

Australian Standard™

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

**Part 3: Software requirements**

This Australian Standard was prepared by Committee IT/6, Information Technology for Industrial Automation Systems and Integration. It was approved on behalf of the Council of Standards Australia on 14 July 1999 and published on 5 August 1999.

---

The following interests are represented on Committee IT/6:

Australian Association of Consulting Engineers  
Australian Electrical and Electronic Manufacturers Association  
Australian Information Industry Association  
CSIRO Centre for Planning and Design  
CSIRO Manufacturing Science and Technology  
Department of Defence (Australia)  
Department of Industry Science and Resources (Commonwealth)  
Federal Chamber of Automotive Industries  
Institution of Engineers Australia  
Monash University  
New South Wales TAFE Commission  
RMIT University  
The Royal Australian Institute of Architects  
University of Melbourne

---

**Review of Australian Standards.** To keep abreast of progress in industry, Australian Standards are subject to periodic review and are kept up to date by the issue of amendments or new editions as necessary. It is important therefore that Standards users ensure that they are in possession of the latest edition, and any amendments thereto.

Full details of all Australian Standards and related publications will be found in the Standards Australia Catalogue of Publications; this information is supplemented each month by the magazine 'The Australian Standard', which subscribing members receive, and which gives details of new publications, new editions and amendments, and of withdrawn Standards.

Suggestions for improvements to Australian Standards, addressed to the head office of Standards Australia, are welcomed. Notification of any inaccuracy or ambiguity found in an Australian Standard should be made without delay in order that the matter may be investigated and appropriate action taken.

---

This Standard was issued in draft form for comment as DR 99166.

Australian Standard™

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

**Part 3: Software requirements**

First published as AS 61508.3—1999.

## PREFACE

This Standard was prepared by the Standards Australia Committee IT/6, Information Technology for Industrial Automation and Integration. This Standard is identical with and has been reproduced from IEC 61508-3:1998, *Functional safety of electrical/electronic/programmable electronic safety-related systems*, Part 3: *Software requirements*.

The objective of this Standard is to provide designers of electrical/electronic/programmable electronic devices used in safety related applications with the software requirements for a generic approach for all safety lifecycle activities when applied to safety-related software.

A reference to an International Standard identified in the normative references clause (Clause 2) by strikethrough (~~example~~) is replaced by a reference to the Australian Standard listed immediately thereafter and identified by shading (example). Where the struck-through referenced document and the referenced Australian Standard are identical, this is indicated in parenthesis after the title of the latter.

The terms 'normative' and 'informative' have been used in this Standard to define the application of the annex to which they apply. A normative annex is an integral part of a Standard, whereas an informative annex is only for information and guidance.

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 identification is shown only on the cover and title page.
- (b) In the source text 'this part of IEC 61508' should read 'this Australian Standard', and 'this International Standard' should read 'this series of Standards'.
- (c) A full point should be substituted for a comma when referring to a decimal marker.

© Copyright – STANDARDS AUSTRALIA

Users of Standards are reminded that copyright subsists in all Standards Australia publications and software. Except where the Copyright Act allows and except where provided for below no publications or software produced by Standards Australia may be reproduced, stored in a retrieval system in any form or transmitted by any means without prior permission in writing from Standards Australia. Permission may be conditional on an appropriate royalty payment. Requests for permission and information on commercial software royalties should be directed to the head office of Standards Australia.

Standards Australia will permit up to 10 percent of the technical content pages of a Standard to be copied for use exclusively in-house by purchasers of the Standard without payment of a royalty or advice to Standards Australia.

Standards Australia will also permit the inclusion of its copyright material in computer software programs for no royalty payment provided such programs are used exclusively in-house by the creators of the programs.

Care should be taken to ensure that material used is from the current edition of the Standard and that it is updated whenever the Standard is amended or revised. The number and date of the Standard should therefore be clearly identified.

The use of material in print form or in computer software programs to be used commercially, with or without payment, or in commercial contracts is subject to the payment of a royalty. This policy may be varied by Standards Australia at any time.

## CONTENTS

	<i>Page</i>
1 Scope.....	1
2 Normative references.....	4
3 Definitions and abbreviations.....	4
4 Conformance to this standard.....	5
5 Documentation.....	5
6 Software quality management system.....	5
6.1 Objectives.....	5
6.2 Requirements.....	5
7 Software safety lifecycle requirements.....	6
7.1 General.....	6
7.2 Software safety requirements specification.....	12
7.3 Software safety validation planning.....	14
7.4 Software design and development.....	16
7.5 Programmable electronics integration (hardware and software).....	22
7.6 Software operation and modification procedures.....	23
7.7 Software safety validation.....	23
7.8 Software modification.....	25
7.9 Software verification.....	27
8 Functional safety assessment.....	31
Annexes	
Annex A (normative) Guide to the selection of techniques and measures.....	32
Annex B (normative) Detailed tables.....	38
Annex C (informative) Bibliography.....	42
Tables	
1 Software safety lifecycle: overview.....	9
A.1 Software safety requirements specification (see 7.2).....	33
A.2 Software design and development: software architecture design (see 7.4.3).....	33
A.3 Software design and development: support tools and programming language (see 7.4.4).....	34
A.4 Software design and development: detailed design (see 7.4.5 and 7.4.6).....	34
A.5 Software design and development: software module testing and integration (see 7.4.7 and 7.4.8).....	35
A.6 Programmable electronics integration (hardware and software) (see 7.5).....	35
A.7 Software safety validation (see 7.7).....	35
A.8 Modification (see 7.8).....	36

	<i>Page</i>
A.9 Software verification (see 7.9) .....	36
A.10 Functional safety assessment (see clause 8) .....	37
B.1 Design and coding standards (referenced by table A.4).....	38
B.2 Dynamic analysis and testing (referenced by tables A.5 and A.9) .....	38
B.3 Functional and black-box testing (referenced by tables A.5, A.6 and A.7).....	39
B.4 Failure analysis (referenced by table A.10) .....	39
B.5 Modelling (referenced by table A.7).....	39
B.6 Performance testing (referenced by tables A.5 and A.6) .....	40
B.7 Semi-formal methods (referenced by tables A.1, A.2 and A.4).....	40
B.8 Static analysis (referenced by table A.9).....	40
B.9 Modular approach (referenced by table A.4).....	41
<b>Figures</b>	
1 Overall framework of this standard .....	3
2 E/E/PES safety lifecycle (in realisation phase) .....	7
3 Software safety lifecycle (in realisation phase) .....	7
4 Relationship between and scope of IEC 61508-2 and 61508-3 .....	8
5 Software safety integrity and the development lifecycle (the V-model) .....	8
6 Relationship between the hardware and software architectures of programmable electronics .....	12

## 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 also provides a framework within which safety-related systems based on other technologies may be considered.

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

This International Standard

- considers all relevant overall E/E/PE and software safety lifecycle phases (for example, from initial concept, through design, implementation, operation and maintenance to decommissioning) when E/E/PEs 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/PEs, to be developed; the development of application sector international standards, within the framework of this International 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 use 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.

## STANDARDS AUSTRALIA

**Functional safety of electrical/electronic/programmable electronic safety-related systems**Part 3:  
Software requirements**1 Scope****1.1** This part of IEC 61508

- a) is intended to be utilised only after a thorough understanding of IEC 61508-1 and IEC 61508-2;
- b) applies to any software forming part of a safety-related system or used to develop a safety-related system within the scope of IEC 61508-1 and IEC 61508-2. Such software is termed safety-related software.

- Safety-related software includes operating systems, system software, software in communication networks, human-computer interface functions, support tools and firmware as well as application programs.
- Application programs include high level programs, low level programs and special purpose programs in limited variability languages (see 3.2.7 of IEC 61508-4).

- c) requires that the software safety functions and software safety integrity levels are specified.

NOTE 1 – If this has already been done as part of the specification of the E/E/PE safety-related systems (see 7.2 of IEC 61508-2), then it does not have to be repeated in this part.

NOTE 2 – Specifying the software safety functions and software safety integrity levels is an iterative procedure; see figures 2 and 6.

NOTE 3 – See clause 5 and annex of IEC 61508-1 for documentation structure. The documentation structure may take account of company procedures, and of the working practices of specific application sectors.

- d) establishes requirements for safety lifecycle phases and activities which shall be applied during the design and development of the safety-related software (the software safety lifecycle model). These requirements include the application of measures and techniques, which are graded against the safety integrity level, for the avoidance of and control of faults and failures in the software.
- e) provides requirements for information relating to the software safety validation to be passed to the organisation carrying out the E/E/PES integration.
- f) provides requirements for the preparation of information and procedures concerning software needed by the user for the operation and maintenance of the E/E/PE safety-related system.
- g) provides requirements to be met by the organisation carrying out modifications to safety-related software.
- h) provides, in conjunction with IEC 61508-1 and IEC 61508-2, requirements for support tools such as development and design tools, language translators, testing and debugging tools, configuration management tools.

NOTE 4 – Figures 4 and 6 show the relationship between IEC 61508-2 and IEC 61508-3.