INTERNATIONAL STANDARD

IEC 61508-7

First edition
2000-03

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

Part 7: Overview of techniques and measures

*This **English-language** version is derived from the original **bilingual** publication by leaving out all French-language pages. Missing page numbers correspond to the French-language pages.*

Reference number
IEC 61508-7:2000(E)

Publication numbering

As from 1 January 1997 all IEC publications are issued with a designation in the 60000 series. For example, IEC 34-1 is now referred to as IEC 60034-1.

Consolidated editions

The IEC is now publishing consolidated versions of its publications. For example, edition numbers 1.0, 1.1 and 1.2 refer, respectively, to the base publication, the base publication incorporating amendment 1 and the base publication incorporating amendments 1 and 2.

Further information on IEC publications

The technical content of IEC publications is kept under constant review by the IEC, thus ensuring that the content reflects current technology. Information relating to this publication, including its validity, is available in the IEC Catalogue of publications (see below) in addition to new editions, amendments and corrigenda. Information on the subjects under consideration and work in progress undertaken by the technical committee which has prepared this publication, as well as the list of publications issued, is also available from the following:

- **IEC Web Site (www.iec.ch)**

- **Catalogue of IEC publications**

  The on-line catalogue on the IEC web site (www.iec.ch/searchpub) enables you to search by a variety of criteria including text searches, technical committees and date of publication. On-line information is also available on recently issued publications, withdrawn and replaced publications, as well as corrigenda.

- **IEC Just Published**

  This summary of recently issued publications (www.iec.ch/online_news/ justpub) is also available by email. Please contact the Customer Service Centre (see below) for further information.

- **Customer Service Centre**

  If you have any questions regarding this publication or need further assistance, please contact the Customer Service Centre:

  Email: custserv@iec.ch
  Tel: +41 22 919 02 11
  Fax: +41 22 919 03 00

INTERNATIONAL STANDARD

IEC 61508-7

First edition
2000-03

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

Part 7: Overview of techniques and measures

International Electrotechnical Commission, 3, rue de Varembé, PO Box 131, CH-1211 Geneva 20, Switzerland
Telephone: +41 22 919 02 11 Telefax: +41 22 919 03 00 E-mail: inmail@iec.ch Web: www.iec.ch

IEC

Commission Electrotechnique Internationale
International Electrotechnical Commission
Международная Электротехническая Комиссия

PRICE CODE XE

For price, see current catalogue

CONTENTS

Page

FOREWORD ... 15

INTRODUCTION ... 19

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

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.

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.

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.