

Australian Standard™

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

**Part 7: Overview of techniques and  
measures**



This Australian Standard was prepared by Committee IT-006, Information Technology for Industrial Automation and Integration. It was approved on behalf of the Council of Standards Australia on 18 April 2001 and published on 19 June 2001.

---

The following interests are represented on Committee IT-006:

Australian Electrical and Electronic Manufacturers Association  
CSIRO Centre for Planning and Design  
CSIRO Manufacturing Science and Technology  
Industrial Instrument Industry Association of Australia  
Institution of Engineers, Australia  
Monash University  
RMIT University  
The Association of Consulting Engineers, Australia  
The Royal Australian Institute of Architects  
The University of Melbourne

---

#### **Keeping Standards up-to-date**

Standards are living documents which reflect progress in science, technology and systems. To maintain their currency, all Standards are periodically reviewed, and new editions are published. Between editions, amendments may be issued. Standards may also be withdrawn. It is important that readers assure themselves they are using a current Standard, which should include any amendments which may have been published since the Standard was purchased.

Detailed information about Standards can be found by visiting the Standards Australia website at [www.standards.com.au](http://www.standards.com.au) and looking up the relevant Standard in the on-line catalogue.

Alternatively, the printed Catalogue provides information current at 1 January each year, and the monthly magazine, *The Australian Standard*, has a full listing of revisions and amendments published each month.

We also welcome suggestions for improvement in our Standards, and especially encourage readers to notify us immediately of any apparent inaccuracies or ambiguities. Contact us via email at [mail@standards.com.au](mailto:mail@standards.com.au), or write to the Chief Executive, Standards Australia International Ltd, GPO Box 5420, Sydney, NSW 2001.

---

Australian Standard™

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

**Part 7: Overview of techniques and  
measures**

First published as AS 61508.7—2001.

**COPYRIGHT**

© Standards Australia International

All rights are reserved. No part of this work may be reproduced or copied in any form or by any means, electronic or mechanical, including photocopying, without the written permission of the publisher.

Published by Standards Australia International Ltd  
GPO Box 5420, Sydney, NSW 2001, Australia

ISBN 0 7337 3898 2

## PREFACE

This Standard was prepared by the Standards Australia Committee IT-006, Information Technology for Industrial Automation and Integration.

The objective of this Standard is to provide designers of safety lifecycle activities in systems comprised of electrical/electronic/programmable electronic devices with an overview of various safety techniques and measures as outlined in Part 2 and in Part 3 of this Standard.

This Standard is identical with and has been reproduced from IEC 61508-7:2000, *Functional safety of electrical/electronic/programmable electronic safety-related systems—Part 7: Overview of techniques and measures*.

A reference to an International Standard identified in the Normative References table by strikethrough (~~example~~) is replaced by a reference to the Australian or Australian/New Zealand Standard(s) listed immediately thereafter and identified by shading (example). Where the struck-through referenced document and the referenced Australian or Australian/New Zealand Standard are identical, this is indicated in parenthesis after the title of the latter.

In this Standard, the following print types are used:

- requirements proper: in arial type;
- *test specifications: in italic type;*
- explanatory matter: in smaller arial type.

As this Standard is reproduced from an International Standard, the following applies:

- (a) Its number does not appear on each page of text and its identity is shown only on the cover and title page.
- (b) In the source text 'this standard' should read 'this Australian Standard'.
- (c) A full point should be substituted for a comma when referring to a decimal marker.

The term 'informative' has been used in this Standard to define the application of the annex to which it applies. An 'informative' annex is only for information and guidance.

## CONTENTS

	<i>Page</i>
1 Scope.....	1
2 Normative references .....	3
3 Definitions and abbreviations .....	4

## ANNEXES

Annex A (informative) Overview of techniques and measures for E/E/PES: control of random hardware failures (see IEC 61508-2) .....	5
A.1 Electrical.....	5
A.1.1 Failure detection by on-line monitoring .....	5
A.1.2 Monitoring of relay contacts.....	5
A.1.3 Comparator .....	5
A.1.4 Majority voter.....	6
A.1.5 Idle current principle (de-energised to trip) .....	6
A.2 Electronic.....	6
A.2.1 Tests by redundant hardware .....	6
A.2.2 Dynamic principles .....	7
A.2.3 Standard test access port and boundary scan architecture .....	7
A.2.4 Fail-safe hardware.....	7
A.2.5 Monitored redundancy.....	8
A.2.6 Electrical/electronic components with automatic check .....	8
A.2.7 Analogue signal monitoring.....	8
A.2.8 De-rating .....	9
A.3 Processing units.....	9
A.3.1 Self-test by software: limited number of patterns (one-channel) .....	9
A.3.2 Self-test by software: walking bit (one-channel) .....	9
A.3.3 Self-test supported by hardware (one-channel).....	9
A.3.4 Coded processing (one-channel) .....	10
A.3.5 Reciprocal comparison by software .....	10
A.4 Invariable memory ranges .....	10
A.4.1 Word-saving multi-bit redundancy (for example ROM monitoring with a modified Hamming code) .....	10
A.4.2 Modified checksum .....	11
A.4.3 Signature of one word (8-bit) .....	11
A.4.4 Signature of a double word (16-bit).....	11
A.4.5 Block replication (for example double ROM with hardware or software comparison) .....	12
A.5 Variable memory ranges .....	12
A.5.1 RAM test "checkerboard" or "march".....	12
A.5.2 RAM test "walkpath" .....	13
A.5.3 RAM test "galpat" or "transparent galpat".....	13
A.5.4 RAM test "Abraham" .....	14
A.5.5 One-bit redundancy (for example RAM monitoring with a parity bit) .....	14

	<i>Page</i>
A.5.6 RAM monitoring with a modified Hamming code, or detection of data failures with error-detection-correction codes (EDC) .....	14
A.5.7 Double RAM with hardware or software comparison and read/write test.....	15
A.6 I/O-units and interfaces (external communication) .....	15
A.6.1 Test pattern .....	15
A.6.2 Code protection .....	15
A.6.3 Multi-channel parallel output.....	16
A.6.4 Monitored outputs.....	16
A.6.5 Input comparison/voting.....	17
A.7 Data paths (internal communication) .....	17
A.7.1 One-bit hardware redundancy.....	17
A.7.2 Multi-bit hardware redundancy.....	17
A.7.3 Complete hardware redundancy .....	17
A.7.4 Inspection using test patterns .....	18
A.7.5 Transmission redundancy .....	18
A.7.6 Information redundancy .....	18
A.8 Power supply .....	18
A.8.1 Overvoltage protection with safety shut-off .....	18
A.8.2 Voltage control (secondary) .....	19
A.8.3 Power-down with safety shut-off.....	19
A.9 Temporal and logical program sequence monitoring.....	19
A.9.1 Watch-dog with separate time base without time-window .....	19
A.9.2 Watch-dog with separate time base and time-window .....	20
A.9.3 Logical monitoring of program sequence.....	20
A.9.4 Combination of temporal and logical monitoring of program sequences.....	20
A.9.5 Temporal monitoring with on-line check .....	20
A.10 Ventilation and heating .....	21
A.10.1 Temperature sensor .....	21
A.10.2 Fan control .....	21
A.10.3 Activation of the safety shut-off via thermal fuse.....	21
A.10.4 Staggered message from thermo-sensors and conditional alarm .....	21
A.10.5 Connection of forced-air cooling and status indication .....	21
A.11 Communication and mass-storage.....	22
A.11.1 Separation of electrical energy lines from information lines.....	22
A.11.2 Spatial separation of multiple lines .....	22
A.11.3 Increase of interference immunity.....	22
A.11.4 Antivalent signal transmission.....	23
A.12 Sensors.....	23
A.12.1 Reference sensor .....	23
A.12.2 Positive-activated switch .....	23
A.13 Final elements (actuators).....	23
A.13.1 Monitoring .....	23
A.13.2 Cross-monitoring of multiple actuators.....	24
A.14 Measures against the physical environment .....	24

Annex B (informative) Overview of techniques and measures for E/E/PES: avoidance of systematic failures (see IEC 61508-2 and IEC 61508-3).....	25
B.1 General measures and techniques .....	25
B.1.1 Project management.....	25
B.1.2 Documentation .....	26
B.1.3 Separation of safety-related systems from non-safety-related systems.....	27
B.1.4 Diverse hardware .....	27
B.2 E/E/PES safety requirements specification.....	28
B.2.1 Structured specification .....	28
B.2.2 Formal methods.....	28
B.2.3 Semi-formal methods.....	29
B.2.3.1 General .....	29
B.2.3.2 Finite state machines/state transition diagrams .....	29
B.2.3.3 Time Petri nets .....	30
B.2.4 Computer-aided specification tools .....	30
B.2.4.1 General .....	30
B.2.4.2 Tools oriented towards no specific method .....	31
B.2.4.3 Model orientated procedure with hierarchical analysis .....	31
B.2.4.4 Entity models.....	31
B.2.4.5 Incentive and answer.....	32
B.2.5 Checklists.....	32
B.2.6 Inspection of the specification .....	33
B.3 E/E/PES design and development .....	33
B.3.1 Observance of guidelines and standards .....	33
B.3.2 Structured design .....	34
B.3.3 Use of well-tried components.....	35
B.3.4 Modularisation .....	35
B.3.5 Computer-aided design tools .....	36
B.3.6 Simulation .....	36
B.3.7 Inspection (reviews and analysis) .....	36
B.3.8 Walk-through.....	37
B.4 E/E/PES operation and maintenance procedures .....	37
B.4.1 Operation and maintenance instructions .....	37
B.4.2 User friendliness.....	38
B.4.3 Maintenance friendliness .....	38
B.4.4 Limited operation possibilities.....	38
B.4.5 Operation only by skilled operators.....	39
B.4.6 Protection against operator mistakes .....	39
B.4.7 (Not used) .....	39
B.4.8 Modification protection.....	39
B.4.9 Input acknowledgement .....	39
B.5 E/E/PES integration .....	40
B.5.1 Functional testing .....	40
B.5.2 Black-box testing .....	40
B.5.3 Statistical testing .....	41

	<i>Page</i>
B.5.4	Field experience ..... 41
B.6	E/E/PES safety validation..... 42
B.6.1	Functional testing under environmental conditions..... 42
B.6.2	Interference surge immunity testing ..... 43
B.6.3	(Not used) ..... 43
B.6.4	Static analysis ..... 43
B.6.5	Dynamic analysis..... 44
B.6.6	Failure analysis ..... 44
B.6.6.1	Failure modes and effects analysis..... 44
B.6.6.2	Cause consequence diagrams ..... 44
B.6.6.3	Event tree analysis ..... 45
B.6.6.4	Failure modes, effects and criticality analysis ..... 45
B.6.6.5	Fault tree analysis ..... 46
B.6.7	Worst-case analysis ..... 46
B.6.8	Expanded functional testing..... 46
B.6.9	Worst-case testing..... 47
B.6.10	Fault insertion testing ..... 47
Annex C (informative)	Overview of techniques and measures for achieving software safety integrity (see IEC 61508-3) ..... 48
C.1	General..... 48
C.2	Requirements and detailed design ..... 48
C.2.1	Structured methods ..... 48
C.2.1.1	General ..... 48
C.2.1.2	CORE – Controlled Requirements Expression ..... 49
C.2.1.3	JSD – Jackson System Development..... 49
C.2.1.4	MASCOT – Modular Approach to Software Construction, Operation and Test ..... 50
C.2.1.5	Real-time Yunion..... 50
C.2.1.6	SADT – Structured Analysis and Design Technique ..... 51
C.2.2	Data flow diagrams ..... 52
C.2.3	Structure diagrams ..... 53
C.2.4	Formal methods..... 53
C.2.4.1	General ..... 53
C.2.4.2	CCS – Calculus of Communicating Systems ..... 54
C.2.4.3	CSP – Communicating Sequential Processes ..... 54
C.2.4.4	HOL – Higher Order Logic ..... 55
C.2.4.5	LOTOS ..... 55
C.2.4.6	OBJ ..... 55
C.2.4.7	Temporal logic..... 56
C.2.4.8	VDM, VDM++ – Vienna Development Method ..... 57
C.2.4.9	Z ..... 58
C.2.5	Defensive programming..... 59
C.2.6	Design and coding standards..... 60
C.2.6.1	General ..... 60
C.2.6.2	Coding standards ..... 60
C.2.6.3	No dynamic variables or dynamic objects ..... 61

C.2.6.4	On-line checking during creation of dynamic variables or dynamic objects.....	61
C.2.6.5	Limited use of interrupts .....	61
C.2.6.6	Limited use of pointers .....	62
C.2.6.7	Limited use of recursion .....	62
C.2.7	Structured programming .....	62
C.2.8	Information hiding/encapsulation .....	63
C.2.9	Modular approach.....	64
C.2.10	Use of trusted/verified software modules and components.....	64
C.3	Architecture design .....	65
C.3.1	Fault detection and diagnosis .....	65
C.3.2	Error detecting and correcting codes .....	66
C.3.3	Failure assertion programming .....	66
C.3.4	Safety bag.....	67
C.3.5	Software diversity (diverse programming) .....	67
C.3.6	Recovery block.....	68
C.3.7	Backward recovery .....	69
C.3.8	Forward recovery.....	69
C.3.9	Re-try fault recovery mechanisms.....	69
C.3.10	Memorising executed cases.....	70
C.3.11	Graceful degradation .....	70
C.3.12	Artificial intelligence fault correction .....	71
C.3.13	Dynamic reconfiguration .....	71
C.4	Development tools and programming languages .....	72
C.4.1	Strongly typed programming languages .....	72
C.4.2	Language subsets .....	72
C.4.3	Certified tools and certified translators.....	73
C.4.4	Tools and translators: increased confidence from use.....	73
C.4.4.1	Comparison of source program and executable code.....	74
C.4.5	Library of trusted/verified software modules and components .....	74
C.4.6	Suitable programming languages.....	75
C.5	Verification and modification .....	78
C.5.1	Probabilistic testing .....	78
C.5.2	Data recording and analysis .....	79
C.5.3	Interface testing.....	79
C.5.4	Boundary value analysis.....	79
C.5.5	Error guessing .....	80
C.5.6	Error seeding.....	80
C.5.7	Equivalence classes and input partition testing.....	81
C.5.8	Structure-based testing.....	81
C.5.9	Control flow analysis.....	82
C.5.10	Data flow analysis .....	83
C.5.11	Sneak circuit analysis .....	83
C.5.12	Symbolic execution.....	84
C.5.13	Formal proof .....	84
C.5.14	Complexity metrics .....	85
C.5.15	Fagan inspections .....	85

	<i>Page</i>
C.5.16 Walk-throughs/design reviews .....	86
C.5.17 Prototyping/animation .....	86
C.5.18 Process simulation .....	87
C.5.19 Performance requirements.....	87
C.5.20 Performance modelling.....	88
C.5.21 Avalanche/stress testing.....	88
C.5.22 Response timing and memory constraints.....	89
C.5.23 Impact analysis.....	89
C.5.24 Software configuration management.....	90
C.6 Functional safety assessment .....	90
C.6.1 Decision tables (truth tables) .....	90
C.6.2 Hazard and Operability Study (HAZOP) .....	90
C.6.3 Common cause failure analysis .....	92
C.6.4 Markov models .....	92
C.6.5 Reliability block diagrams .....	93
C.6.6 Monte-Carlo simulation.....	94
Annex D (informative) A probabilistic approach to determining software safety integrity for pre-developed software.....	95
D.1 General.....	95
D.2 Statistical testing formulae and examples of their use .....	96
D.2.1 Simple statistical test for low demand mode of operation .....	96
D.2.1.1 Prerequisites .....	96
D.2.1.2 Results .....	96
D.2.1.3 Example .....	96
D.2.2 Testing of an input space (domain) for a low demand mode of operation.....	96
D.2.2.1 Prerequisites.....	96
D.2.2.2 Results.....	96
D.2.2.3 Example.....	97
D.2.3 Simple statistical test for high demand or continuous mode of operation.....	97
D.2.3.1 Prerequisites .....	97
D.2.3.2 Results.....	97
D.2.3.3 Example .....	98
D.2.4 Complete test.....	98
D.2.4.1 Prerequisites .....	98
D.2.4.2 Results.....	98
D.2.4.3 Example .....	99
D.3 References.....	99
Bibliography.....	100
Index .....	102

## STANDARDS AUSTRALIA

---

**Australian 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.