

Australian Standard™

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

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

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 Standards may also be withdrawn.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](http://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](mailto: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.

**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 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 |

This is a free preview. Purchase the entire publication at the link below:

[Product Page](#)

- 
- [Looking for additional Standards? Visit Intertek Inform Infostore](#)
  - [Learn about LexConnect, All Jurisdictions, Standards referenced in Australian legislation](#)
-