



Functional safety—Safety instrumented systems for the process industry

Part 2: Guidelines for the application of AS IEC 61511.1

AS IEC 61511.2:2018

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 26 September 2018.

This Standard was published on 6 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 & Automation Aust
- Institution of Chemical Engineers
- ISACA
- Process Control Society
- Workplace Health and Safety Queensland

This Standard was issued in draft form for comment as DR AS IEC 61511.2:2018.

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 203 6



Functional safety—Safety instrumented systems for the process industry

Part 2: Guidelines for the application of AS IEC 61511.1

Originated as AS IEC 61511.2—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 61511.2—2004.

The objective of this Standard is to provide guidance on the specification, design, installation, operation and maintenance of safety instrumented functions (SIFs) and related safety instrumented systems (SISs) as defined in AS IEC 61511.1.

NOTE 1 Annex A (informative) has been organized so that each clause and subclause number therein addresses the corresponding clause and subclause number in AS IEC 61511.1 except for being preceded by “A”.

NOTE 2 Annex A now contains material previously in the body of the first edition. These changes are required for conformance with IEC rules which prohibit a standard being wholly informative.

NOTE 3 To achieve maximum use of this Standard—

(a) review the section guidance as well as the specific clause guidance (e.g. when looking for guidance on Clause 5.2.6.1.3, consider guidance in Clause 5.2.6); and

(b) when specific clause guidance is not provided (e.g. no further guidance provided), consider reviewing the section guidance as well, as it can be applicable).

NOTE 4 Examples given in the annexes of this Standard are intended only as case specific examples of implementing AS IEC 61511 requirements in a specific instance, and the user should satisfy themselves that the chosen methods and techniques are appropriate to their situation.

This Standard is identical with, and has been reproduced from, IEC 61511-2:2016, *Functional safety — Safety instrumented systems for the process industry sector — Part 2: Guidelines for the application of IEC 61511-1:2016*.

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.....9

INTRODUCTION..... 11

1 Scope..... 13

2 Normative references 13

3 Terms, definitions, and abbreviations 13

Annex A (informative) Guidance for IEC 61511-1 14

 A.1 Scope 14

 A.2 Normative references 14

 A.3 Terms, definitions and abbreviations..... 14

 A.4 Conformance to the IEC 61511-1:–..... 14

 A.5 Management of functional safety 14

 A.5.1 Objective 14

 A.5.2 Guidance to "Requirements" 14

 A.6 Safety life-cycle requirements..... 23

 A.6.1 Objectives..... 23

 A.6.2 Guidance to "Requirements"..... 23

 A.6.3 Guidance to "Application program SIS safety life-cycle requirements" 24

 A.7 Verification..... 25

 A.7.1 Objective 25

 A.7.2 Guidance to "Requirements"..... 25

 A.8 Process hazard and risk assessment (H&RA) 27

 A.8.1 Objectives..... 27

 A.8.2 Guidance to "Requirements"..... 27

 A.9 Allocation of safety functions to protection layers 30

 A.9.1 Objective 30

 A.9.2 Guidance to "Requirements of the allocation process"..... 30

 A.9.3 Guidance to "Requirements on the basic process control system as a protection layer"..... 32

 A.9.4 Guidance to "Requirements for preventing common cause, common mode and dependent failures" 35

 A.10 SIS safety requirements specification 36

 A.10.1 Objective 36

 A.10.2 Guidance to "General requirements"..... 36

 A.10.3 Guidance to "SIS safety requirements" 36

 A.11 SIS design and engineering..... 40

 A.11.1 Objective 40

 A.11.2 Guidance to "General requirements"..... 40

 A.11.3 Guidance to "Requirements for system behaviour on detection of a fault"..... 47

 A.11.4 Guidance to "Hardware fault tolerance" 47

 A.11.5 Guidance to "Requirements for selection of devices"..... 50

 A.11.6 Field devices 53

 A.11.7 Interfaces 53

 A.11.8 Guidance to "Maintenance or testing design requirements" 55

 A.11.9 Guidance to "Quantification of random failure" 56

 A.12 SIS application program development..... 62

A.12.1	Objective	62
A.12.2	Guidance to "General requirements".....	62
A.12.3	Guidance to "Application program design"	64
A.12.4	Guidance to "Application program implementation"	66
A.12.5	Guidance to "Requirements for application program verification (review and testing)"	67
A.12.6	Guidance to "Requirements for application program methodology and tools"	70
A.13	Factory acceptance testing (FAT)	73
A.13.1	Objectives.....	73
A.13.2	Guidance to "Recommendations".....	73
A.14	SIS installation and commissioning.....	73
A.14.1	Objectives.....	73
A.14.2	Guidance to "Requirements".....	73
A.15	SIS safety validation	74
A.15.1	Objective	74
A.15.2	Guidance to "Requirements".....	74
A.16	SIS operation and maintenance	74
A.16.1	Objectives.....	74
A.16.2	Guidance to "Requirements".....	75
A.16.3	Proof testing and inspection	76
A.17	SIS modification	78
A.17.1	Objective	78
A.17.2	Guidance to "Requirements".....	79
A.18	SIS decommissioning	79
A.18.1	Objectives.....	79
A.18.2	Guidance to "Requirements".....	79
A.19	Information and documentation requirements.....	80
A.19.1	Objectives.....	80
A.19.2	Guidance to "Requirements".....	80
Annex B (informative)	Example of SIS logic solver application program development using function block diagram	81
B.1	General.....	81
B.2	Application program development and validation philosophy	81
B.3	Application description	82
B.3.1	General	82
B.3.2	Process description.....	82
B.3.3	Safety instrumented functions	83
B.3.4	Risk reduction and domino effects	84
B.4	Application program safety life-cycle execution	84
B.4.1	General	84
B.4.2	Inputs to application program SRS development	84
B.4.3	Application program design and development	87
B.4.4	Application program production	101
B.4.5	Application program verification and testing.....	101
B.4.6	Validation	101
Annex C (informative)	Considerations when converting from NP technologies to PE technologies	102

Annex D (informative) Example of how to get from a piping and instrumentation diagram (P&ID) to application program	104
Annex E (informative) Methods and tools for application programming	107
E.1 Typical toolset for application programming	107
E.2 Rules and constraints for application program design	108
E.3 Rules and constraints for application programming	108
Annex F (informative) Example SIS project illustrating each phase of the safety life cycle with application program development using relay ladder language	110
F.1 Overview	110
F.2 Project definition	110
F.2.1 General	110
F.2.2 Conceptual planning	111
F.2.3 Process hazards analysis	111
F.3 Simplified process description	111
F.4 Preliminary design	113
F.5 IEC 61511 application	113
F.5.1 General	113
F.5.2 Step F.1: Hazard & risk assessment	117
F.5.3 Hazard identification	117
F.5.4 Preliminary hazard evaluation	117
F.5.5 Accident history	117
F.6 Preliminary process design safety considerations	120
F.7 Recognized process hazards	120
F.8 Process design definitions strategy	121
F.9 Preliminary hazard assessment	124
F.9.1 General	124
F.9.2 Step F.2: Allocation of safety functions	128
F.10 SIF safety integrity level determination	129
F.11 Layer of protection analysis (LOPA) applied to example	129
F.12 Tolerable risk criteria	130
F.13 Step F.3: SIS safety requirements specifications	133
F.13.1 Overview	133
F.13.2 Input requirements	133
F.13.3 Safety functional requirements	134
F.13.4 Safety integrity requirements	135
F.14 Functional description and conceptual design	136
F.14.1 Narrative for example reactor system logic	136
F.15 SIL verification calculations	137
F.16 Application program requirements	144
F.17 Step F.4: SIS safety life-cycle	151
F.18 Technology and device selection	151
F.18.1 General	151
F.18.2 Logic solver	151
F.18.3 Sensors	152
F.18.4 Final elements	152
F.18.5 Solenoid valves	152
F.18.6 Emergency vent valves	153
F.18.7 Modulating valves	153
F.18.8 Bypass valves	153

F.18.9	Human-machine interfaces (HMIs).....	153
F.18.10	Separation.....	154
F.19	Common cause and systematic failures.....	155
F.19.1	General.....	155
F.19.2	Diversity.....	155
F.19.3	Specification errors.....	155
F.19.4	Hardware design errors.....	155
F.19.5	Software design errors.....	156
F.19.6	Environmental overstress.....	156
F.19.7	Temperature.....	156
F.19.8	Humidity.....	156
F.19.9	Contaminants.....	157
F.19.10	Vibration.....	157
F.19.11	Grounding.....	157
F.19.12	Power line conditioning.....	157
F.19.13	Electro-magnetic compatibility (EMC).....	157
F.19.14	Utility sources.....	158
F.19.15	Sensors.....	159
F.19.16	Process corrosion or fouling.....	159
F.19.17	Maintenance.....	159
F.19.18	Susceptibility to mis-operation.....	159
F.19.19	SIS architecture.....	159
F.20	SIS application program design features.....	160
F.21	Wiring practices.....	161
F.22	Security.....	161
F.23	Step F.5: SIS installation, commissioning, validation.....	162
F.24	Installation.....	162
F.25	Commissioning.....	163
F.26	Documentation.....	164
F.27	Validation.....	164
F.28	Testing.....	165
F.29	Step F.6: SIS operation and maintenance.....	178
F.30	Step F.7: SIS Modification.....	181
F.31	Step F.8: SIS decommissioning.....	181
F.32	Step F.9: SIS verification.....	181
F.33	Step F.10: Management of functional safety and SIS FSA.....	182
F.34	Management of functional safety.....	183
F.34.1	General.....	183
F.34.2	Competence of personnel.....	183
F.35	Functional safety assessment.....	183
Annex G (informative)	Guidance on developing application programming practices.....	184
G.1	Purpose of this guidance.....	184
G.2	Generic safe application programming attributes.....	184
G.3	Reliability.....	184
G.3.1	General.....	184
G.3.2	Predictability of memory utilisation.....	185
G.3.3	Predictability of control flow.....	186
G.3.4	Accounting for precision and accuracy.....	188
G.3.5	Predictability of timing.....	190

G.4	Predictability of mathematical or logical result.....	190
G.5	Robustness.....	191
G.5.1	General	191
G.5.2	Controlling use of diversity	191
G.5.3	Controlling use of exception handling	192
G.5.4	Checking input and output.....	193
G.6	Traceability	194
G.6.1	General	194
G.6.2	Controlling use of built-in functions.....	194
G.6.3	Controlling use of compiled libraries	194
G.7	Maintainability.....	194
G.7.1	General	194
G.7.2	Readability.....	195
G.7.3	Data abstraction.....	198
G.7.4	Functional cohesiveness	199
G.7.5	Malleability	199
G.7.6	Portability	199
	Bibliography	201
	Figure 1 – Overall framework of IEC 61511 series	12
	Figure A.1 – Application program V-Model.....	25
	Figure A.2 – Independence of a BPCS protection layer and an initiating source in the BPCS	34
	Figure A.3 – Independence of two protection layers allocated to the BPCS	35
	Figure A.4 – Relationship of system, SIS hardware, and SIS application program.....	39
	Figure A.5 – Illustration of uncertainties on a reliability parameter.....	60
	Figure A.6 – Illustration of the 70 % confidence upper bound	61
	Figure A.7 – Typical probabilistic distribution of target results from Monte Carlo simulation.....	62
	Figure B.1 – Process flow diagram for SIF 02.01	83
	Figure B.2 – Process flow diagram for SIF 06.02	84
	Figure B.3 – Functional specification of SIF02.01 and SIF 06.02.....	85
	Figure B.4 – SIF 02.01 hardware functional architecture	85
	Figure B.5 – SIF 06.02 hardware functional architecture	86
	Figure B.6 – Hardware specification for SOV extracted from piping and instrumentation diagram.....	86
	Figure B.7 – SIF 02.01 hardware physical architecture	87
	Figure B.8 – SIF 06.02 hardware physical architecture	87
	Figure B.9 – Hierarchical structure of model integration	91
	Figure B.10 – Hierarchical structure of model integration including models of safety properties and of BPCS logic	93
	Figure B.11 – State transition diagram	94
	Figure B.12 – SOV typical block diagram.....	95
	Figure B.13 – SOV typical model block diagram	96
	Figure B.14 – Typical model block diagram implementation – BPCS part.....	98
	Figure B.15 – SOV application program typical model implementation – SIS part	99

Figure B.16 – Complete model for final implementation model checking	101
Figure D.1 – Example of P&ID for an oil and gas separator	104
Figure D.2 – Example of (part of) an ESD cause & effect diagram (C&E).....	105
Figure D.3 – Example of (part of) an application program in a safety PLC function block programming	106
Figure F.1 – Simplified flow diagram: the PVC process	112
Figure F.2 – SIS safety life-cycle phases and FSA stages.....	114
Figure F.3 – Example of the preliminary P&ID for PVC reactor unit	123
Figure F.4 – SIF S-1 Bubble diagram showing the $PF_{D_{avg}}$ of each SIS device.....	139
Figure F.5 – S-1 Fault tree	140
Figure F.6 – SIF S-2 Bubble diagram showing the $PF_{D_{avg}}$ of each SIS device.....	141
Figure F.7 – SIF S-2 fault tree.....	142
Figure F.8 – SIF S-3 Bubble diagram showing the $PF_{D_{avg}}$ of each SIS device.....	143
Figure F.9 – SIF S-3 fault tree.....	144
Figure F.10 – P&ID for PVC reactor unit SIF.....	145
Figure F.11 – Legend (1 of 5).....	146
Figure F.12 – SIS for the VCM reactor.....	160
Table B.1 – Modes of operation specification.....	88
Table B.2 – State transition table	93
Table F.1 – SIS safety life-cycle overview	115
Table F.2 – SIS safety life-cycle – Box 1	117
Table F.3 – Some physical properties of vinyl chloride.....	119
Table F.4 – What-If/Checklist	125
Table F.5 – HAZOP	126
Table F.6 – Partial summary of hazard assessment for SIF strategy development	127
Table F.7 – SIS safety life-cycle – Box 2	129
Table F.8 – Tolerable risk ranking	131
Table F.9 – VCM reactor example: LOPA based integrity level.....	132
Table F.10 – SIS safety life-cycle – Box 3	133
Table F.11 – Safety instrumented functions and SILs.....	133
Table F.12 – Functional relationship of I/O for the SIF(s)	134
Table F.13 – SIS sensors, normal operating range & trip points	134
Table F.14 – Cause and effect diagram	137
Table F.15 – MTTFD figures of SIS F.1 devices	138
Table F.16 – SIS safety life-cycle – Box 4	151
Table F.17 – SIS safety life-cycle – Box 5	162
Table F.18 – List of instrument types and testing procedures used.....	166
Table F.19 – Interlock check procedure bypass/simulation check sheet.....	178
Table F.20 – SIS safety life-cycle – Box 6	178
Table F.21 – SIS trip log	179
Table F.22 – SIS device failure log.....	179
Table F.23 – SIS safety life-cycle – Box 7	181

Table F.24 – SIS safety life-cycle – Box 8	181
Table F.25 – SIS safety life-cycle – Box 9	182
Table F.26 – SIS safety life-cycle – Box 10.....	182