AS IEC 61511.1—2004
IEC 61511-1:2003

Australian Standard™

Functional safety—Safety instrumented systems for the process industry sector

Part 1: Framework, definitions, systems, hardware and software requirements

STANDARDS AUSTRALIA

This Australian Standard was prepared by Committee IT-006, Information Technology for Industrial Automation and Integration. It was approved on behalf of the Council of Standards Australia on 5 March 2004 and published on 10 May 2004.

The following are represented on Committee IT-006:

Association of Consulting Engineers Australia

Australian Electrical and Electronic Manufacturers Association

CSIRO Centre for Planning and Design

CSIRO Manufacturing & Infrastructure Technology

Department of Defence (Australia)

Institute of Instrumentation, Control and Automation Australia

Institution of Engineers Australia

Monash University

RMIT University

The University of Melbourne

Keeping Standards up-to-date

Standards are living documents which 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 Standards may also be withdrawn.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 which may have been published since the Standard was purchased.

Detailed information about Standards can be found by visiting the Standards Web Shop at www.standards.com.au and looking up the relevant Standard in the on-line catalogue.

Alternatively, the printed Catalogue provides information current at 1 January each year, and the monthly magazine, *The Global Standard*, has a full listing of revisions and amendments published each month.

Australian Standards™ and other products and services developed by Standards Australia are published and distributed under contract by SAI Global, which operates the Standards Web Shop.

We also welcome suggestions for improvement in our Standards, and especially encourage readers to notify us immediately of any apparent inaccuracies or ambiguities. Contact us via email at mail@standards.org.au, or write to the Chief Executive, Standards Australia International Ltd, GPO Box 5420, Sydney, NSW 2001.

This Standard was issued in draft form for comment as DR 04055.

Australian Standard™

Functional safety—Safety instrumented systems for the process industry sector

Part 1: Framework, definitions, systems, hardware and software requirements

First published as AS IEC 61511.1—2004.

Published by Standards Australia International Ltd
GPO Box 5420, Sydney, NSW 2001, Australia

ISBN 0 7337 5913 0

PREFACE

This Standard was prepared by the Standards Australia Committee IT-006, Information Technology for Industrial Automation and Integration.

This Standard is identical with, and has been reproduced from, IEC 61511-1:2003, *Functional safety—Safety instrumented systems for the process industry sector*—Part 1: *Framework, definitions, systems, hardware and software requirements*.

The objective of this Standard is to provide requirements for the specification, design, installation, operation and maintenance of a safety instrumented system, so that it can be confidently entrusted to place and/or maintain the process in a safe state.

This Standard is Part 1 of AS IEC 61511, *Functional safety—Safety instrumented systems for the process industry sector*, which is published in parts as follows:

Part 1: Framework, definitions, system, hardware and software requirements (this Standard)
Part 2: Guidelines for the application of AS IEC 61511-1
Part 3: Guidance for the determination of the required safety integrity levels

The terms ‘normative’ and ‘informative’ are used 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 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.

CONTENTS

INTRODUCTION vi

1 Scope 1
2 Normative references 6
3 Abbreviations and definitions 7
3.1 Abbreviations 7
3.2 Definitions 8
4 Conformance to this International Standard 22
5 Management of functional safety 22
5.1 Objective 22
5.2 Requirements 22
6 Safety life-cycle requirements 27
6.1 Objectives 27
6.2 Requirements 27
7 Verification 29
7.1 Objective 29
8 Process hazard and risk assessment 29
8.1 Objectives 29
8.2 Requirements 30
9 Allocation of safety functions to protection layers 31
9.1 Objectives 31
9.2 Requirements of the allocation process 31
9.3 Additional requirements for safety integrity level 4 32
9.4 Requirements on the basic process control system as a protection layer 32
9.5 Requirements for preventing common cause, common mode and dependent failures 33
10 SIS safety requirements specification 34
10.1 Objective 34
10.2 General requirements 34
10.3 SIS safety requirements 34
11 SIS design and engineering 35
11.1 Objective 35
11.2 General requirements 35
11.3 Requirements for system behaviour on detection of a fault 37
11.4 Requirements for hardware fault tolerance 38
11.5 Requirements for selection of components and subsystems 39
11.6 Field devices 42
11.7 Interfaces 43
11.8 Maintenance or testing design requirements 45
11.9 SIF probability of failure 45
12 Requirements for application software, including selection criteria for utility software 46
12.1 Application software safety life-cycle requirements 47
12.2 Application software safety requirements specification 53
12.3 Application software safety validation planning 55
12.4 Application software design and development 55
12.5 Integration of the application software with the SIS subsystem 60