AS IEC 61511.3—2004
IEC 61511-3:2003

Australian Standard™

Functional safety—Safety instrumented systems for the process industry sector

Part 3: Guidance for the determination of the required safety integrity levels

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 Standards may also be withdrawn.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 04053.

Australian Standard™

Functional safety—Safety instrumented systems for the process industry sector

Part 3: Guidance for the determination of the required safety integrity levels

First published as AS IEC 61511.3—2004.

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

ISBN 0 7337 5915 7

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 61511-3:2003, *Functional safety—Safety instrumented systems for the process industry sector*—Part 3*: Guidance for the determination of the required safety integrity levels*.

The objective of this Standard is to provide underlying concepts of risk, the relationship of risk to safety integrity, the determination of tolerable risk and a number of different methods that enable the safety integrity levels for the safety instrumented functions to be determined.

This Standard is Part 3 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
Part 2: Guidelines for the application of AS IEC 61511-1
Part 3: Guidance for the determination of the required safety integrity levels (this standard)

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

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

This International Standard addresses safety instrumented systems which are based on the use of Electrical (E)/Electronic (E)/Programmable Electronic (PE) 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 International Standard is process industry specific within the framework of IEC 61508 (see Annex A of IEC 61511-1).

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 be 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). Any safety strategy should consider 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 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 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 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.

This standard deals with guidance in the area of determining the required SIL in hazards and risk analysis (H & RA). The information herein is intended to provide a broad overview of the wide range of global methods used to implement H & RA. The information provided is not of sufficient detail to implement any of these approaches.

Before proceeding, the concept and determination of safety integrity level(s) (SIL) provided in IEC 61511-1 should be reviewed. The annexes in this standard address the following:

Annex A provides an overview of the concepts of tolerable risk and ALARP.

Annex B provides an overview of a semi-quantitative method used to determine the required SIL.

Annex C provides an overview of a safety matrix method to determine the required SIL.

Annex D provides an overview of a method using a semi-qualitative risk graph approach to determine the required SIL.

Annex E provides an overview of a method using a qualitative risk graph approach to determine the required SIL.

Annex F provides an overview of a method using a layer of protection analysis (LOPA) approach to select the required SIL.

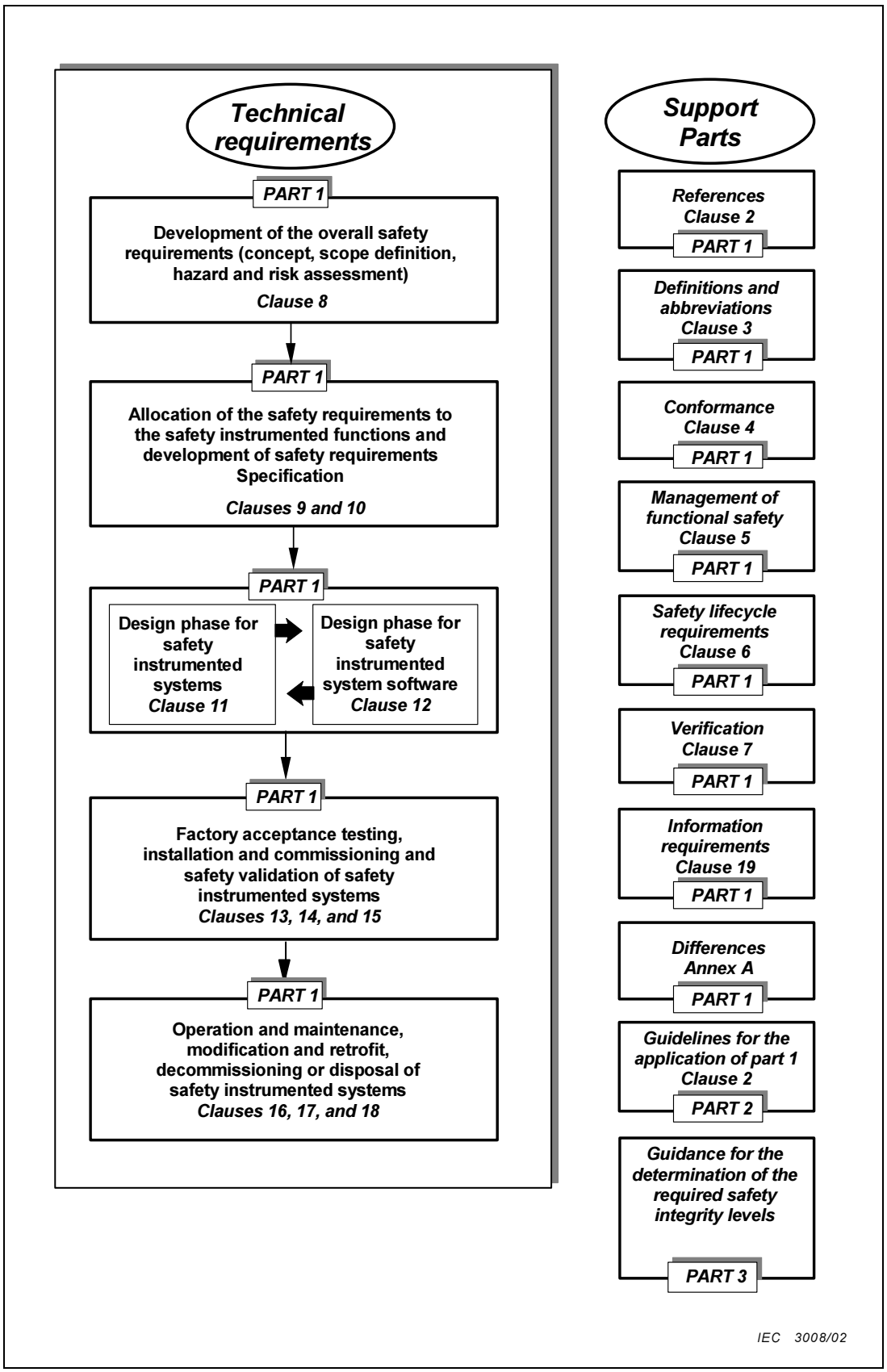

FIGURE 1 – OVERALL FRAMEWORK OF THIS STANDARD

NOTES

STANDARDS AUSTRALIA

Australian Standard

Functional safety—Safety instrumented systems for the process industry sector
Part 3: Guidance for the determination of the required safety integrity levels

1 Scope

1.1 This part provides information on

- the underlying concepts of risk, the relationship of risk to safety integrity, see Clause 3;
- the determination of tolerable risk, see Annex A;
- a number of different methods that enable the safety integrity levels for the safety instrumented functions to be determined, see Annexes B, C, D, E, and F.

In particular, this part

a) applies when functional safety is achieved using one or more safety instrumented functions for the protection of either personnel, the general public, or the environment;

b) may be applied in non-safety applications such as asset protection;

c) illustrates typical hazard and risk assessment methods that may be carried out to define the safety functional requirements and safety integrity levels of each safety instrumented function;

d) illustrates techniques/measures available for determining the required safety integrity levels;

e) provides a framework for establishing safety integrity levels but does not specify the safety integrity levels required for specific applications;

f) does not give examples of determining the requirements for other methods of risk reduction.

1.2 Annexes B, C, D, E, and F 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.

NOTE Those intending to apply the methods indicated in these annexes should consult the source material referenced in each annex.

1.3 Figure 1 shows the overall framework for IEC 61511-1, IEC 61511-2 and IEC 61511-3 and indicates the role that this standard plays in the achievement of functional safety for safety instrumented systems.

Figure 2 gives an overview of risk reduction methods.