AS IEC 61511.2—2004
IEC 61511-2:2003



Australian Standard™

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

## Part 2: Guidelines for the application of AS IEC 61511.1

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 Standards may also be withdrawn.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 04054.*

Australian Standard™

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

# Part 2: Guidelines for the application of AS IEC 61511.1

First published as AS IEC 61511.2—2004.



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

ISBN 0 7337 5914 9

# 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 61511-2:2003, *Functional safety—Safety instrumented systems for the process industry sector*—Part 2*: Guidelines for the application of IEC 61511-1*.

The objective of this Standard is to provide guidance on the specification, design, installation, operation and maintenance of Safety Instrumented Functions and related safety instrumented systems as defined in IEC 61511-1.

This Standard is Part 2 of AS IEC 61511—2004, *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
Part 2: Guidelines for the application of AS IEC 61511-1 (this Standard)
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 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 international standard’ should read ‘this Australian Standard’.

(c) A full point should be substituted for a comma when referring to a decimal marker.

# CONTENTS

INTRODUCTION ..... v

1 Scope ..... 1
2 Normative references ..... 1
3 Terms, definitions and abbreviations ..... 1
4 Conformance to this International Standard ..... 1
5 Management of functional safety ..... 1
5.1 Objective ..... 1
5.2 Requirements ..... 2
6 Safety lifecycle requirements ..... 7
6.1 Objectives ..... 7
6.2 Requirements ..... 8
7 Verification ..... 8
7.1 Objective ..... 8
8 Process hazard and risk assessment ..... 8
8.1 Objectives ..... 8
8.2 Requirements ..... 9
9 Allocation of safety functions to protection layers ..... 11
9.1 Objective ..... 11
9.2 Requirements of the allocation process ..... 11
9.3 Additional requirements for safety integrity level 4 ..... 13
9.4 Requirement on the basic process control system as a layer of protection ..... 13
9.5 Requirements for preventing common cause, common mode and dependent failures ..... 14
10 SIS safety requirements specification ..... 15
10.1 Objective ..... 15
10.2 General requirements ..... 15
10.3 SIS safety requirements ..... 15
11 SIS design and engineering ..... 17
11.1 Objective ..... 17
11.2 General requirements ..... 17
11.3 Requirements for system behaviour on detection of a fault ..... 21
11.4 Requirements for hardware fault tolerance ..... 21
11.5 Requirements for selection of components and subsystems ..... 22
11.6 Field devices ..... 24
11.7 Interfaces ..... 25
11.8 Maintenance or testing design requirements ..... 27
11.9 SIF probability of failure ..... 28
12 Requirements for application software, including selection criteria for utility software ..... 30
12.1 Application software safety lifecycle requirements ..... 30
12.2 Application software safety requirements specification ..... 33
12.3 Application software safety validation planning ..... 35
12.4 Application software design and development ..... 35
12.5 Integration of the application software with the SIS subsystem ..... 42

12.6 FPL and LVL software modification procedures ..... 42
12.7 Application software verification ..... 43
13 Factory acceptance testing (FAT) ..... 44
13.1 Objectives ..... 44
13.2 Recommendations ..... 44
14 SIS installation and commissioning ..... 44
14.1 Objectives ..... 44
14.2 Requirements ..... 45
15 SIS safety validation ..... 45
15.1 Objective ..... 45
15.2 Requirements ..... 45
16 SIS operation and maintenance ..... 46
16.1 Objectives ..... 46
16.2 Requirements ..... 46
16.3 Proof testing and inspection ..... 46
17 SIS modification ..... 47
17.1 Objective ..... 47
17.2 Requirements ..... 47
18 SIS decommissioning ..... 47
18.1 Objectives ..... 47
18.2 Requirements ..... 48
19 Information and documentation requirements ..... 48
19.1 Objectives ..... 48
19.2 Requirements ..... 48

Annex A (informative) Example of techniques for calculating the probability of failure on demand for a safety instrumented function ..... 49
Annex B (informative) Typical SIS architecture development ..... 50
Annex C (informative) Application features of a safety PLC ..... 55
Annex D (informative) Example of SIS logic solver application software development methodology ..... 57
Annex E (informative) Example of development of externally configured diagnostics for a safety-configured PE logic solver ..... 61

Figure 1 – Overall framework of this standard ..... vi
Figure 2 – BPCS function and initiating cause independence illustration ..... 14
Figure 3 – Software development lifecycle (the V-model) ..... 31
Figure C.1 – Logic solver ..... 56
Figure E.1 – EWDT timing diagram ..... 63

Table 1 – Typical Safety Manual organisation and contents ..... 40

# 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.

This International Standard addresses the application of safety instrumented systems for the Process Industries. It also deals with the interface between safety instrumented systems and other safety systems in requiring that a process hazard and risk assessment be carried out. The safety instrumented system includes sensors, logic solvers and final elements.

This International Standard has two concepts, which are fundamental to its application; safety lifecycle and safety integrity levels. The safety lifecycle forms the central framework which links together most of the concepts in this International Standard.

The safety instrumented system logic solvers addressed include Electrical (E)/Electronic (E)/ and Programmable Electronic (PE) technology. Where other technologies are used for logic solvers, the basic principles of this standard may also be applied. This standard also addresses the safety instrumented system sensors and final elements regardless of the technology used. This International Standard is process industry specific within the framework of the IEC 61508 series.

This International Standard sets out an approach for safety lifecycle activities to achieve these minimum standards. This approach has been adopted in order that a rational and consistent technical policy is used. The objective of this standard is to provide guidance on how to comply with IEC 61511-1.

To facilitate use of this standard, the clause and subclause numbers provided are identical to the corresponding normative text in 61511-1 (excluding the annexes).

In most situations, safety is best achieved by an inherently safe process design whenever practicable, combined, if necessary, with a number of protective systems which rely on different technologies (for example, chemical, mechanical, hydraulic, pneumatic, electrical, electronic, thermodynamic (for example, flame arrestors), programmable electronic) which manage any residual identified risk. Any safety strategy considers each individual safety instrumented system in the context of the other protective systems. 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 functions and related safety systems, such as 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 International Standard on safety instrumented systems for the process industry:

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

This 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.

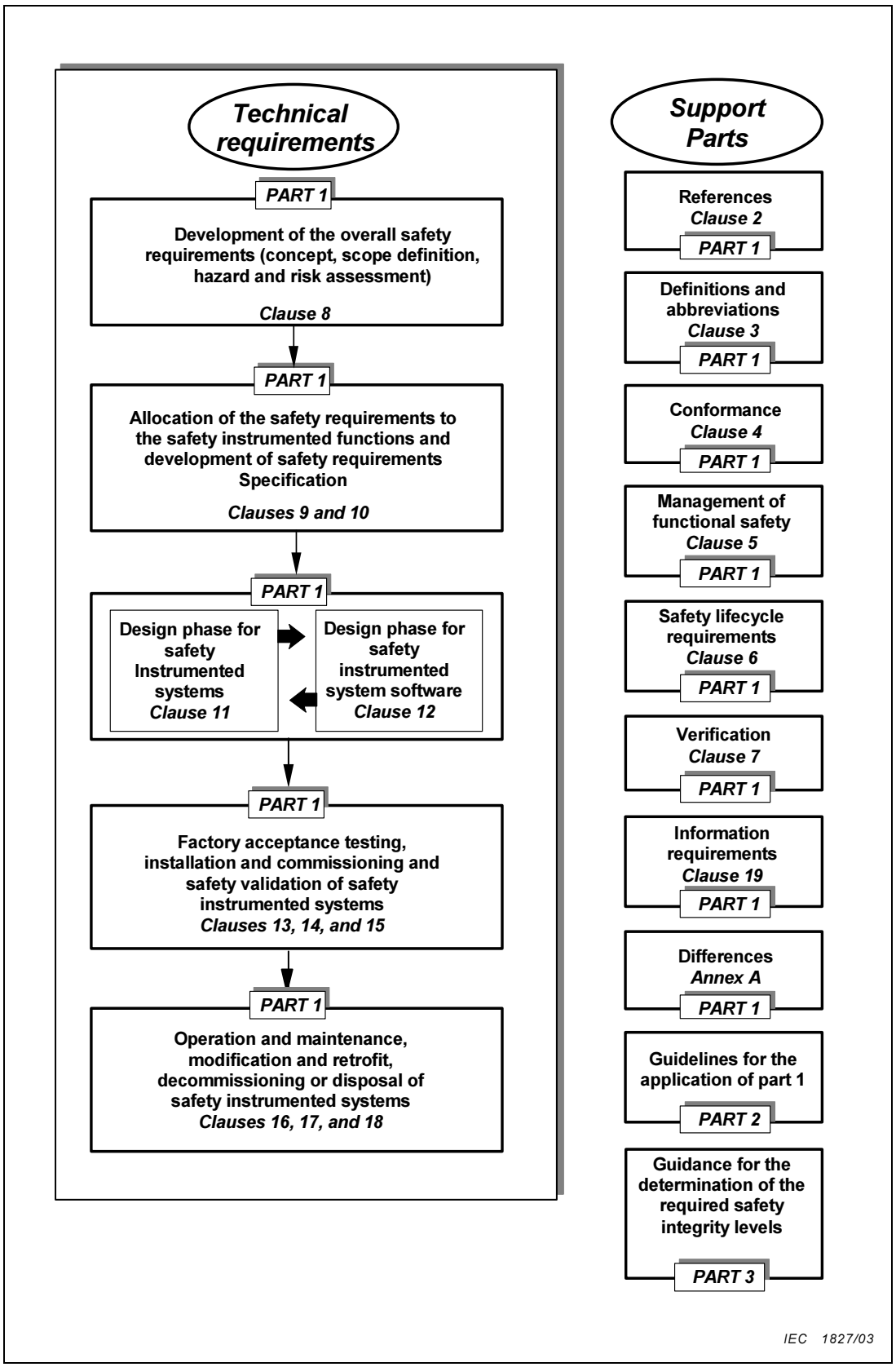


**Figure 1 – Overall framework of this standard**

STANDARDS AUSTRALIA

# Australian Standard

# Functional safety—Safety instrumented systems for the process industry sector
# Part 2: Guidelines for the application of AS IEC 61511.1

## 1 Scope

IEC 61511-2 provides guidance on the specification, design, installation, operation and maintenance of Safety Instrumented Functions and related safety instrumented system as defined in IEC 61511-1. This standard has been organized so that each clause and subclause number herein addresses the same clause number in IEC 61511-1 (with the exception of the annexes).

## 2 Normative references

No further guidance provided.

## 3 Terms, definitions and abbreviations

No further guidance provided except for 3.2.68 and 3.2.71 of IEC 61511-1.

**3.2.68** A safety function should prevent a specified hazardous event. For example, “prevent the pressure in vessel #ABC456 exceeding 100 bar.” A safety function may be achieved by

a) a single safety instrumented system (SIS), or

b) one or more safety instrumented systems and/or other layers of protection.

In case b), each safety instrumented system or other layer of protection has to be capable of achieving the safety function and the overall combination has to achieve the required risk reduction (process safety target).

**3.2.71** Safety instrumented functions are derived from the safety function, have an associated safety integrity level (SIL) and are carried out by a specific safety instrumented system (SIS). For example, “close valve #XY123 within 5 s when pressure in vessel #ABC456 reaches 100 bar”. Note that components of a safety instrumented system may be used by more than one safety instrumented function.

## 4 Conformance to this International Standard

No further guidance provided.

## 5 Management of functional safety

### 5.1 Objective

The objective of Clause 5 of IEC 61511-1 is to provide requirements for implementing the management activities that are necessary to ensure that the functional safety objectives are met.