

Svenska Elektriska Kommissionen, SEK

Fastställt	Utgåva	Sida	Ingår i
2002-10-09	1	1 (1+114)	SEK Område 65

© Copyright SEK. Reproduction in any form without permission is prohibited.

Funktionssäkerhet hos elektriska, elektroniska och programmerbara elektroniska säkerhetskritiska system – Del 7: Översikt över metoder och åtgärder

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

Som svensk standard gäller europastandarden EN 61508-7:2001. Den svenska standarden innehåller den officiella engelska språkversionen av EN 61508-7:2001.

Nationellt förord

Europastandarden EN 61508-7:2001

består av:

- **europastandardens ikraftsättningsdokument**, utarbetat inom CENELEC
- **IEC 61508-7, First edition, 2000 - Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 7: Overview of techniques and measures**

utarbetad inom International Electrotechnical Commission, IEC.

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

Part 7: Overview of techniques and measures

(IEC 61508-7:2000)

Sécurité fonctionnelle des systèmes
électriques/électroniques/électroniques
programmables relatifs à la sécurité
Partie 7: Présentation de techniques et
mesures
(CEI 61508-7:2000)

Funktionale Sicherheit
sicherheitsbezogener elektrischer/
elektronischer/programmierbarer
elektronischer Systeme
Teil 7: Anwendungshinweise über
Verfahren und Maßnahmen
(IEC 61508-7:2000)

This European Standard was approved by CENELEC on 2001-07-03. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the Central Secretariat or to any CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CENELEC member into its own language and notified to the Central Secretariat has the same status as the official versions.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Czech Republic, Denmark, Finland, France, Germany, Greece, Iceland, Ireland, Italy, Luxembourg, Malta, Netherlands, Norway, Portugal, Spain, Sweden, Switzerland and United Kingdom.

CENELEC

European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung

Central Secretariat: rue de Stassart 35, B - 1050 Brussels

Foreword

The text of the International Standard IEC 61508-7:2000, prepared by SC 65A, System aspects, of IEC TC 65, Industrial-process measurement and control, was submitted to the Unique Acceptance Procedure and was approved by CENELEC as EN 61508-7 on 2001-07-03 without any modification.

The following dates were fixed:

- latest date by which the EN has to be implemented
at national level by publication of an identical
national standard or by endorsement (dop) 2002-08-01
- latest date by which the national standards conflicting
with the EN have to be withdrawn (dow) 2004-08-01

Annexes designated "normative" are part of the body of the standard.

Annexes designated "informative" are given for information only.

In this standard, annex ZA is normative and annexes A, B, C and D are informative.

Annex ZA has been added by CENELEC.

IEC 61508 is a basic safety publication covering the functional safety of electrical, electronic and programmable electronic safety-related systems. The scope states:

"This International Standard covers those aspects to be considered when electrical/electronic/programmable electronic systems (E/E/PESs) are used to carry out safety functions. A major objective of this standard is to facilitate the development of application sector international standards by the technical committees responsible for the application sector. This will allow all the relevant factors associated with the application, to be fully taken into account and thereby meet the specific needs of the application sector. A dual objective of this standard is to enable the development of electrical/electronic/programmable electronic (E/E/PE) safety-related systems where application sector international standards may not exist".

The CENELEC Report R0BT-004, ratified by 103 BT (March 2000) accepts that some IEC standards, which today are either published or under development, are sector implementations of IEC 61508. For example:

- IEC 61511, Functional safety - Safety instrumented systems for the process industry sector;
- IEC 62061, Safety of machinery – Functional safety of electrical, electronic and programmable electronic control systems;
- IEC 61513, Nuclear power plants – Instrumentation and control for systems important to safety – General requirements for systems.

The railways sector has also developed a set of European Standards (EN 50126; EN 50128 and prEN 50129).

NOTE EN 50126 and EN 50128 were based on earlier drafts of IEC 61508. prEN 50129 is based on the principles of the latest version of IEC 61508.

This list does not preclude other sector implementations of IEC 61508 which could be currently under development or published within IEC or CENELEC.

Endorsement notice

The text of the International Standard IEC 61508-7:2000 was approved by CENELEC as a European Standard without any modification.

In the official version, for Bibliography, the following notes have to be added for the standards indicated:

IEC 60068-1	NOTE	Harmonized as EN 60068-1:1994 (not modified).
IEC 60529	NOTE	Harmonized as EN 60523:1991 (not modified).
IEC 60812	NOTE	Harmonized as HD 485 S1:1987 (not modified).
IEC 61000-4-1	NOTE	Harmonized as EN 61000-4-1:1994 (not modified).
IEC 61000-4-5	NOTE	Harmonized as EN 61000-4-5:1995 (not modified).
IEC 61025	NOTE	Harmonized as HD 617 S1:1992 (not modified).
IEC 61069-5	NOTE	Harmonized as EN 61069-5:1995 (not modified).
IEC 61078	NOTE	Harmonized as EN 61078:1993 (not modified).
IEC 61131-3	NOTE	Harmonized as EN 61131-3:1993 (not modified).
IEC 61346-1	NOTE	Harmonized as EN 61346-1:1996 (not modified).

Annex ZA (normative)

Normative references to international publications with their corresponding European publications

This European Standard incorporates by dated or undated reference, provisions from other publications. These normative references are cited at the appropriate places in the text and the publications are listed hereafter. For dated references, subsequent amendments to or revisions of any of these publications apply to this European Standard only when incorporated in it by amendment or revision. For undated references the latest edition of the publication referred to applies (including amendments).

NOTE When an international publication has been modified by common modifications, indicated by (mod), the relevant EN/HD applies.

<u>Publication</u>	<u>Year</u>	<u>Title</u>	<u>EN/HD</u>	<u>Year</u>
IEC 61508-1 + corr. May	1998 1999	Functional safety of electrical/electronic/programmable electronic safety-related systems Part 1: General requirements	EN 61508-1	2001
IEC 61508-2	2000	Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems	EN 61508-2	2001
IEC 61508-3 + corr. April	1998 1999	Part 3: Software requirements	EN 61508-3	2001
IEC 61508-4 + corr. April	1998 1999	Part 4: Definitions and abbreviations	EN 61508-4	2001
IEC 61508-5 + corr. April	1998 1999	Part 5: Examples of methods for the determination of safety integrity levels	EN 61508-5	2001
IEC 61508-6	2000	Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3	EN 61508-6	2001
IEC Guide 104	1997	The preparation of safety publications and the use of basic safety publications and group safety publications	-	-
ISO/IEC Guide 51	1990	Guidelines for the inclusion of safety aspects in standards	-	-

CONTENTS

Page

Clause

1	Scope	23
2	Normative references	27
3	Definitions and abbreviations	27
Annex A (informative) Overview of techniques and measures for E/E/PES: control of random hardware failures (see IEC 61508-2).....		29
A.1	Electrical.....	29
A.1.1	Failure detection by on-line monitoring	29
A.1.2	Monitoring of relay contacts	29
A.1.3	Comparator	29
A.1.4	Majority voter	31
A.1.5	Idle current principle (de-energised to trip).....	31
A.2	Electronic	31
A.2.1	Tests by redundant hardware.....	31
A.2.2	Dynamic principles	33
A.2.3	Standard test access port and boundary-scan architecture	33
A.2.4	Fail-safe hardware	33
A.2.5	Monitored redundancy	35
A.2.6	Electrical/electronic components with automatic check.....	35
A.2.7	Analogue signal monitoring	35
A.2.8	De-rating	37
A.3	Processing units	37
A.3.1	Self-test by software: limited number of patterns (one-channel).....	37
A.3.2	Self-test by software: walking bit (one-channel)	37
A.3.3	Self-test supported by hardware (one-channel)	37
A.3.4	Coded processing (one-channel)	39
A.3.5	Reciprocal comparison by software	39
A.4	Invariable memory ranges	39
A.4.1	Word-saving multi-bit redundancy (for example ROM monitoring with a modified Hamming code)	39
A.4.2	Modified checksum	41
A.4.3	Signature of one word (8-bit).....	41
A.4.4	Signature of a double word (16-bit)	41
A.4.5	Block replication (for example double ROM with hardware or software comparison).....	43
A.5	Variable memory ranges	43
A.5.1	RAM test "checkerboard" or "march".....	43
A.5.2	RAM test "walkpath".....	45
A.5.3	RAM test "galpat" or "transparent galpat".....	45
A.5.4	RAM test "Abraham"	47
A.5.5	One-bit redundancy (for example RAM monitoring with a parity bit).....	47
A.5.6	RAM monitoring with a modified Hamming code, or detection of data failures with error-detection-correction codes (EDC)	47
A.5.7	Double RAM with hardware or software comparison and read/write test	49

Clause	Page
A.6 I/O-units and interfaces (external communication)	49
A.6.1 Test pattern.....	49
A.6.2 Code protection.....	49
A.6.3 Multi-channel parallel output	51
A.6.4 Monitored outputs	51
A.6.5 Input comparison/voting	53
A.7 Data paths (internal communication)	53
A.7.1 One-bit hardware redundancy.....	53
A.7.2 Multi-bit hardware redundancy	53
A.7.3 Complete hardware redundancy	53
A.7.4 Inspection using test patterns	55
A.7.5 Transmission redundancy	55
A.7.6 Information redundancy	55
A.8 Power supply.....	55
A.8.1 Overvoltage protection with safety shut-off	55
A.8.2 Voltage control (secondary)	57
A.8.3 Power-down with safety shut-off	57
A.9 Temporal and logical program sequence monitoring	57
A.9.1 Watch-dog with separate time base without time-window	57
A.9.2 Watch-dog with separate time base and time-window.....	59
A.9.3 Logical monitoring of program sequence	59
A.9.4 Combination of temporal and logical monitoring of program sequences	59
A.9.5 Temporal monitoring with on-line check.....	59
A.10 Ventilation and heating.....	61
A.10.1 Temperature sensor.....	61
A.10.2 Fan control.....	61
A.10.3 Actuation of the safety shut-off via thermal fuse.....	61
A.10.4 Staggered message from thermo-sensors and conditional alarm.....	61
A.10.5 Connection of forced-air cooling and status indication	61
A.11 Communication and mass-storage	63
A.11.1 Separation of electrical energy lines from information lines	63
A.11.2 Spatial separation of multiple lines.....	63
A.11.3 Increase of interference immunity	63
A.11.4 Antivalent signal transmission	65
A.12 Sensors.....	65
A.12.1 Reference sensor.....	65
A.12.2 Positive-activated switch	65
A.13 Final elements (actuators)	65
A.13.1 Monitoring	65
A.13.2 Cross-monitoring of multiple actuators.....	67
A.14 Measures against the physical environment.....	67
Annex B (informative) Overview of techniques and measures for E/E/PES: avoidance of systematic failures (see IEC 61508-2 and IEC 61508-3).....	69
B.1 General measures and techniques.....	69
B.1.1 Project management.....	69
B.1.2 Documentation.....	71
B.1.3 Separation of safety-related systems from non-safety-related systems	73
B.1.4 Diverse hardware.....	73

Clause	Page
B.2 E/E/PES safety requirements specification	75
B.2.1 Structured specification	75
B.2.2 Formal methods	75
B.2.3 Semi-formal methods	77
B.2.3.1 General	77
B.2.3.2 Finite state machines/state transition diagrams	77
B.2.3.3 Time Petri nets	79
B.2.4 Computer-aided specification tools	79
B.2.4.1 General	79
B.2.4.2 Tools oriented towards no specific method	81
B.2.4.3 Model orientated procedure with hierarchical analysis	81
B.2.4.4 Entity models	81
B.2.4.5 Incentive and answer	83
B.2.5 Checklists	83
B.2.6 Inspection of the specification	85
B.3 E/E/PES design and development	85
B.3.1 Observance of guidelines and standards	85
B.3.2 Structured design	87
B.3.3 Use of well-tried components	89
B.3.4 Modularisation	89
B.3.5 Computer-aided design tools	91
B.3.6 Simulation	91
B.3.7 Inspection (reviews and analysis)	91
B.3.8 Walk-through	93
B.4 E/E/PES operation and maintenance procedures	93
B.4.1 Operation and maintenance instructions	93
B.4.2 User friendliness	95
B.4.3 Maintenance friendliness	95
B.4.4 Limited operation possibilities	95
B.4.5 Operation only by skilled operators	97
B.4.6 Protection against operator mistakes	97
B.4.7 (Not used)	97
B.4.8 Modification protection	97
B.4.9 Input acknowledgement	97
B.5 E/E/PES integration	99
B.5.1 Functional testing	99
B.5.2 Black-box testing	99
B.5.3 Statistical testing	101
B.5.4 Field experience	101
B.6 E/E/PES safety validation	103
B.6.1 Functional testing under environmental conditions	103
B.6.2 Interference surge immunity testing	105
B.6.3 (Not used)	105
B.6.4 Static analysis	105
B.6.5 Dynamic analysis	107

Clause	Page
B.6.6 Failure analysis	107
B.6.6.1 Failure modes and effects analysis	107
B.6.6.2 Cause consequence diagrams	109
B.6.6.3 Event tree analysis	109
B.6.6.4 Failure modes, effects and criticality analysis.....	109
B.6.6.5 Fault tree analysis	111
B.6.7 Worst-case analysis	111
B.6.8 Expanded functional testing	111
B.6.9 Worst-case testing	113
B.6.10 Fault insertion testing.....	113
Annex C (informative) Overview of techniques and measures for achieving software safety integrity (see IEC 61508-3)	115
C.1 General	115
C.2 Requirements and detailed design	115
C.2.1 Structured methods.....	115
C.2.1.1 General	115
C.2.1.2 CORE – Controlled Requirements Expression	117
C.2.1.3 JSD – Jackson System Development.....	117
C.2.1.4 MASCOT – Modular Approach to Software Construction, Operation and Test	119
C.2.1.5 Real-time Yourdon	119
C.2.1.6 SADT – Structured Analysis and Design Technique.....	121
C.2.2 Data flow diagrams	123
C.2.3 Structure diagrams.....	125
C.2.4 Formal methods	125
C.2.4.1 General	125
C.2.4.2 CCS – Calculus of Communicating Systems.....	127
C.2.4.3 CSP – Communicating Sequential Processes.....	127
C.2.4.4 HOL – Higher Order Logic.....	129
C.2.4.5 LOTOS	129
C.2.4.6 OBJ	129
C.2.4.7 Temporal logic.....	131
C.2.4.8 VDM, VDM++ – Vienna Development Method.....	133
C.2.4.9 Z.....	135
C.2.5 Defensive programming	137
C.2.6 Design and coding standards.....	139
C.2.6.1 General	139
C.2.6.2 Coding standards	139
C.2.6.3 No dynamic variables or dynamic objects	141
C.2.6.4 On-line checking during creation of dynamic variables or dynamic objects	141
C.2.6.5 Limited use of interrupts	141
C.2.6.6 Limited use of pointers	143
C.2.6.7 Limited use of recursion	143
C.2.7 Structured programming	143
C.2.8 Information hiding/encapsulation.....	145
C.2.9 Modular approach	147
C.2.10 Use of trusted/verified software modules and components	147

Clause	Page
C.3 Architecture design.....	149
C.3.1 Fault detection and diagnosis	149
C.3.2 Error detecting and correcting codes	151
C.3.3 Failure assertion programming.....	151
C.3.4 Safety bag.....	153
C.3.5 Software diversity (diverse programming)	153
C.3.6 Recovery block	155
C.3.7 Backward recovery.....	157
C.3.8 Forward recovery	157
C.3.9 Re-try fault recovery mechanisms.....	157
C.3.10 Memorising executed cases.....	159
C.3.11 Graceful degradation.....	159
C.3.12 Artificial intelligence fault correction	161
C.3.13 Dynamic reconfiguration	161
C.4 Development tools and programming languages.....	163
C.4.1 Strongly typed programming languages.....	163
C.4.2 Language subsets.....	163
C.4.3 Certified tools and certified translators	165
C.4.4 Tools and translators: increased confidence from use	165
C.4.4.1 Comparison of source program and executable code	167
C.4.5 Library of trusted/verified software modules and components.....	167
C.4.6 Suitable programming languages.....	169
C.5 Verification and modification	175
C.5.1 Probabilistic testing	175
C.5.2 Data recording and analysis.....	177
C.5.3 Interface testing	177
C.5.4 Boundary value analysis	177
C.5.5 Error guessing.....	179
C.5.6 Error seeding	179
C.5.7 Equivalence classes and input partition testing.....	181
C.5.8 Structure-based testing	181
C.5.9 Control flow analysis	183
C.5.10 Data flow analysis	185
C.5.11 Sneak circuit analysis.....	185
C.5.12 Symbolic execution	187
C.5.13 Formal proof.....	187
C.5.14 Complexity metrics.....	189
C.5.15 Fagan inspections	189
C.5.16 Walk-throughs/design reviews	191
C.5.17 Prototyping/animation	191
C.5.18 Process simulation.....	193
C.5.19 Performance requirements.....	193
C.5.20 Performance modelling	195
C.5.21 Avalanche/stress testing	195
C.5.22 Response timing and memory constraints	197
C.5.23 Impact analysis	197
C.5.24 Software configuration management.....	199

Clause	Page
C.6 Functional safety assessment	199
C.6.1 Decision tables (truth tables).....	199
C.6.2 Hazard and Operability Study (HAZOP).....	199
C.6.3 Common cause failure analysis	203
C.6.4 Markov models.....	203
C.6.5 Reliability block diagrams.....	205
C.6.6 Monte-Carlo simulation	207
Annex D (informative) A probabilistic approach to determining software safety integrity for pre-developed software.....	209
D.1 General	209
D.2 Statistical testing formulae and examples of their use.....	211
D.2.1 Simple statistical test for low demand mode of operation.....	211
D.2.1.1 Prerequisites	211
D.2.1.2 Results	211
D.2.1.3 Example	211
D.2.2 Testing of an input space (domain) for a low demand mode of operation	211
D.2.2.1 Prerequisites	211
D.2.2.2 Results	211
D.2.2.3 Example	213
D.2.3 Simple statistical test for high demand or continuous mode of operation	213
D.2.3.1 Prerequisites	213
D.2.3.2 Results	213
D.2.3.3 Example	215
D.2.4 Complete test.....	215
D.2.4.1 Prerequisites	215
D.2.4.2 Results	215
D.2.4.3 Example	217
D.3 References.....	217
Bibliography	219
Index	223
Table C.1 – Recommendations for specific programming languages	173
Table D.1 – Necessary history for confidence to safety integrity levels	209
Table D.2 – Probabilities of failure for low demand mode of operation.....	211
Table D.3 – Mean distances of two test points.....	213
Table D.4 – Probabilities of failure for high demand or continuous mode of operation	215
Table D.5 – Probability of testing all program properties.....	217

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.

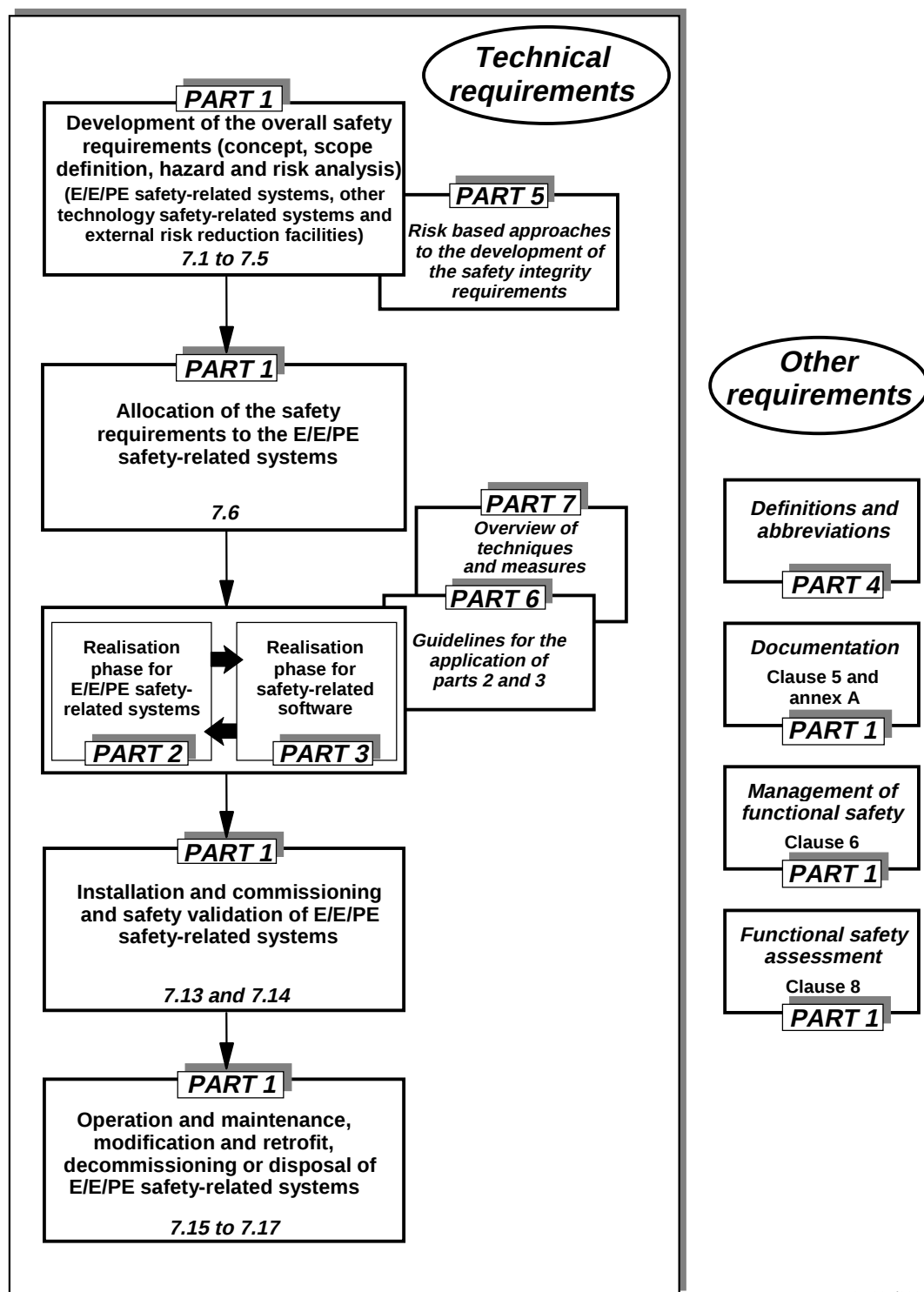
1.2 IEC 61508-1, IEC 61508-2, IEC 61508-3 and IEC 61508-4 are basic safety publications, although this status does not apply in the context of low-complexity E/E/PE safety-related systems (see 3.4.4 of IEC 61508-4). As basic safety publications, they are intended for use by technical committees in the 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.



IEC 225/2000

Figure 1 – Overall framework of IEC 61508