AS 61508 Supp1—2012

AS 61508 Supplement 1—2012

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

Supplement 1: Commented version

(Supplement 1 to AS 61508 series)

STANDARDS Australia

This Australian Standard Supplement was prepared by Committee IT-006, Industrial Process Measurement, Control and Automation. It was approved on behalf of the Council of Standards Australia on 16 March 2012.
This Supplement was published on 28 March 2012.

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

Standards Australia wishes to acknowledge the participation of the expert individuals that contributed to the development of this Supplement through their representation on the Committee.

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Standards may also be withdrawn.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.

AS 61508 Supplement 1—2012

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

Supplement 1: Commented version

(Supplement 1 to AS 61508 series)

First published as AS 61508 Supp1—2012.

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

ISBN 978 1 74342 038 6

PREFACE

This Supplement was prepared by the Standards Australia Committee IT-006, Industrial Process Measurement, Control and Automation.

This Supplement is identical with and has been reproduced from *S+ IEC 61508 Commented Version—Functional safety of electrical/electronic/programmable electronic safety-related systems* as a supplement to the AS 61508 series.

The AS 61508 series comprises:

AS	
61508	Functional safety of electrical/electronic/programmable electronic safety-related systems
61508.1	Part 1: General requirements
61508.2	Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems
61508.3	Part 3: Software requirements
61508.4	Part 4: Definitions and abbreviations
61508.5	Part 5: Examples of methods for the determination of safety integrity levels
61508.6	Part 6: Guidelines on the application of AS 61508.2 and AS 61508.3
61508.7	Part 7: Overview of techniques and measures

The IEC 61508 Commented Version is a marked-up and commented single-file PDF version of IEC 61508 Parts 1 to 7; complete with bookmarks, links and cross-references; and enriched with:

- track changes in red, highlighting all the changes made to the technical content of Edition 1.0;
- hundreds of comments by a leading expert in Functional Safety, indicated by a yellow-background number. Mousing over a number will display a pop-up note with a comment;
- figures associated with comments, indicated by a green paperclip; and
- a summary of comments and attachments, provided at the end of the file.

The single-file PDF Commented Version is enabled for user commenting and reviewing.

A separately published document AS 61508.0—2006, *Functional safety of electrical/electronic/programmable electronic safety-related systems*, Part 0: *Functional safety and AS 61508*, (adopted from IEC/TR 61508-0:2005) introduces the concept of functional safety and gives an overview of the AS 61508 series of standards. You should read AS 61508.0—2006 if you—

- wish to know whether AS 61508 applies to you;
- are involved in the development of electrical, electronic or programmable; electronic systems which may have safety implications; or
- are drafting any other standard where functional safety is a relevant factor.

INTERNATIONAL ELECTROTECHNICAL COMMISSION

FUNCTIONAL SAFETY OF ELECTRICAL/ELECTRONIC/ PROGRAMMABLE ELECTRONIC SAFETY-RELATED SYSTEMS –

Part 1: General requirements

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of 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, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). 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. 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 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 IEC National Committees.
3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
6) All users should ensure that they have the latest edition of this publication.
7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

DISCLAIMER
This Redline version is not an official IEC Standard and is intended only to provide the user with an indication of what changes have been made to the previous version. Only the current version of the standard is to be considered the official document.

This Redline version provides you with a quick and easy way to compare all the changes between this standard and its previous edition. Additions and deletions are displayed in red, with deletions being struck through.

International Standard IEC 61508-1 has been prepared by subcommittee 65A: System aspects, of IEC technical committee 65: Industrial-process measurement, control and automation.

This second edition cancels and replaces the first edition published in 1998. This edition constitutes a technical revision.

This edition has been subject to a thorough review and incorporates many comments received at the various revision stages.

It has the status of a basic safety publication according to IEC Guide 104.

The text of this standard is based on the following documents:

FDIS	Report on voting
65A/548/FDIS	65A/572/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 2.

A list of all parts of the IEC 61508 series, published under the general title *Functional safety of electrical / electronic / programmable electronic safety-related systems*, can be found on the IEC website.

The committee has decided that the contents of this publication will remain unchanged until the maintenance result date indicated on the IEC web site under "http://webstore.iec.ch" in the data related to the specific publication. 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~~ elements (1) 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 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 ~~components (electrical/electronic/programmable electronic systems (E/E/PESs))~~ (E/E/PE) (2) elements (1) 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 ~~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 (1) 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 recognized that there is a great variety of ~~E/E/PES~~ 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 that application. This International Standard, by being generic, will enable such measures to be formulated in future product and (10) application sector international standards and in revisions of those that already exist.

This International Standard

– considers all relevant overall, E/E/PE~~S~~ system (2) and software safety lifecycle phases (for example, from initial concept, through design, implementation, operation and maintenance to decommissioning) when E/E/PE~~Ss~~ systems (2) 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 ~~E/E/PESs~~ systems (2), to be developed; the development of product and (10) 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 ~~for the determination of~~ by which the safety integrity ~~level~~ requirements can be determined;

– ~~uses~~ 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 ~~numerical~~ (3) 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~~, in a dangerous mode of failure, that can be claimed~~ for a safety function carried out by a single E/E/PE safety-related system (4). 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~~ a dangerous failure on demand of 10^{-5} ~~to perform its design function on demand~~;(4)

  – a high demand or a continuous mode of operation, the lower limit is set at ~~a probability~~ an average frequency of a dangerous failure of 10^{-9} ~~per hour~~ [h^{-1}];(4)

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.(6)

– 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;(7)

– introduces systematic capability which applies to an element (1) with respect to its confidence that the systematic safety integrity meets the requirements of the specified safety integrity level;(8)

– 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 ~~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.~~(5) 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.(9)

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 ~~(E/E/PESs)~~ (2) 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 ~~dual~~ second objective of this standard is to enable the development of ~~electrical/electronic/programmable electronic (E/E/PE)~~ safety-related systems where product or application sector international standards ~~may~~ do not exist.(10)

1.2 In particular, this standard

a) applies to safety-related systems when one or more of such systems incorporates electrical/electronic/programmable electronic ~~devices~~ elements;(1)

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 ~~3.4.4~~ 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; ~~1)~~

c) ~~covers possible hazards caused by failures of the safety functions to be performed by E/E/PE safety-related systems (i.e. distinct from hazards arising from the E/E/PE equipment itself (for example electric shock etc);~~ covers the achievement of a tolerable risk through the application of E/E/PE safety-related systems, but does not cover hazards (52) arising from the E/E/PE equipment itself (for example electric shock);(11)

d) applies to all types of E/E/PE safety-related systems, including protection systems and control systems;(12)

~~de~~) does not cover E/E/PE systems where

- a single E/E/PE system is capable ~~of providing the necessary risk reduction~~ 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).(4)

~~ef~~) 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.

~~1)~~ Applies to French text only.