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which subscribing members receive, and which gives details of new publications, new editions and amendments, and of withdrawn Standards.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.

Published by Standards Australia
(Standards Association of Australia)
1 The Crescent, Homebush NSW 2140

ISBN 0 7337 2878 2

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 Standards 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 identity 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.

CONTENTS

Page

Page

Figures

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 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/PE applications 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 application sector international standards.

This International Standard

– considers all relevant overall, E/E/PES and software safety lifecycle phases (for example, from initial concept, through design, implementation, operation and maintenance to decommissioning) when E/E/PESs 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/PESs, 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 A 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.