

Australian Standard™

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

**Part 6: Guidelines on the application of  
AS 61508.2 and AS 61508.3**

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 Standards may also be withdrawn.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 web site 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 6: Guidelines on the application of  
AS 61508.2 and AS 61508.3**

First published as AS 61508.6—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 3897 4

## 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 guidelines on the applications, calculations and methodologies as outlined in Part 2 and in Part 3 of this Standard.

This Standard is identical with and has been reproduced from IEC 61508-6:2000, *Functional safety of electrical/electronic/programmable electronic safety-related systems—Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3*.

A reference to an International Standard identified in the Normative References Clause 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 .....	3
<b>ANNEXES</b>	
Annex A (informative) Application of IEC 61508-2 and of IEC 61508-3.....	4
A.1 General.....	4
A.2 Functional steps in the application of IEC 61508-2 .....	6
A.3 Functional steps in the application of IEC 61508-3 .....	10
Annex B (informative) Example technique for evaluating probabilities of hardware failure.....	12
B.1 General.....	12
B.2 Average probability of failure on demand (for low demand mode of operation).....	16
B.3 Probability of failure per hour (for high demand or continuous mode of operation).....	29
B.4 References.....	37
Annex C (informative) Calculation of diagnostic coverage and safe failure fraction: worked example.....	38
Annex D (informative) A methodology for quantifying the effect of hardware-related common cause failures in E/E/PE systems .....	42
D.1 General.....	42
D.2 Brief overview .....	42
D.3 Scope of the methodology .....	46
D.4 Points taken into account in the methodology.....	46
D.5 Using the $\beta$ -factor to calculate the probability of failure in an E/E/PE safety-related system due to common cause failures .....	47
D.6 Using the tables to estimate $\beta$ .....	48
D.7 Examples of the use of the methodology .....	52
D.8 References.....	53
Annex E (informative) Example applications of software safety integrity tables of IEC 61508-3 .....	54
E.1 General.....	54
E.2 Example for safety integrity level 2.....	54
E.3 Example for safety integrity level 3.....	59
Bibliography.....	64

## FIGURES

Figure 1 – Overall framework of IEC 61508 .....	2
Figure A.1 – Application of IEC 61508-2 .....	8
Figure A.2 – Application of IEC 61508-2 (continued).....	9
Figure A.3 – Application of IEC 61508-3 .....	11
Figure B.1 – Example configuration for two sensor channels .....	14
Figure B.2 – Subsystem structure .....	16
Figure B.3 – 1oo1 physical block diagram.....	17
Figure B.4 – 1oo1 reliability block diagram .....	17
Figure B.5 – 1oo2 physical block diagram.....	18
Figure B.6 – 1oo2 reliability block diagram .....	19
Figure B.7 – 2oo2 physical block diagram.....	19
Figure B.8 – 2oo2 reliability block diagram .....	19
Figure B.9 – 1oo2D physical block diagram .....	20
Figure B.10 – 1oo2D reliability block diagram .....	20
Figure B.11 – 2oo3 physical block diagram.....	21
Figure B.12 – 2oo3 reliability block diagram.....	21
Figure B.13 – Architecture of an example for low demand mode of operation.....	26
Figure B.14 – Architecture of an example for high demand or continuous mode of operation .....	35
Figure D.1 – Relationship of common cause failures to the failures of individual channels.....	44

## TABLES

Table B.1 – Terms and their ranges used in this annex (applies to 1oo1, 1oo2, 2oo2, 1oo2D and 2oo3) .....	15
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 .....	22
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 .....	23
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.....	24
Table B.5 – Average probability of failure on demand for a proof-test interval of 10 years and a mean time to restoration of 8 h .....	25
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) .....	26
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) .....	27
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) .....	27
Table B.9 – Example for a non-perfect proof test .....	29
Table B.10 – Probability of failure per hour (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.....	31

Table B.11 – Probability of failure per hour (in high demand or continuous mode of operation) for a proof test interval of three months and a mean time to restoration of 8 h .....	32
Table B.12 – Probability of failure per hour (in high demand or continuous mode of operation) for a proof test interval of six months and a mean time to restoration of 8 h .....	33
Table B.13 – Probability of failure per hour (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 .....	34
Table B.14 – Probability of failure per hour for the sensor subsystem in the example for high demand or continuous mode of operation (six month proof-test interval and 8 h MTTR) .....	35
Table B.15 – Probability of failure per hour for the logic subsystem in the example for high demand or continuous mode of operation (six month proof-test interval and 8 h MTTR) .....	36
Table B.16 – Probability of failure per hour for the final element subsystem in the example for high demand or continuous mode of operation (six month proof-test interval and 8 h MTTR) .....	36
Table C.1 – Example calculations for diagnostic coverage and safe failure fraction .....	40
Table C.2 – Diagnostic coverage and effectiveness for different subsystems .....	41
Table D.1 – Scoring programmable electronics or sensors/final elements .....	49
Table D.2 – Value of Z: programmable electronics .....	51
Table D.3 – Value of Z: sensors or final elements .....	51
Table D.4 – Calculation of $\beta$ or $\beta_D$ .....	52
Table D.5 – Example values for programmable electronics .....	53
Table E.1 – Software safety requirements specification (see 7.2 of IEC 61508-3) .....	55
Table E.2 – Software design and development: software architecture design (see 7.4.3 of IEC 61508-3) .....	56
Table E.3 – Software design and development: support tools and programming language (see 7.4.4 of IEC 61508-3) .....	56
Table E.4 – Software design and development: detailed design (see 7.4.5 and 7.4.6 of IEC 61508-3) (this includes software system design, software module design and coding) .....	57
Table E.5 – Software design and development: software module testing and integration (see 7.4.7 and 7.4.8 of IEC 61508-3) .....	57
Table E.6 – Programmable electronics integration (hardware and software) (see 7.5 of IEC 61508-3) .....	57
Table E.7 – Software safety validation (see 7.7 of IEC 61508-3) .....	58
Table E.8 – Software modification (see 7.8 of IEC 61508-3) .....	58
Table E.9 – Software verification (see 7.9 of part 3) .....	58
Table E.10 – Functional safety assessment (see clause 8 of IEC 61508-3) .....	59
Table E.11 – Software safety requirements specification (see 7.2 of IEC 61508-3) .....	60
Table E.12 – Software design and development: software architecture design (see 7.4.3 of IEC 61508-3) .....	60
Table E.13 – Software design and development: support tools and programming language (see 7.4.4 of IEC 61508-3) .....	61
Table E.14 – Software design and development: detailed design (see 7.4.5 and 7.4.6 of IEC 61508-3) (this includes software system design, software module design and coding) .....	61

	<i>Page</i>
Table E.15 – Software design and development: software module testing and integration (see 7.4.7 and 7.4.8 of IEC 61508-3).....	62
Table E.16 – Programmable electronics integration (hardware and software) (see 7.5 of IEC 61508-3) .....	62
Table E.17 – Software safety validation (see 7.7 of IEC 61508-3).....	62
Table E.18 – Modification (see 7.8 of IEC 61508-3) .....	63
Table E.19 – Software verification (see 7.9 of IEC 61508-3) .....	63
Table E.20 – Functional safety assessment (see clause 8 of IEC 61508-3).....	63

## STANDARDS AUSTRALIA

---

**Australian Standard****Functional safety of electrical/electronic/programmable electronic safety-related systems**Part 6: Guidelines on the application of AS 61508.2 and AS 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 3.4.4 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 IEC/ISO Guide 51. IEC 61508 is also intended for use as a stand-alone standard.

**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 do not apply unless specifically referred to or included in the publications prepared by those technical committees.

**NOTE** In the USA and Canada, until the proposed process sector implementation of IEC 61508 (i.e. IEC 61511) is published as an international standard, 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.

**1.4** Figure 1 shows the overall framework for parts 1 to 7 of this standard and indicates the role that IEC 61508-6 plays in the achievement of functional safety for E/E/PE safety-related systems.