D.2.1.2 Results	106
D.2.1.3 Example	106
D.2.2 Testing of an input space (domain) for a low demand mode of operation	106
D.2.2.1 Prerequisites	106
D.2.2.2 Results	106
D.2.2.3 Example	107
D.2.3 Simple statistical test for high demand or continuous mode of operation	107
D.2.3.1 Prerequisites	107
D.2.3.2 Results	107
D.2.3.3 Example	108
D.2.4 Complete test.....	108
D.2.4.1 Prerequisites	108
D.2.4.2 Results	108
D.2.4.3 Example	109
D.3 References	109
Bibliography	110
Index	112
Table C.1 – Recommendations for specific programming languages	87
Table D.1 – Necessary history for confidence to safety integrity levels	105
Table D.2 – Probabilities of failure for low demand mode of operation.....	106
Table D.3 – Mean distances of two test points.....	107
Table D.4 – Probabilities of failure for high demand or continuous mode of operation	108
Table D.5 – Probability of testing all program properties.....	109

INTERNATIONAL ELECTROTECHNICAL COMMISSION

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

Part 7: Overview of techniques and measures

FOREWORD

- 1) The IEC (International Electrotechnical Commission) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of the IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, the IEC publishes International Standards. Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. The IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
- 2) The formal decisions or agreements of the IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested National Committees.
- 3) The documents produced have the form of recommendations for international use and are published in the form of standards, technical specifications, technical reports or guides and they are accepted by the National Committees in that sense.
- 4) In order to promote international unification, IEC National Committees undertake to apply IEC International Standards transparently to the maximum extent possible in their national and regional standards. Any divergence between the IEC Standard and the corresponding national or regional standard shall be clearly indicated in the latter.
- 5) The IEC provides no marking procedure to indicate its approval and cannot be rendered responsible for any equipment declared to be in conformity with one of its standards.
- 6) Attention is drawn to the possibility that some of the elements of this International Standard may be the subject of patent rights. The IEC shall not be held responsible for identifying any or all such patent rights.

International Standard IEC 61508-7 has been prepared by subcommittee 65A: System aspects, of IEC technical committee 65: Industrial-process measurement and control.

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

FDIS	Report on voting
65A/293/FDIS	65A/299/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 3.

Annexes A, B, C and D are for information only.

IEC 61508 consists of the following parts, under the general title *Functional safety of electrical/electronic/programmable electronic safety-related systems*:

- Part 1: General requirements
- Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems
- Part 3: Software requirements
- Part 4: Definitions and abbreviations
- Part 5: Examples of methods for the determination of safety integrity levels
- Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3
- Part 7: Overview of techniques and measures

The committee has decided that the contents of this publication will remain unchanged until 2006. At this date, the publication will be

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

iTech Standards
(<https://standards.iteh.ai>)
Document Preview

<https://standards.iteh.ai> IEC 61508-7:2000

<https://standards.iteh.ai/standards/iec/4d69740-ca18-40f7-8f62-52f6d6ef7719/iec-61508-7-2000>

INTRODUCTION

Systems comprised of electrical and/or electronic components have been used for many years to perform safety functions in most application sectors. Computer-based systems (generically referred to as programmable electronic systems (PESs)) are being used in all application sectors to perform non-safety functions and, increasingly, to perform safety functions. If computer system technology is to be effectively and safely exploited, it is essential that those responsible for making decisions have sufficient guidance on the safety aspects on which to make those decisions.

This International Standard sets out a generic approach for all safety lifecycle activities for systems comprised of electrical and/or electronic and/or programmable electronic components (electrical/electronic/programmable electronic systems (E/E/PESs)) that are used to perform safety functions. This unified approach has been adopted in order that a rational and consistent technical policy be developed for all electrically based safety-related systems. A major objective is to facilitate the development of application sector standards.

In most situations, safety is achieved by a number of protective systems which rely on many technologies (for example mechanical, hydraulic, pneumatic, electrical, electronic, programmable electronic). Any safety strategy must therefore consider not only all the elements within an individual system (for example sensors, controlling devices and actuators) but also all the safety-related systems making up the total combination of safety-related systems. Therefore, while this International Standard is concerned with electrical/electronic/programmable electronic (E/E/PE) safety-related systems, it may also provide a framework within which safety-related systems based on other technologies may be considered.

It is recognised that there is a great variety of E/E/PES applications in a variety of application sectors and covering a wide range of complexity, hazard and risk potentials. In any particular application, the exact prescription of safety measures will be dependent on many factors specific to the application. This International Standard, by being generic, will enable such a prescription to be formulated in future application sector International Standards.

This International Standard

- considers all relevant overall, E/E/PES and software safety lifecycle phases (for example, from initial concept, through design, implementation, operation and maintenance to decommissioning) when E/E/PESs are used to perform safety functions;
- has been conceived with a rapidly developing technology in mind; the framework is sufficiently robust and comprehensive to cater for future developments;
- enables application sector International Standards, dealing with safety-related E/E/PESs, to be developed; the development of application sector international standards, within the framework of this standard, should lead to a high level of consistency (for example, of underlying principles, terminology, etc.) both within application sectors and across application sectors; this will have both safety and economic benefits;
- provides a method for the development of the safety requirements specification necessary to achieve the required functional safety for E/E/PE safety-related systems;

- uses safety integrity levels for specifying the target level of safety integrity for the safety functions to be implemented by the E/E/PE safety-related systems;
- adopts a risk-based approach for the determination of the safety integrity level requirements;
- sets numerical target failure measures for E/E/PE safety-related systems which are linked to the safety integrity levels;
- sets a lower limit on the target failure measures, in a dangerous mode of failure, that can be claimed for a single E/E/PE safety-related system; for E/E/PE safety-related systems operating in
 - a low demand mode of operation, the lower limit is set at an average probability of failure of 10^{-5} to perform its design function on demand;
 - a high demand or continuous mode of operation, the lower limit is set at a probability of a dangerous failure of 10^{-9} per hour;

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

- adopts a broad range of principles, techniques and measures to achieve functional safety for E/E/PE safety-related systems, but does not rely on the concept of fail-safe, which may be of value when the failure modes are well defined and the level of complexity is relatively low – the concept of fail-safe was considered inappropriate because of the full range of complexity of E/E/PE safety-related systems that are within the scope of the standard.

iTech Standards
(<https://standards.iteh.ai>)
Document Preview

IEC 61508-7:2000

<https://standards.iteh.ai/doc/standards/iec/4469740-ca18-40f7-8f62-52f6d6ef7719/iec-61508-7-2000>

WITHDRAWN

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

Part 7: Overview of techniques and measures

1 Scope

1.1 This part of IEC 61508 contains an overview of various safety techniques and measures relevant to IEC 61508-2 and IEC 61508-3.

NOTE The references should be considered as basic references to methods and tools or as examples, and may not represent the state of the art.

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 3.4.4 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 is also intended for use as a stand-alone standard.

One of the responsibilities of a technical committee is, wherever applicable, to make use of basic safety publications in the preparation of its own publications. In this context, the requirements, test methods or test conditions of this basic safety publication will not apply unless specifically referred to or included in the publications prepared by those technical committees.

NOTE 1 The functional safety of an E/E/PE safety-related system can only be achieved when all related requirements are met. Therefore it is important that all related requirements are carefully considered and adequately referenced.

NOTE 2 In the USA and Canada, until the proposed process sector implementation of IEC 61508 (i.e. IEC 61511) is published as an international standard in the USA and Canada, existing national process safety standards based on IEC 61508 (i.e. ANSI/ISA S84.01-1996) can be applied to the process sector instead of IEC 61508.

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