



Functional Safety—Safety instrumented systems for the process industry sector

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



AS IEC 61511.3:2018

This Australian Standard ® was prepared by IT-006, Industrial Process Measurement, Control and Automation. It was approved on behalf of the Council of Standards Australia on 4 October 2018.

This Standard was published on 2 November 2018.

The following are represented on Committee IT-006:

- Australian Computer Society
- Australian Industry Group
- Australian Petroleum Production and Exploration Association
- Consult Australia
- Institute of Instrumentation, Control and Automation, Australia
- Institution of Chemical Engineers
- ISACA
- Process Control Society, Engineers Australia
- Workplace Health and Safety Queensland

This Standard was issued in draft form for comment as DR AS IEC 61511.3:2018.

Keeping Standards up-to-date

Ensure you have the latest versions of our publications and keep up-to-date about Amendments, Rulings, Withdrawals, and new projects by visiting:

www.standards.org.au

www.saiglobal.com (sales and distribution)

ISBN 978 1 76072 204 3



Functional Safety—Safety instrumented systems for the process industry sector

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

Originated as AS IEC 61511.3—2004.
Second edition 2018.

COPYRIGHT

© IEC 2018 — All rights reserved
© Standards Australia Limited 2018

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, unless otherwise permitted under the Copyright Act 1968 (Cth).

Published by SAI Global Limited under licence from Standards Australia Limited, GPO Box 476, Sydney, NSW 2001, Australia.

Preface

This Standard was prepared by the Standards Australia Committee IT-006, Industrial Process Measurement, Control and Automation, to supersede AS IEC 61511.3—2004.

The objective of this Standard is to provide information on—

- (a) the underlying concepts of risk and the relationship of risk to safety integrity (see Clause A.4);
- (b) the determination of tolerable risk (see Annex K);
- (c) a number of different methods that enable the safety integrity level (SIL) for the safety instrumented functions (SIF) to be determined (see Annexes B through K); and
- (d) the impact of multiple safety systems on calculations determining the ability to achieve the desired risk reduction (see Annex J).

This Standard is identical with, and has been reproduced from, IEC 61511-3:2016, *Functional safety — Safety instrumented systems for the process industry sector — Part 3: Guidance for the determination of the required safety integrity levels*.

As this document has been reproduced from an International Standard, the following applies:

- (i) In the source text “this part of IEC 61511” should read “this Australian Standard”.
- (ii) A full point substitutes for a comma when referring to a decimal marker.

Australian or Australian/New Zealand Standards that are identical adoptions of international normative references may be used interchangeably. Refer to the online catalogue for information on specific Standards.

The term “informative” is used in Standards to define the application of the annexes to which it applies. An “informative” annex is only for information and guidance.

CONTENTS

FOREWORD.....	7
INTRODUCTION.....	9
1 Scope.....	12
2 Normative references	13
3 Terms, definitions and abbreviations	13
Annex A (informative) Risk and safety integrity – general guidance.....	14
A.1 General.....	14
A.2 Necessary risk reduction	14
A.3 Role of safety instrumented systems.....	14
A.4 Risk and safety integrity	16
A.5 Allocation of safety requirements	17
A.6 Hazardous event, hazardous situation and harmful event.....	17
A.7 Safety integrity levels	18
A.8 Selection of the method for determining the required safety integrity level	18
Annex B (informative) Semi-quantitative method – event tree analysis	20
B.1 Overview	20
B.2 Compliance with IEC 61511-1:2016	20
B.3 Example	20
B.3.1 General	20
B.3.2 Process safety target	21
B.3.3 Hazard analysis	21
B.3.4 Semi-quantitative risk analysis technique.....	22
B.3.5 Risk analysis of existing process	23
B.3.6 Events that do not meet the process safety target.....	25
B.3.7 Risk reduction using other protection layers.....	26
B.3.8 Risk reduction using a safety instrumented function	26
Annex C (informative) The safety layer matrix method	28
C.1 Overview	28
C.2 Process safety target	29
C.3 Hazard analysis	29
C.4 Risk analysis technique	30
C.5 Safety layer matrix	31
C.6 General procedure	32
Annex D (informative) A semi-qualitative method: calibrated risk graph	34
D.1 Overview	34
D.2 Risk graph synthesis	34
D.3 Calibration	35
D.4 Membership and organization of the team undertaking the SIL assessment	36
D.5 Documentation of results of SIL determination	37
D.6 Example calibration based on typical criteria.....	37
D.7 Using risk graphs where the consequences are environmental damage	40
D.8 Using risk graphs where the consequences are asset loss	41
D.9 Determining the integrity level of instrument protection function where the consequences of failure involve more than one type of loss.....	41
Annex E (informative) A qualitative method: risk graph	42

E.1	General.....	42
E.2	Typical implementation of instrumented functions	42
E.3	Risk graph synthesis	43
E.4	Risk graph implementation: personnel protection	43
E.5	Relevant issues to be considered during application of risk graphs.....	45
Annex F (informative) Layer of protection analysis (LOPA)		47
F.1	Overview	47
F.2	Impact event	48
F.3	Severity level	48
F.4	Initiating cause.....	49
F.5	Initiation likelihood	50
F.6	Protection layers	50
F.7	Additional mitigation.....	51
F.8	Independent protection layers (IPL).....	51
F.9	Intermediate event likelihood	52
F.10	SIF integrity level	52
F.11	Mitigated event likelihood	52
F.12	Total risk.....	52
F.13	Example	53
F.13.1	General	53
F.13.2	Impact event and severity level	53
F.13.3	Initiating cause	53
F.13.4	Initiating likelihood	53
F.13.5	General process design.....	53
F.13.6	BPCS	53
F.13.7	Alarms	53
F.13.8	Additional mitigation.....	54
F.13.9	Independent protection layer(s) (IPL).....	54
F.13.10	Intermediate event likelihood.....	54
F.13.11	SIS	54
F.13.12	Next SIF	54
Annex G (informative) Layer of protection analysis using a risk matrix		56
G.1	Overview	56
G.2	Procedure.....	58
G.2.1	General	58
G.2.2	Step 1: General Information and node definition	58
G.2.3	Step 2: Describe hazardous event	59
G.2.4	Step 3: Evaluate initiating event frequency	62
G.2.5	Step 4: Determine hazardous event consequence severity and risk reduction factor	63
G.2.6	Step 5: Identify independent protection layers and risk reduction factor	64
G.2.7	Step 6: Identify consequence mitigation systems and risk reduction factor	65
G.2.8	Step 7: Determine CMS risk gap.....	66
G.2.9	Step 8: Determine scenario risk gap	69
G.2.10	Step 9: Make recommendations when needed	69
Annex H (informative) A qualitative approach for risk estimation & safety integrity level (SIL) assignment		71
H.1	Overview	71

H.2	Risk estimation and SIL assignment	73
H.2.1	General	73
H.2.2	Hazard identification/indication	73
H.2.3	Risk estimation	73
H.2.4	Consequence parameter selection (C) (Table H.2)	74
H.2.5	Probability of occurrence of that harm	75
H.2.6	Estimating probability of harm	77
H.2.7	SIL assignment	77
Annex I (informative)	Designing & calibrating a risk graph	80
I.1	Overview	80
I.2	Steps involved in risk graph design and calibration	80
I.3	Risk graph development	80
I.4	The risk graph parameters	81
I.4.1	Choosing parameters	81
I.4.2	Number of parameters	81
I.4.3	Parameter value	81
I.4.4	Parameter definition	81
I.4.5	Risk graph	82
I.4.6	Tolerable event frequencies (Tef) for each consequence	82
I.4.7	Calibration	83
I.4.8	Completion of the risk graph	84
Annex J (informative)	Multiple safety systems	85
J.1	Overview	85
J.2	Notion of systemic dependencies	85
J.3	Semi-quantitative approaches	88
J.4	Boolean approaches	89
J.5	State-transition approach	92
Annex K (informative)	As low as reasonably practicable (ALARP) and tolerable risk concepts	96
K.1	General	96
K.2	ALARP model	96
K.2.1	Overview	96
K.2.2	Tolerable risk target	97
Bibliography	99
Figure 1	– Overall framework of the IEC 61511 series	11
Figure 2	– Typical protection layers and risk reduction means	13
Figure A.1	– Risk reduction: general concepts	16
Figure A.2	– Risk and safety integrity concepts	17
Figure A.3	– Harmful event progression	18
Figure A.4	– Allocation of safety requirements to the non-SIS protection layers and other protection layers	19
Figure B.1	– Pressurized vessel with existing safety systems	21
Figure B.2	– Fault tree for overpressure of the vessel	24
Figure B.3	– Hazardous events with existing safety systems	25
Figure B.4	– Hazardous events with SIL 2 safety instrumented function	27
Figure C.1	– Protection layers	28

Figure C.2 – Example of safety layer matrix.....	32
Figure D.1 – Risk graph: general scheme	38
Figure D.2 – Risk graph: environmental loss.....	41
Figure E.1 – VDI/VDE 2180 Risk graph – personnel protection and relationship to SILs.....	44
Figure F.1 – Layer of protection analysis (LOPA) report.....	49
Figure G.1 – Layer of protection graphic highlighting proactive and reactive IPL.....	56
Figure G.2 – Work process used for Annex G	58
Figure G.3 – Example process node boundary for selected scenario	59
Figure G.4 – Acceptable secondary consequence risk	67
Figure G.5 – Unacceptable secondary consequence risk	67
Figure G.6 – Managed secondary consequence risk	69
Figure H.1 – Workflow of SIL assignment process	72
Figure H.2 – Parameters used in risk estimation.....	74
Figure I.1 – Risk graph parameters to consider.....	81
Figure I.2 – Illustration of a risk graph with parameters from Figure I.1.....	82
Figure J.1 – Conventional calculations	85
Figure J.2 – Accurate calculations.....	86
Figure J.3 – Redundant SIS	88
Figure J.4 – Corrective coefficients for hazardous event frequency calculations when the proof tests are performed at the same time.....	89
Figure J.5 – Expansion of the simple example	89
Figure J.6 – Fault tree modelling of the multi SIS presented in Figure J.5.....	90
Figure J.7 – Modelling CCF between SIS ₁ and SIS ₂	91
Figure J.8 – Effect of tests staggering	91
Figure J.9 – Effect of partial stroking	92
Figure J.10 – Modelling of repair resource mobilisation.....	93
Figure J.11 – Example of output from Monte Carlo simulation	94
Figure J.12 – Impact of repairs due to shared repair resources	95
Figure K.1 – Tolerable risk and ALARP	97
Table B.1 – HAZOP study results	22
Table C.1 – Frequency of hazardous event likelihood (without considering PLs).....	31
Table C.2 – Criteria for rating the severity of impact of hazardous events.....	31
Table D.1 – Descriptions of process industry risk graph parameters.....	35
Table D.2 – Example calibration of the general purpose risk graph	39
Table D.3 – General environmental consequences	40
Table E.1 – Data relating to risk graph (see Figure E.1).....	45
Table F.1 – HAZOP developed data for LOPA	48
Table F.2 – Impact event severity levels.....	49
Table F.3 – Initiation likelihood.....	50
Table F.4 – Typical protection layers (prevention and mitigation) PFD _{avg}	51
Table G.1 – Selected scenario from HAZOP worksheet.....	59
Table G.2 – Selected scenario from LOPA worksheet	61

Table G.3 – Example initiating causes and associated frequency	63
Table G.4 – Consequence severity decision table	64
Table G.5 – Risk reduction factor matrix.....	64
Table G.6 – Examples of independent protection layers (IPL) with associated risk reduction factors (RRF) and probability of failure on demand (PFD)	66
Table G.7 – Examples of consequence mitigation system (CMS) with associated risk reduction factors (RRF) and probability of failure on demand (PFD)	66
Table G.8 – Step 7 LOPA worksheet (1 of 2)	68
Table G.9 – Step 8 LOPA worksheet (1 of 2)	70
Table H.1 – List of SIFs and hazardous events to be assessed	73
Table H.2 – Consequence parameter/severity level	74
Table H.3 – Occupancy parameter/Exposure probability (F).....	75
Table H.4 – Avoidance parameter/avoidance probability	76
Table H.5 – Demand rate parameter (W)	77
Table H.6 – Risk graph matrix (SIL assignment form for safety instrumented functions).....	78
Table H.7 – Example of consequence categories	78
Table K.1 – Example of risk classification of incidents	98
Table K.2 – Interpretation of risk classes	98

INTERNATIONAL ELECTROTECHNICAL COMMISSION

**FUNCTIONAL SAFETY –
SAFETY INSTRUMENTED SYSTEMS
FOR THE PROCESS INDUSTRY SECTOR –****Part 3: Guidance for the determination
of the required safety integrity levels**

FOREWORD

- 1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
- 2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
- 3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
- 4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
- 5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
- 6) All users should ensure that they have the latest edition of this publication.
- 7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
- 8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
- 9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

International Standard IEC 61511-3: has been prepared by subcommittee 65A: System aspects, of IEC technical committee 65: Industrial-process measurement, control and automation.

This second edition cancels and replaces the first edition published in 2003. This edition constitutes a technical revision. This edition includes the following significant technical changes with respect to the previous edition:

Additional H&RA example(s) and quantitative analysis consideration annexes are provided.

The text of this document is based on the following documents:

FDIS	Report on voting
65A/779/FDIS	65A786/RVD

Full information on the voting for the approval of this standard can be found in the report on voting indicated in the above table.

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.

A list of all parts in the IEC 61511 series, published under the general title *Functional safety – Safety instrumented systems for the process industry sector*, can be found on the IEC website.

The committee has decided that the contents of this publication will remain unchanged until the stability date indicated on the IEC website under "<http://webstore.iec.ch>" in the data related to the specific publication. At this date, the publication will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

INTRODUCTION

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

The IEC 61511 series addresses the application of SIS for the process industries. A process hazard and risk assessment is carried out to enable the specification for SIS 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 SIS. The SIS includes all devices and subsystems necessary to carry out the SIF from sensor(s) to final element(s).

The IEC 61511 series has two concepts which are fundamental to its application; SIS safety life-cycle and safety integrity levels (SIL).

The IEC 61511 series addresses SIS 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 the IEC 61511 series should be applied. The IEC 61511 series also addresses the SIS sensors and final elements regardless of the technology used. The IEC 61511 series is process industry specific within the framework of IEC 61508:2010.

The IEC 61511 series sets out an approach for SIS 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, and programmable electronic). Any safety strategy should consider each individual SIS in the context of the other protective systems. To facilitate this approach, the IEC 61511 series covers:

- a hazard and risk assessment is carried out to identify the overall safety requirements;
- an allocation of the safety requirements to the SIS is carried out;
- works within a framework which is applicable to all instrumented means 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;
- addressing all SIS safety life-cycle phases from initial concept, design, implementation, operation and maintenance through to decommissioning;
- enabling existing or new country specific process industry standards to be harmonized with the IEC 61511 series.

The IEC 61511 series 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 regulations, these take precedence over the requirements defined in the IEC 61511-1.

The IEC 61511-3 deals with guidance in the area of determining the required SIL in hazards and risk assessment. The information herein is intended to provide a broad overview of the wide range of global methods used to implement hazards and risk assessment. The information provided is not of sufficient detail to implement any of these approaches.

Before proceeding, the concept and determination of SIL provided in IEC 61511-1:2016 should be reviewed. The informative annexes in the IEC 61511-3 address the following:

- Annex A provides information that is common to each of the hazard and risk assessment methods shown herein.
- 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.
- Annex G provides a layer of protection analysis using a risk matrix.
- Annex H provides an overview of a qualitative approach for risk estimation & SIL assignment.
- Annex I provides an overview of the basic steps involved in designing and calibrating a risk graph.
- Annex J provides an overview of the impact of multiple safety systems on determining the required SIL.
- Annex K provides an overview of the concepts of tolerable risk and ALARP.

Figure 1 shows the overall framework for IEC 61511-1, IEC 61511-2 and IEC 61511-3 and indicates the role that the IEC 61511 series plays in the achievement of functional safety for SIS.

FUNCTIONAL SAFETY – SAFETY INSTRUMENTED SYSTEMS FOR THE PROCESS INDUSTRY SECTOR –

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

1 Scope

This part of IEC 61511 provides information on:

- the underlying concepts of risk and the relationship of risk to safety integrity (see Clause A.4);
- the determination of tolerable risk (see Annex K);
- a number of different methods that enable the safety integrity level (SIL) for the safety instrumented functions (SIF) to be determined (see Annexes B through K);
- the impact of multiple safety systems on calculations determining the ability to achieve the desired risk reduction (see Annex J).

In particular, this part of IEC 61511:

- a) applies when functional safety is achieved using one or more SIF 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 SIL of each SIF;
- d) illustrates techniques/measures available for determining the required SIL;
- e) provides a framework for establishing SIL but does not specify the SIL required for specific applications;
- f) does not give examples of determining the requirements for other methods of risk reduction.

NOTE Examples given in the Annexes of this Standard are intended only as case specific examples of implementing IEC 61511 requirements in a specific instance, and the user should satisfy themselves that the chosen methods and techniques are appropriate to their situation.

Annexes B through K 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 1 Those intending to apply the methods indicated in these annexes can consult the source material referenced in each annex.

NOTE 2 The methods of SIL determination included in Part 3 may not be suitable for all applications. In particular, specific techniques or additional factors that are not illustrated may be required for high demand or continuous mode of operation.

NOTE 3 The methods as illustrated herein may result in non-conservative results when they are used beyond their underlying limits and when factors such as common cause, fault tolerance, holistic considerations of the application, lack of experience with the method being used, independence of the protection layers, etc., are not properly considered. See Annex J.

Figure 2 gives an overview of typical protection layers and risk reduction means.