AS 61508.5—1999
IEC 61508-5:1998

Australian Standard™

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

Part 5: Examples of methods for the determination of safety integrity levels

This Australian Standard was prepared by Committee IT/6, Information Technology for Industrial Automation 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

This Standard was issued in draft form for comment as DR 99168.

Australian Standard™

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

Part 5: Examples of methods for the determination of safety integrity levels

First published as AS 61508.5—1999.

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

ISBN 0 7337 2876 6

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 61508-5:1998, *Functional safety of electrical/electronic/ programmable electronic safety-related systems*, Part 5: *Examples of methods for the determination of safety integrity levels*.

The objective of this Standard is to provide designers of electrical/electronic/programmable electronic devices used in safety-related applications with the concepts and relationship of risk to safety integrity together with methods of determining safety integrity levels.

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 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.

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

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 recognised that there is a great variety of E/E/PES 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 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.

NOTES

STANDARDS AUSTRALIA

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

Part 5: Examples of methods for the determination of safety integrity levels

1 Scope

1.1 This part of IEC 61508 provides information on

– the underlying concepts of risk and the relationship of risk to safety integrity (see annex A);

– a number of methods that will enable the safety integrity levels for the E/E/PE safety-related systems, other technology safety-related systems and external risk reduction facilities to be determined (see annexes B, C, D and E).

1.2 The method selected will depend upon the application sector and the specific circumstances under consideration. Annexes B, C, D and E illustrate quantitative and qualitative approaches and have been simplified in order to illustrate the underlying principles. These annexes have been included to illustrate the general principles of a number of methods but do not provide a definitive account. Those intending to apply the methods indicated in these annexes should consult the source material referenced.

NOTE – For more information on the approaches illustrated in annexes B, D and E, see references [4], [2] and [3] respectively in annex F. See also reference [5] in annex F for a description of an additional approach.

1.3 Parts 1, 2, 3 and 4 of this standard 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 ISO/IEC Guide 51. One of the responsibilities of a technical committee is, wherever applicable, to make use of basic safety publications in the preparation of its own publications. IEC 61508 is also intended for use as a stand-alone standard.

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 in the USA and Canada, 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 IEC 61508 and indicates the role that IEC 61508-5 plays in the achievement of functional safety for E/E/PE safety-related systems.