AS 4048.1(Int)—1992
IEC 65A (Secretariat) 123
(Expires 14 September 1994)

WITHDRAWN
EXPIRY DATE REACHED
TAS DECEMBER 1994

Interim Australian Standard®

Functional safety of electrical/ electronic/programmable electronic systems—Generic aspects

Part 1: General requirements

STANDARDS AUSTRALIA

This Interim Australian Standard was prepared by Committee IT/6, Information Processing Systems for Industrial Automation. It was approved on behalf of the Council of Standards Australia on 19 June 1992 and published on 14 September 1992.

The following interests are represented on Committee IT/6:

The Association of Consulting Engineers Australia
Australian Electrical and Electronic Manufacturers Associati[illegible]
Australian Information Industry Association
Confederation of Australian Industry
Department of Technical and Further Education, N.[illegible]W.
Division of Manufacturing Technology, CS[illegible]O
University of Melbourne
University of New South Wales

Revie[illegible]f A[illegible]tralian Standards. To keep abreast of progress in industry, Australian Standards are subject to [illegible]riod[illegible] review and are kept up to date by the issue of amendments or new editions as necessary. It is im[illegible]ort[illegible]t therefore that Standards users ensure that they are in possession of the latest edition, and any a[illegible]dments thereto.

Full deta[illegible]s of all Australian Standards and related publications will be found in the Standards Australia [illegible]talogue 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which subscribing members receive, and which gives details of new publications, new editions and amendments, and of withdrawn Standards.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 91247.

Interim Australian Standard®

Functional safety of electrical/ electronic/programmable electronic systems—Generic aspects

Part 1: General requirements

First published as AS 4048.1(Int)—1992.

PUBLISHED BY STANDARDS AUSTRALIA
(STANDARDS ASSOCIATION OF AUSTRALIA)
STANDARDS HOUSE, 80 ARTHUR ST, NORTH SYDNEY NSW
ISBN 0 7262 7654 5

PREFACE

This Interim Standard was prepared by the Standards Australia Committee on Information Systems for Industrial Automation.

The purpose of the Interim Standard is to provide guidelines on the aspects that need to be addressed when programmable electronic systems are used to carry out safety functions. This standard is based on the international committee draft which has still not been finalised. It is, however, at a stage which will provide guidance and assistance to users. Accordingly, it is now being made available.

Standards Australia invites comment on this Interim Standard from persons and organizations concerned with this subject. The date of expiry for comment is 2 years after publication at which time this Interim Australian Standard will either be confirmed, withdrawn or revised in the light of public comment.

For the purpose of this Interim Standard the term 'tolerable risk' does not necessarily mean the exclusion of safeguarding requirements. It should be read in conjunction with the requirements of the local statutory authority. This definition of tolerable risk will be confirmed prior to publication of the Standard.

During the life of this document the committee will monitor all comment as it is received.

Attention is drawn to the fact that this document is an Interim Australian Standard and should be regarded as a developmental Standard liable to future alteration.

Under arrangement made between Standards Australia and the International Standards bodies, ISO and IEC as well as certain other Standards organizations, users of this Australian Standard are advised of the following:

(a) Copyright is vested in Standards Australia.

(b) The number of this Standard is not reproduced on each page; its identity is shown only on the cover and title pages.

For the purpose of this Interim Australian Standard, the IEC text should be modified as follows:

(i) *Terminology* The words 'Interim Australian Standard' should replace the words 'International Standard' wherever they appear.

(ii) *References* The references to International Standards should be replaced by references to Australian Standards as below.

Reference to International Standard		*Australian Standard*	
ISO		AS	
9001	Quality Systems—Model for quality assurance in design, development, production, installation and servicing	3901	Quality systems for design/development, production, installation and servicing

CONTENTS

FIGURES:

TABLES:

INTRODUCTION

Electrical/electronic systems 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 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.

In most situations, safety is achieved by a number of protective systems and rely on many technologies (mechanical/hydraulic/pneumatic/electrical/electronic/programmable electronic). Any safety strategy must therefore consider not only all the elements within an individual system (eg. sensors/controlling device/ actuators) but also all the safety-related systems making up the total combination of safety-related systems. Therefore, whilst this International Standard is primarily concerned with E/E/PESs, it nevertheless provides a safety framework within which safety-related systems based on other technologies can be addressed.

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 potential. In any specific application, the exact prescription of safety measures will be dependent upon many factors specific to the application. This International Standard, by being at a generic level, will enable such a prescription to be formulated in future application-specific International Standards.

This International Standard:

- addresses all relevant Safety Lifecycle phases (eg. from initial concept, through ..... design, implementation, operation and maintenance ..... to decommissioning) when E/E/PESs are used to perform safety functions;
- has been developed with a rapidly developing technology in mind. Programmable electronic technology is rapidly developing and it is important that the framework set out in this International Standard is sufficiently robust and comprehensive to cater for future developments;
- enables application specific International Standards, dealing with safety-related E/E/PESs, to be developed. The development of application-specific International Standards, within the framework of this International Standard, should lead to a high level of consistency (eg. of underlying principles, terminology, documentation etc) both within application-sectors and across application sectors. This will have both safety and economic benefits.

This International Standard is Part 1 of a series; future parts are under consideration. It is intended that future parts will cover the detailed requirements of E/E/PES safety-related systems. A key objective will be to facilitate the development of application-specific standards.

The considerations underlying the guidance are given in Annexes A and B.

STANDARDS AUSTRALIA

Interim Australian Standard

Functional safety of electrical/electronic/programmable electronic systems—Generic aspects

Part 1: General requirements

1. SCOPE

This International Standard covers those aspects that need to be addressed when electrical/electronic/programmable electronic systems (E/E/PES) are used to carry out safety functions. A major objective of the International Standard is to enable the development of **application-specific International Standards** by the Technical Committees responsible for the application sector. This will allow all the relevant factors, associated with the application to be fully taken into account and thereby meet the specific needs (technical, personnel competencies, work practices etc) of the application sector. (See Clause 12)

In particular the International Standard:

- applies to safety-related systems when one or more of such systems incorporate electrical/electronic/programmable electronic devices.
- is generically based and applicable to all safety-related systems irrespective of the application. Examples of the application sectors coming within the scope of the Standard include:
  - process industries (emergency-shutdown systems, fire and gas detection systems, burner controls);
  - manufacturing industries (industrial robots, machine tools);
  - transportation (railway signalling, braking systems, lifts);
  - medical (miscellaneous electro-medical apparatus, radiography);
- specifies the requirements for achieving functional safety of the safety-related systems and external risk reduction facities but does not specify those who shall be responsible for implementing the requirements (eg. designers, suppliers, users, contractors or others). The allocation of responsibilities is the responsibility of the Safety Management (see Clause 6).
- is mainly concerned with safety to persons but is also applicable to environmental issues;
- applies to the total combination of safety-related systems;
- uses a **Safety Lifecycle Model** for all activities necessary for ensuring that the required system-integrity levels are met for the safety-related systems under consideration.

  NOTE: 1) Although the Safety Lifecycle is primarily concerned with E/E/PES safety-related systems, it does provide an overall framework which is applicable to any safety-related system irrespective of the technology of the system (eg. electrical/electronic/programmable electronic/ mechanical/hydraulic/pneumatic).
- specifies the safety requirements to achieve an adequate level of **Functional Safety** for the safety-related systems by means of a **Safety Requirements Specification** which is divided into a :
  - **Functional Requirements Specification; and,**
  - **Safety Integrity Requirements Specification.**