Australian Standard®

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

Part 1: General requirements

This Australian Standard® was prepared by Committee IT-006, Industrial Process Measurement, Control and Automation. It was approved on behalf of the Council of Standards Australia on 10 March 2011.
This Standard was published on 28 March 2011.

The following are represented on Committee IT-006:

- Australia Safety Critical Systems Association
- Australian Computer Society
- Australian Petroleum Production and Exploration Association
- Consult Australia
- Consumers Federation of Australia
- Engineers Australia
- Institute of Chemical Engineers Australia
- Institute of Instrumentation, Control and Automation Australia
- Process Control Society
- The University of Queensland
- Workplace Health and Safety Queensland
- WorkSafe Victoria

This Standard was issued in draft form for comment as DR AS 61508.1.

Standards Australia wishes to acknowledge the participation of the expert individuals that contributed to the development of this Standard through their representation on the Committee and through the public comment period.

Keeping Standards up-to-date

Australian Standards® are living documents that 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Standards may also be withdrawn.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 that may have been published since the Standard was published.

Detailed information about Australian Standards, drafts, amendments and new projects can be found by visiting **www.standards.org.au**

Standards Australia welcomes suggestions for improvements, and encourages readers to notify us immediately of any apparent inaccuracies or ambiguities. Contact us via email at **mail@standards.org.au**, or write to Standards Australia, GPO Box 476, Sydney, NSW 2001.

Australian Standard®

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

Part 1: General requirements

Originally as AS 61508.1—1999.
Second edition 2011.

Published by SAI Global Limited under licence from Standards Australia Limited, GPO Box 476, Sydney, NSW 2001, Australia

ISBN 978 0 7337 9796 5

PREFACE

This Standard was prepared by the Standards Australia Committee IT-006, Industrial Process Measurement, Control and Automation, to supersede AS 61508.1—1999.

The objective of this revision is to adopt the current edition of IEC 61508-1.

This Standard is identical with, and has been reproduced from IEC 61508-1 Ed.2.0 (2010), *Functional safety of electrical/electronic/programmable electronic safety-related systems—Part 1: General requirements*.

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

(a) Its number appears on the cover and title page while the international standard number appears only on the cover.

(b) In the source text 'this International Standard' should read 'this Australian Standard'.

(c) A full point substitutes for a comma when referring to a decimal marker.

References to International Standards should be replaced by references to Australian or Australian/New Zealand Standards, as follows:

Reference to International Standard		*Australian Standard*	
IEC		AS	
61508	Functional safety of electrical/electronic/programmable electronic safety-related systems	61508	Functional safety of electrical/electronic/programmable electronic safety-related systems
61508-2	Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems	61508.2	Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems
61508-3	Part 3: Software requirements	61508.3	Part 3: Software requirements
61508-4	Part 4: Definitions and abbreviations	61508.4	Part 4: Definitions and abbreviations
Guide 104	The preparation of safety publications and the use of basic safety publications and group safety publications	—	
ISO/IEC			
Guide 51	Guidelines for their inclusion in standards	—	

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

CONTENTS

Page

1 Scope 9
2 Normative references 12
3 Definitions and abbreviations 12
4 Conformance to this standard 12
5 Documentation 13
5.1 Objectives 13
5.2 Requirements 13
6 Management of functional safety 14
6.1 Objectives 14
6.2 Requirements 14
7 Overall safety lifecycle requirements 17
7.1 General 17
7.1.1 Introduction 17
7.1.2 Objectives and requirements – general 20
7.1.3 Objectives 25
7.1.4 Requirements 25
7.2 Concept 25
7.2.1 Objective 25
7.2.2 Requirements 26
7.3 Overall scope definition 26
7.3.1 Objectives 26
7.3.2 Requirements 26
7.4 Hazard and risk analysis 27
7.4.1 Objectives 27
7.4.2 Requirements 27
7.5 Overall safety requirements 28
7.5.1 Objective 29
7.5.2 Requirements 29
7.6 Overall safety requirements allocation 30
7.6.1 Objectives 30
7.6.2 Requirements 31
7.7 Overall operation and maintenance planning 35
7.7.1 Objective 35
7.7.2 Requirements 35
7.8 Overall safety validation planning 37
7.8.1 Objective 37
7.8.2 Requirements 37
7.9 Overall installation and commissioning planning 38
7.9.1 Objectives 38
7.9.2 Requirements 38
7.10 E/E/PE system safety requirements specification 38
7.10.1 Objective 39
7.10.2 Requirements 39
7.11 E/E/PE safety-related systems – realisation 41

7.11.1 Objective 41
7.11.2 Requirements 41
7.12 Other risk reduction measures – specification and realisation 41
7.12.1 Objective 41
7.12.2 Requirements 41
7.13 Overall installation and commissioning 41
7.13.1 Objectives 41
7.13.2 Requirements 42
7.14 Overall safety validation 42
7.14.1 Objective 42
7.14.2 Requirements 42
7.15 Overall operation, maintenance and repair 43
7.15.1 Objective 43
7.15.2 Requirements 43
7.16 Overall modification and retrofit 46
7.16.1 Objective 46
7.16.2 Requirements 47
7.17 Decommissioning or disposal 48
7.17.1 Objective 48
7.17.2 Requirements 48
7.18 Verification 49
7.18.1 Objective 49
7.18.2 Requirements 49
8 Functional safety assessment 50
8.1 Objective 50
8.2 Requirements 50
Annex A (informative) Example of a documentation structure 54
Bibliography 60

Figure 1 – Overall framework of the IEC 61508 series 11
Figure 2 – Overall safety lifecycle 18
Figure 3 – E/E/PE system safety lifecycle (in realisation phase) 19
Figure 4 – Software safety lifecycle (in realisation phase) 19
Figure 5 – Relationship of overall safety lifecycle to the E/E/PE system and software safety lifecycles 20
Figure 6 – Allocation of overall safety requirements to E/E/PE safety-related systems and other risk reduction measures 32
Figure 7 – Example of operations and maintenance activities model 45
Figure 8 – Example of operation and maintenance management model 46
Figure 9 – Example of modification procedure model 48
Figure A.1 – Structuring information into document sets for user groups 59

Table 1 – Overall safety lifecycle – overview 21
Table 2 – Safety integrity levels – target failure measures for a safety function operating in low demand mode of operation 33
Table 3 – Safety integrity levels – target failure measures for a safety function operating in high demand mode of operation or continuous mode of operation 34

Table 4 – Minimum levels of independence of those carrying out functional safety assessment (overall safety lifecycle phases 1 to 8 and 12 to 16 inclusive (see Figure 2)) 53

Table 5 – Minimum levels of independence of those carrying out functional safety assessment (overall safety lifecycle phases 9 and 10, including all phases of E/E/PE system and software safety lifecycles (see Figures 2, 3 and 4)) 53

Table A.1 – Example of a documentation structure for information related to the overall safety lifecycle 56

Table A.2 – Example of a documentation structure for information related to the E/E/PE system safety lifecycle..... 57

Table A.3 – Example of a documentation structure for information related to the software safety lifecycle 58

INTRODUCTION

Systems comprised of electrical and/or electronic elements have been used for many years to perform safety functions in most application sectors. Computer-based systems (generically referred to as programmable electronic systems) 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 these 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 (E/E/PE) elements 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 product and application sector international standards based on the IEC 61508 series.

NOTE 1 Examples of product and application sector international standards based on the IEC 61508 series are given in the Bibliography (see references [1], [2] and [3]).

In most situations, safety is achieved by a number of 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 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 recognized that there is a great variety of applications using E/E/PE safety-related systems in a variety of application sectors and covering a wide range of complexity, hazard 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 product and application sector international standards and in revisions of those that already exist.

This International Standard

- considers all relevant overall, E/E/PE system and software safety lifecycle phases (for example, from initial concept, through design, implementation, operation and maintenance to decommissioning) when E/E/PE systems 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 product and application sector international standards, dealing with E/E/PE safety-related systems, to be developed; the development of product and 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;

  adopts a risk-based approach by which the safety integrity requirements can be determined;
- introduces 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;

NOTE 2 The standard does not specify the safety integrity level requirements for any safety function, nor does it mandate how the safety integrity level is determined. Instead it provides a risk-based conceptual framework and example techniques.

– sets target failure measures for safety functions carried out by E/E/PE safety-related systems, which are linked to the safety integrity levels;

– sets a lower limit on the target failure measures for a safety function carried out by 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 a dangerous failure on demand of 10^{-5};

  – a high demand or a continuous mode of operation, the lower limit is set at an average frequency of a dangerous failure of 10^{-9} [h^{-1}];

NOTE 3 A single E/E/PE safety-related system does not necessarily mean a single-channel architecture.

NOTE 4 It may be possible to achieve designs of safety-related systems with lower values for the target safety integrity for non-complex systems, but these limits are considered to represent what can be achieved for relatively complex systems (for example programmable electronic safety-related systems) at the present time.

– sets requirements for the avoidance and control of systematic faults, which are based on experience and judgement from practical experience gained in industry. Even though the probability of occurrence of systematic failures cannot in general be quantified the standard does, however, allow a claim to be made, for a specified safety function, that the target failure measure associated with the safety function can be considered to be achieved if all the requirements in the standard have been met;

– introduces systematic capability which applies to an element with respect to its confidence that the systematic safety integrity meets the requirements of the specified safety integrity level;

– adopts a broad range of principles, techniques and measures to achieve functional safety for E/E/PE safety-related systems, but does not explicitly use the concept of fail safe. However, the concepts of “fail safe” and “inherently safe” principles may be applicable and adoption of such concepts is acceptable providing the requirements of the relevant clauses in the standard are met.

AUSTRALIAN STANDARD

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

Part 1:
General requirements

1 Scope

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

1.2 In particular, this standard

a) applies to safety-related systems when one or more of such systems incorporates electrical/electronic/programmable electronic elements;

NOTE 1 In the context of low complexity E/E/PE safety-related systems, certain requirements specified in this standard may be unnecessary, and exemption from compliance with such requirements is possible (see 4.2, and the definition of a low complexity E/E/PE safety-related system in 3.4.3 of IEC 61508-4).

NOTE 2 Although a person can form part of a safety-related system (see 3.4.1 of IEC 61508-4), human factor requirements related to the design of E/E/PE safety-related systems are not considered in detail in this standard.

b) is generically-based and applicable to all E/E/PE safety-related systems irrespective of the application;

c) covers the achievement of a tolerable risk through the application of E/E/PE safety-related systems, but does not cover hazards arising from the E/E/PE equipment itself (for example electric shock);

d) applies to all types of E/E/PE safety-related systems, including protection systems and control systems;

e) does not cover E/E/PE systems where

   – a single E/E/PE system is capable on its own of meeting the tolerable risk, and

   – the required safety integrity of the safety functions of the single E/E/PE system is less than that specified for safety integrity level 1 (the lowest safety integrity level in this standard).

f) is mainly concerned with the E/E/PE safety-related systems whose failure could have an impact on the safety of persons and/or the environment; however, it is recognized that the consequences of failure could also have serious economic implications and in such cases this standard could be used to specify any E/E/PE system used for the protection of equipment or product;

NOTE 3 See 3.1.1 of IEC 61508-4.

g) considers E/E/PE safety-related systems and other risk reduction measures, in order that the safety requirements specification for the E/E/PE safety-related systems can be determined in a systematic, risk-based manner;

h) uses an overall safety lifecycle model as the technical framework for dealing systematically with the activities necessary for ensuring the functional safety of the E/E/PE safety-related systems;