

Australian Standard™

**Functional safety—Safety instrumented
systems for the process industry sector**

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

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 Standards may also be withdrawn.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.

COPYRIGHT

© Standards Australia International

All rights are reserved. No part of this work may be reproduced or copied in any form or by any means, electronic or mechanical, including photocopying, without the written permission of the publisher.

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

12.6	FPL and LVL software modification procedures.....	61
12.7	Application software verification.....	61
13	Factory acceptance testing (FAT).....	62
13.1	Objectives.....	62
13.2	Recommendations.....	62
14	SIS installation and commissioning.....	64
14.1	Objectives.....	64
14.2	Requirements.....	64
15	SIS safety validation.....	65
15.1	Objective.....	65
15.2	Requirements.....	65
16	SIS operation and maintenance.....	67
16.1	Objectives.....	67
16.2	Requirements.....	67
16.3	Proof testing and inspection.....	69
17	SIS modification.....	70
17.1	Objectives.....	70
17.2	Requirements.....	70
18	SIS decommissioning.....	71
18.1	Objectives.....	71
18.2	Requirements.....	71
19	Information and documentation requirements.....	71
19.1	Objectives.....	71
19.2	Requirements.....	72
	Annex A (informative) Differences.....	73
	Bibliography.....	74
	Figure 1 – Overall framework of this standard.....	vii
	Figure 2 – Relationship between IEC 61511 and IEC 61508.....	3
	Figure 3 – Relationship between IEC 61511 and IEC 61508 (see Clause 1).....	4
	Figure 4 – Relationship between safety instrumented functions and other functions.....	5
	Figure 5 – Relationship between system, hardware, and software of IEC 61511-1.....	6
	Figure 6 – Programmable electronic system (PES): structure and terminology.....	15
	Figure 7 – Example of SIS architecture.....	17
	Figure 8 – SIS safety life-cycle phases and functional safety assessment stages.....	25
	Figure 9 – Typical risk reduction methods found in process plants.....	33
	Figure 10 – Application software safety life cycle and its relationship to the SIS safety life cycle.....	47
	Figure 11 – Application software safety life cycle (in realization phase).....	49
	Figure 12 – Software development life cycle (the V-model).....	50
	Figure 13 – Relationship between the hardware and software architectures of SIS.....	53
	Table 1 – Abbreviations used in IEC 61511.....	7
	Table 2 – SIS safety life-cycle overview.....	27

Table 3 – Safety integrity levels: probability of failure on demand.....	31
Table 4 – Safety integrity levels: frequency of dangerous failures of the SIF	31
Table 5 – Minimum hardware fault tolerance of PE logic solvers.....	38
Table 6 – Minimum hardware fault tolerance of sensors and final elements and non-PE logic solvers	39
Table 7 – Application software safety life cycle: overview	51

INTRODUCTION

Safety instrumented systems have been used for many years to perform safety instrumented functions in the process industries. If instrumentation is to be effectively used for safety instrumented functions, it is essential that this instrumentation achieves certain minimum standards and performance levels.

This standard addresses the application of safety instrumented systems for the process industries. It also requires a process hazard and risk assessment to be carried out to enable the specification for safety instrumented systems to be derived. Other safety systems are only considered so that their contribution can be taken into account when considering the performance requirements for the safety instrumented systems. The safety instrumented system includes all components and subsystems necessary to carry out the safety instrumented function from sensor(s) to final element(s).

This standard has two concepts which are fundamental to its application; safety lifecycle and safety integrity levels.

This standard addresses safety instrumented systems which are based on the use of electrical/electronic/programmable electronic technology. Where other technologies are used for logic solvers, the basic principles of this standard should be applied. This standard also addresses the safety instrumented system sensors and final elements regardless of the technology used. This standard is process industry specific within the framework of IEC 61508 (see Annex A).

This standard sets out an approach for safety life-cycle activities to achieve these minimum standards. This approach has been adopted in order that a rational and consistent technical policy is used.

In most situations, safety is best achieved by an inherently safe process design. If necessary, this may be combined with a protective system or systems to address any residual identified risk. Protective systems can rely on different technologies (chemical, mechanical, hydraulic, pneumatic, electrical, electronic, programmable electronic). To facilitate this approach, this standard

- requires that a hazard and risk assessment is carried out to identify the overall safety requirements;
- requires that an allocation of the safety requirements to the safety instrumented system(s) is carried out;
- works within a framework which is applicable to all instrumented methods of achieving functional safety;
- details the use of certain activities, such as safety management, which may be applicable to all methods of achieving functional safety.

This standard on safety instrumented systems for the process industry

- addresses all safety life-cycle phases from initial concept, design, implementation, operation and maintenance through to decommissioning;
- enables existing or new country specific process industry standards to be harmonized with this standard.

This International Standard is intended to lead to a high level of consistency (for example, of underlying principles, terminology, information) within the process industries. This should have both safety and economic benefits.

In jurisdictions where the governing authorities (for example, national, federal, state, province, county, city) have established process safety design, process safety management, or other requirements, these take precedence over the requirements defined in this standard.

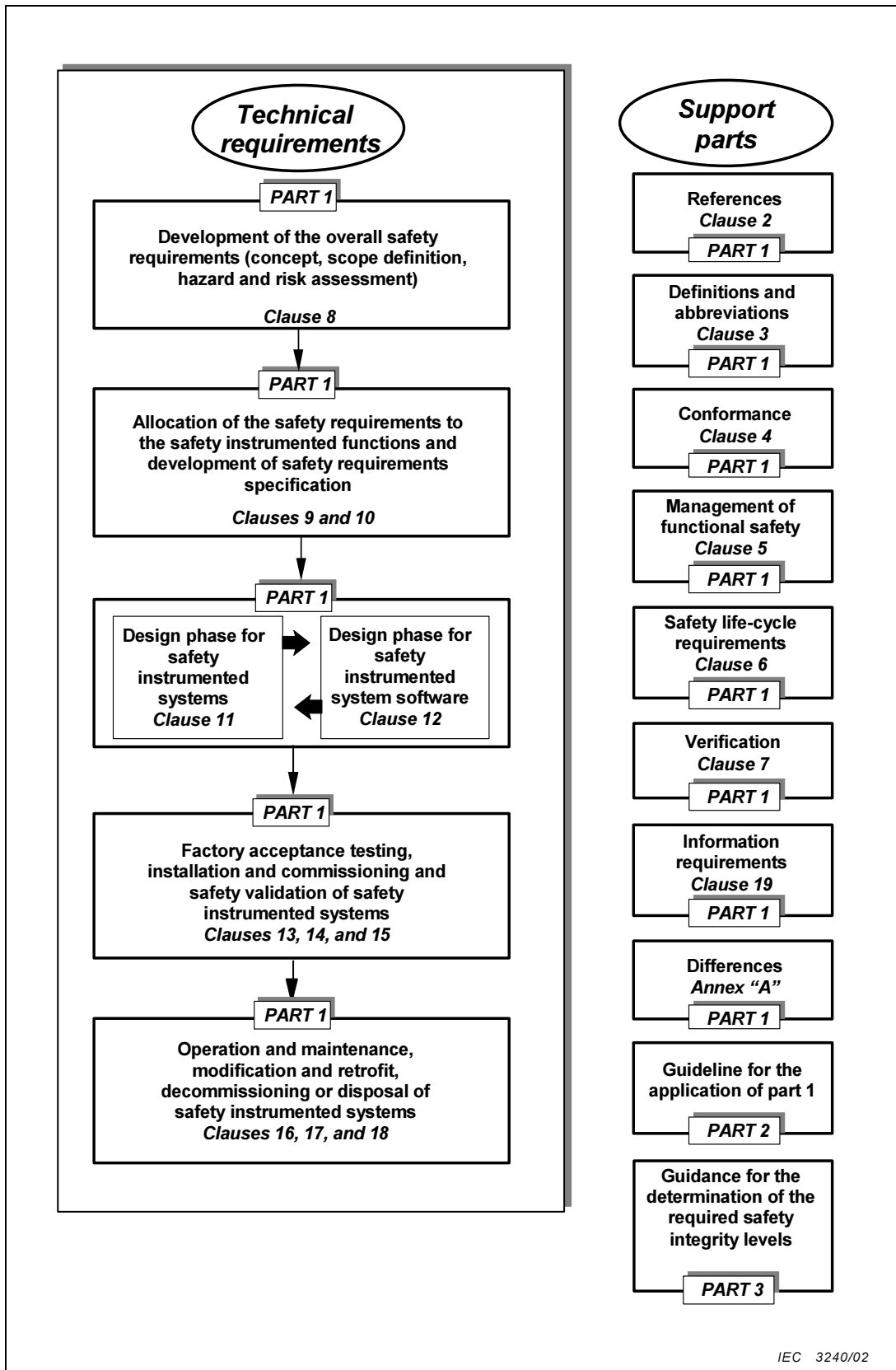


Figure 1 – Overall framework of this standard

STANDARDS AUSTRALIA

Australian Standard**Functional safety—Safety instrumented systems for the process industry sector****Part 1: Framework, definitions, systems, hardware and software requirements**

Any table, figure or text of the international standard that is struck through is not part of this standard. Any Australian/New Zealand table, figure or text that is added is part of this standard and is identified by shading.

1 Scope

This International Standard gives 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 has been developed as a process sector implementation of IEC 61508.

In particular, this standard

- a) specifies the requirements for achieving functional safety but does not specify who is responsible for implementing the requirements (for example, designers, suppliers, owner/operating company, contractor); this responsibility will be assigned to different parties according to safety planning and national regulations;
- b) applies when equipment that meets the requirements of IEC 61508, or of 11.5 of IEC 61511-1, is integrated into an overall system that is to be used for a process sector application but does not apply to manufacturers wishing to claim that devices are suitable for use in safety instrumented systems for the process sector (see IEC 61508-2 and IEC 61508-3);
- c) defines the relationship between IEC 61511 and IEC 61508 (Figures 2 and 3);
- d) applies when application software is developed for systems having limited variability or fixed programmes but does not apply to manufacturers, safety instrumented systems designers, integrators and users that develop embedded software (system software) or use full variability languages (see IEC 61508-3);
- e) applies to a wide variety of industries within the process sector including chemicals, oil refining, oil and gas production, pulp and paper, non-nuclear power generation;
NOTE Within the process sector some applications, (for example, off-shore), may have additional requirements that have to be satisfied.
- f) outlines the relationship between safety instrumented functions and other functions (Figure 4);
- g) results in the identification of the functional requirements and safety integrity requirements for the safety instrumented function(s) taking into account the risk reduction achieved by other means;
- h) specifies requirements for system architecture and hardware configuration, application software, and system integration;