



**Standards**

- Certification
- Education & Training
- Publishing
- Conferences & Exhibits

*Setting the Standard for Automation™*

AMERICAN NATIONAL STANDARD

**ANSI/ISA-61511-2-2018 / 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  
(IEC 61511-2:2016, IDT)**

**Approved 11 July 2018**

**NOTICE OF COPYRIGHT**

This is a copyright document and may not be copied or distributed in any form or manner without the permission of ISA. This copy of the document was made for the sole use of the person to whom ISA provided it and is subject to the restrictions stated in ISA's license to that person. It may not be provided to any other person in print, electronic, or any other form. Violations of ISA's copyright will be prosecuted to the fullest extent of the law and may result in substantial civil and criminal penalties.

ANSI/ISA-61511-2-2018 / 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 (IEC 61511-2:2016, IDT)

ISBN: 978-1-945541-96-4

Copyright © 2016 IEC. Copyright © 2018 ISA. These materials are subject to copyright claims of IEC and ISA. No part of this publication may be reproduced in any form, including an electronic retrieval system, without the prior written permission of ISA. All requests pertaining to the ANSI/ISA-61511-2-2018 / IEC 61511-2:2016 Standard should be submitted to ISA.

ISA  
67 T.W. Alexander Drive  
P.O. Box 12277  
Research Triangle Park, North Carolina 27709  
E-mail: [standards@isa.org](mailto:standards@isa.org)

## Preface

This preface is included for information purposes only and is not part of ANSI/ISA-61511-2-2018 / IEC 61511-2:2016.

This standard has been prepared as part of the service of ISA, the International Society of Automation, toward a goal of uniformity in the field of automation. To be of real value, this document should not be static but should be subject to periodic review. Toward this end, the Society welcomes all comments and criticisms and asks that they be addressed to the Secretary, Standards and Practices Board; ISA, 67 T.W. Alexander Drive; P.O. Box 12277; Research Triangle Park, NC 277099; Telephone (919) 549-8411; Fax (919) 549-8288; E-mail: [standards@isa.org](mailto:standards@isa.org).

The ISA Standards and Practices Department is aware of the growing need for attention to the metric system of units in general, and the International System of Units (SI) in particular, in the preparation of instrumentation standards, recommended practices, and technical reports. The Department is further aware of the benefits of USA users of ISA standards of incorporating suitable references to the SI (and the metric system) in their business and professional dealings with other countries. Toward this end, the Department will endeavor to introduce SI and acceptable metric units in all new and revised standards to the greatest extent possible. The Metric Practice Guide, which has been published by the Institute of Electrical and Electronics Engineers (IEEE) as ANSI/IEEE Std. 268-1992, and future revisions, will be the reference guide for definitions, symbols, abbreviations, and conversion factors.

It is the policy of ISA to encourage and welcome the participation of all interested individuals in the development of ISA standards. Participation in the ISA standards-making process by an individual in no way constitutes endorsement by the employer of that individual, of ISA, or of any of the standards, recommended practices, and technical reports that ISA develops.

**CAUTION — ISA ADHERES TO THE POLICY OF THE AMERICAN NATIONAL STANDARDS INSTITUTE WITH REGARD TO PATENTS. IF ISA IS INFORMED OF AN EXISTING PATENT THAT IS REQUIRED FOR USE OF THE DOCUMENT, IT WILL REQUIRE THE OWNER OF THE PATENT TO EITHER GRANT A ROYALTY-FREE LICENSE FOR USE OF THE PATENT BY USERS COMPLYING WITH THE DOCUMENT OR A LICENSE ON REASONABLE TERMS AND CONDITIONS THAT ARE FREE FROM UNFAIR DISCRIMINATION.**

**EVEN IF ISA IS UNAWARE OF ANY PATENT COVERING THIS DOCUMENT, THE USER IS CAUTIONED THAT IMPLEMENTATION OF THE DOCUMENT MAY REQUIRE USE OF TECHNIQUES, PROCESSES, OR MATERIALS COVERED BY PATENT RIGHTS. ISA TAKES NO POSITION ON THE EXISTENCE OR VALIDITY OF ANY PATENT RIGHTS THAT MAY BE INVOLVED IN IMPLEMENTING THE DOCUMENT. ISA IS NOT RESPONSIBLE FOR IDENTIFYING ALL PATENTS THAT MAY REQUIRE A LICENSE BEFORE IMPLEMENTATION OF THE DOCUMENT OR FOR INVESTIGATING THE VALIDITY OR SCOPE OF ANY PATENTS BROUGHT TO ITS ATTENTION. THE USER SHOULD CAREFULLY INVESTIGATE RELEVANT PATENTS BEFORE USING THE DOCUMENT FOR THE USER'S INTENDED APPLICATION.**

**HOWEVER, ISA ASKS THAT ANYONE REVIEWING THIS DOCUMENT WHO IS AWARE OF ANY PATENTS THAT MAY IMPACT IMPLEMENTATION OF THE DOCUMENT NOTIFY THE ISA STANDARDS AND PRACTICES DEPARTMENT OF THE PATENT AND ITS OWNER. ADDITIONALLY, THE USE OF THIS DOCUMENT MAY INVOLVE HAZARDOUS MATERIALS, OPERATIONS OR EQUIPMENT. THE DOCUMENT CANNOT ANTICIPATE ALL POSSIBLE APPLICATIONS OR ADDRESS ALL POSSIBLE SAFETY ISSUES ASSOCIATED WITH USE IN HAZARDOUS CONDITIONS. THE USER OF THIS DOCUMENT MUST EXERCISE SOUND PROFESSIONAL JUDGMENT CONCERNING ITS USE AND APPLICABILITY UNDER THE USER'S PARTICULAR CIRCUMSTANCES. THE USER MUST ALSO CONSIDER THE**

**APPLICABILITY OF ANY GOVERNMENTAL REGULATORY LIMITATIONS AND ESTABLISHED SAFETY AND HEALTH PRACTICES BEFORE IMPLEMENTING THIS DOCUMENT.**

**THE USER OF THIS DOCUMENT SHOULD BE AWARE THAT THIS DOCUMENT MAY BE IMPACTED BY ELECTRONIC SECURITY ISSUES. THE COMMITTEE HAS NOT YET ADDRESSED THE POTENTIAL ISSUES IN THIS VERSION.**

ISA ([www.isa.org](http://www.isa.org)) is a nonprofit professional association that sets the standard for those who apply engineering and technology to improve the management, safety, and cybersecurity of modern automation and control systems used across industry and critical infrastructure. Founded in 1945, ISA develops widely used global standards; certifies industry professionals; provides education and training; publishes books and technical articles; hosts conferences and exhibits; and provides networking and career development programs for its 40,000 members and 400,000 customers around the world.

ISA owns [Automation.com](http://Automation.com), a leading online publisher of automation-related content, and is the founding sponsor of The Automation Federation ([www.automationfederation.org](http://www.automationfederation.org)), an association of non-profit organizations serving as "The Voice of Automation." Through a wholly owned subsidiary, ISA bridges the gap between standards and their implementation with the ISA Security Compliance Institute ([www.isasecure.org](http://www.isasecure.org)) and the ISA Wireless Compliance Institute ([www.isa100wci.org](http://www.isa100wci.org)).

## CONTENTS

CONTENTS .....	5
US NATIONAL FOREWORD FOR ISA-61511-2 .....	13
FOREWORD .....	15
INTRODUCTION .....	17
1 Scope .....	19
2 Normative references .....	19
3 Terms, definitions, and abbreviations .....	19
Annex A (informative) Guidance for IEC 61511-1 .....	21
A.1 Scope .....	21
A.2 Normative references .....	21
A.3 Terms, definitions and abbreviations .....	21
A.4 Conformance to the IEC 61511-1:– .....	21
A.5 Management of functional safety .....	21
A.5.1 Objective .....	21
A.5.2 Guidance to "Requirements" .....	22
A.6 Safety life-cycle requirements .....	30
A.6.1 Objectives .....	30
A.6.2 Guidance to "Requirements" .....	31
A.6.3 Guidance to "Application program SIS safety life-cycle requirements" .....	31
A.7 Verification .....	33
A.7.1 Objective .....	33
A.7.2 Guidance to "Requirements" .....	34
A.8 Process hazard and risk assessment (H&RA) .....	35
A.8.1 Objectives .....	35
A.8.2 Guidance to "Requirements" .....	35
A.9 Allocation of safety functions to protection layers .....	38
A.9.1 Objective .....	38
A.9.2 Guidance to "Requirements of the allocation process" .....	38
A.9.3 Guidance to "Requirements on the basic process control system as a protection layer" .....	41
A.9.4 Guidance to "Requirements for preventing common cause, common mode and dependent failures" .....	43
A.10 SIS safety requirements specification .....	44
A.10.1 Objective .....	44
A.10.2 Guidance to "General requirements" .....	44
A.10.3 Guidance to "SIS safety requirements" .....	45
A.11 SIS design and engineering .....	49
A.11.1 Objective .....	49
A.11.2 Guidance to "General requirements" .....	49
A.11.3 Guidance to "Requirements for system behaviour on detection of a fault" .....	56
A.11.4 Guidance to "Hardware fault tolerance" .....	56

A.11.5	Guidance to "Requirements for selection of devices" .....	60
A.11.6	Field devices .....	62
A.11.7	Interfaces .....	63
A.11.8	Guidance to "Maintenance or testing design requirements" .....	65
A.11.9	Guidance to "Quantification of random failure" .....	66
A.12	SIS application program development.....	73
A.12.1	Objective.....	73
A.12.2	Guidance to "General requirements" .....	73
A.12.3	Guidance to "Application program design" .....	74
A.12.4	Guidance to "Application program implementation" .....	77
A.12.5	Guidance to "Requirements for application program verification (review and testing)" .....	78
A.12.6	Guidance to "Requirements for application program methodology and tools".....	82
A.13	Factory acceptance testing (FAT) .....	84
A.13.1	Objectives .....	84
A.13.2	Guidance to "Recommendations" .....	84
A.14	SIS installation and commissioning.....	85
A.14.1	Objectives .....	85
A.14.2	Guidance to "Requirements" .....	85
A.15	SIS safety validation .....	85
A.15.1	Objective.....	85
A.15.2	Guidance to "Requirements".....	85
A.16	SIS operation and maintenance .....	86
A.16.1	Objectives .....	86
A.16.2	Guidance to "Requirements".....	86
A.16.3	Proof testing and inspection .....	88
A.17	SIS modification .....	90
A.17.1	Objective.....	90
A.17.2	Guidance to "Requirements".....	90
A.18	SIS decommissioning .....	91
A.18.1	Objectives .....	91
A.18.2	Guidance to "Requirements".....	91
A.19	Information and documentation requirements .....	91
A.19.1	Objectives .....	91
A.19.2	Guidance to "Requirements".....	92
Annex B (informative)	Example of SIS logic solver application program development using function block diagram .....	93
B.1	General .....	93
B.2	Application program development and validation philosophy.....	93
B.3	Application description .....	95
B.3.1	General.....	95
B.3.2	Process description.....	95
B.3.3	Safety instrumented functions .....	95
B.3.4	Risk reduction and domino effects.....	97

B.4	Application program safety life-cycle execution.....	97
B.4.1	General.....	97
B.4.2	Inputs to application program SRS development .....	97
B.4.3	Application program design and development.....	101
B.4.4	Application program production .....	115
B.4.5	Application program verification and testing .....	115
B.4.6	Validation.....	115
Annex C (informative)	Considerations when converting from NP technologies to PE technologies.....	117
Annex D (informative)	Example of how to get from a piping and instrumentation diagram (P&ID) to application program .....	119
Annex E (informative)	Methods and tools for application programming .....	123
E.1	Typical toolset for application programming .....	123
E.2	Rules and constraints for application program design .....	124
E.3	Rules and constraints for application programming .....	125
Annex F (informative)	Example SIS project illustrating each phase of the safety life cycle with application program development using relay ladder language.....	127
F.1	Overview .....	127
F.2	Project definition.....	128
F.2.1	General.....	128
F.2.2	Conceptual planning.....	128
F.2.3	Process hazards analysis.....	128
F.3	Simplified process description .....	128
F.4	Preliminary design .....	130
F.5	IEC 61511 application .....	130
F.5.1	General.....	130
F.5.2	Step F.1: Hazard & risk assessment.....	134
F.5.3	Hazard identification.....	134
F.5.4	Preliminary hazard evaluation .....	134
F.5.5	Accident history.....	135
F.6	Preliminary process design safety considerations .....	137
F.7	Recognized process hazards .....	138
F.8	Process design definitions strategy .....	139
F.9	Preliminary hazard assessment .....	141
F.9.1	General.....	141
F.9.2	Step F.2: Allocation of safety functions.....	145
F.10	SIF safety integrity level determination .....	146
F.11	Layer of protection analysis (LOPA) applied to example .....	146
F.12	Tolerable risk criteria .....	148
F.13	Step F.3: SIS safety requirements specifications .....	150
F.13.1	Overview.....	150
F.13.2	Input requirements .....	150
F.13.3	Safety functional requirements .....	151
F.13.4	Safety integrity requirements.....	153

F.14	Functional description and conceptual design .....	153
F.14.1	Narrative for example reactor system logic .....	154
F.15	SIL verification calculations .....	154
F.16	Application program requirements .....	162
F.17	Step F.4: SIS safety life-cycle.....	169
F.18	Technology and device selection .....	169
F.18.1	General.....	169
F.18.2	Logic solver.....	169
F.18.3	Sensors.....	170
F.18.4	Final elements.....	170
F.18.5	Solenoid valves .....	170
F.18.6	Emergency vent valves .....	171
F.18.7	Modulating valves .....	171
F.18.8	Bypass valves .....	171
F.18.9	Human-machine interfaces (HMIs) .....	171
F.18.10	Separation .....	173
F.19	Common cause and systematic failures .....	173
F.19.1	General.....	173
F.19.2	Diversity.....	173
F.19.3	Specification errors .....	174
F.19.4	Hardware design errors .....	174
F.19.5	Software design errors .....	174
F.19.6	Environmental overstress .....	174
F.19.7	Temperature .....	175
F.19.8	Humidity.....	175
F.19.9	Contaminants .....	175
F.19.10	Vibration .....	175
F.19.11	Grounding .....	175
F.19.12	Power line conditioning .....	175
F.19.13	Electro-magnetic compatibility (EMC).....	176
F.19.14	Utility sources .....	177
F.19.15	Sensors.....	177
F.19.16	Process corrosion or fouling .....	177
F.19.17	Maintenance .....	177
F.19.18	Susceptibility to mis-operation.....	177
F.19.19	SIS architecture .....	178
F.20	SIS application program design features .....	180
F.21	Wiring practices.....	180
F.22	Security.....	180
F.23	Step F.5: SIS installation, commissioning, validation .....	181
F.24	Installation.....	181
F.25	Commissioning .....	183
F.26	Documentation .....	183
F.27	Validation .....	184



F.28	Testing .....	184
F.29	Step F.6: SIS operation and maintenance .....	198
F.30	Step F.7: SIS Modification .....	201
F.31	Step F.8: SIS decommissioning .....	201
F.32	Step F.9: SIS verification .....	202
F.33	Step F.10: Management of functional safety and SIS FSA .....	203
F.34	Management of functional safety .....	203
F.34.1	General .....	203
F.34.2	Competence of personnel.....	203
F.35	Functional safety assessment.....	203
Annex G (informative)	Guidance on developing application programming practices .....	205
G.1	Purpose of this guidance .....	205
G.2	Generic safe application programming attributes .....	205
G.3	Reliability .....	206
G.3.1	General.....	206
G.3.2	Predictability of memory utilisation .....	206
G.3.3	Predictability of control flow.....	207
G.3.4	Accounting for precision and accuracy .....	209
G.3.5	Predictability of timing .....	211
G.4	Predictability of mathematical or logical result .....	212
G.5	Robustness .....	212
G.5.1	General.....	212
G.5.2	Controlling use of diversity .....	212
G.5.3	Controlling use of exception handling .....	214
G.5.4	Checking input and output.....	215
G.6	Traceability.....	216
G.6.1	General.....	216
G.6.2	Controlling use of built-in functions.....	216
G.6.3	Controlling use of compiled libraries .....	216
G.7	Maintainability .....	216
G.7.1	General .....	216
G.7.2	Readability .....	217
G.7.3	Data abstraction .....	220
G.7.4	Functional cohesiveness .....	221
G.7.5	Malleability.....	221
G.7.6	Portability.....	222
Bibliography	.....	223

Figure 1 – Overall framework of IEC 61511 series 18

Figure A.1 – Application program V-Model..... 33

Figure A.2 – Independence of a BPCS protection layer and an initiating source in the BPCS..... 42

Figure A.3 – Independence of two protection layers allocated to the BPCS ..... 43

Figure A.4 – Relationship of system, SIS hardware, and SIS application program ..... 48

Figure A.5 – Illustration of uncertainties on a reliability parameter .....	70
Figure A.6 – Illustration of the 70 % confidence upper bound .....	71
Figure A.7 – Typical probabilistic distribution of target results from Monte Carlo simulation .....	72
Figure B.1 – Process flow diagram for SIF 02.01 .....	96
Figure B.2 – Process flow diagram for SIF 06.02 .....	97
Figure B.3 – Functional specification of SIF02.01 and SIF 06.02 .....	98
Figure B.4 – SIF 02.01 hardware functional architecture .....	99
Figure B.5 – SIF 06.02 hardware functional architecture .....	99
Figure B.6 – Hardware specification for SOV extracted from piping and instrumentation diagram .....	100
Figure B.7 – SIF 02.01 hardware physical architecture .....	101
Figure B.8 – SIF 06.02 hardware physical architecture .....	101
Figure B.9 – Hierarchical structure of model integration .....	105
Figure B.10 – Hierarchical structure of model integration including models of safety properties and of BPCS logic .....	107
Figure B.11 – State transition diagram .....	108
Figure B.12 – SOV typical block diagram .....	109
Figure B.13 – SOV typical model block diagram .....	110
Figure B.14 – Typical model block diagram implementation – BPCS part .....	112
Figure B.15 – SOV application program typical model implementation – SIS part .....	113
Figure B.16 – Complete model for final implementation model checking .....	115
Figure D.1 – Example of P&ID for an oil and gas separator .....	119
Figure D.2 – Example of (part of) an ESD cause & effect diagram (C&E) .....	120
Figure D.3 – Example of (part of) an application program in a safety PLC function block programming .....	121
Figure F.1 – Simplified flow diagram: the PVC process .....	129
Figure F.2 – SIS safety life-cycle phases and FSA stages .....	131
Figure F.3 – Example of the preliminary P&ID for PVC reactor unit .....	140
Figure F.4 – SIF S-1 Bubble diagram showing the $PFD_{avg}$ of each SIS device .....	156
Figure F.5 – S-1 Fault tree .....	157
Figure F.6 – SIF S-2 Bubble diagram showing the $PFD_{avg}$ of each SIS device .....	158
Figure F.7 – SIF S-2 fault tree .....	159
Figure F.8 – SIF S-3 Bubble diagram showing the $PFD_{avg}$ of each SIS device .....	160
Figure F.9 – SIF S-3 fault tree .....	161
Figure F.10 – P&ID for PVC reactor unit SIF .....	163
Figure F.11 – Legend (1 of 5) .....	164
Figure F.12 – SIS for the VCM reactor .....	179

Table B.1 – Modes of operation specification.....	102
Table B.2 – State transition table.....	108
Table F.1 – SIS safety life-cycle overview .....	132
Table F.2 – SIS safety life-cycle – Box 1 .....	134
Table F.3 – Some physical properties of vinyl chloride .....	136
Table F.4 – What-If/Checklist .....	142
Table F.5 – HAZOP .....	143
Table F.6 – Partial summary of hazard assessment for SIF strategy development .....	144
Table F.7 – SIS safety life-cycle – Box 2 .....	146
Table F.8 – Tolerable risk ranking .....	148
Table F.9 – VCM reactor example: LOPA based integrity level .....	149
Table F.10 – SIS safety life-cycle – Box 3 .....	150
Table F.11 – Safety instrumented functions and SILs .....	150
Table F.12 – Functional relationship of I/O for the SIF(s).....	151
Table F.13 – SIS sensors, normal operating range & trip points.....	151
Table F.14 – Cause and effect diagram .....	154
Table F.15 – MTTFd figures of SIS F.1 devices .....	155
Table F.16 – SIS safety life-cycle – Box 4 .....	169
Table F.17 – SIS safety life-cycle – Box 5 .....	181
Table F.18 – List of instrument types and testing procedures used .....	186
Table F.19 – Interlock check procedure bypass/simulation check sheet.....	198
Table F.20 – SIS safety life-cycle – Box 6 .....	198
Table F.21 – SIS trip log.....	199
Table F.22 – SIS device failure log.....	199
Table F.23 – SIS safety life-cycle – Box 7 .....	201
Table F.24 – SIS safety life-cycle – Box 8 .....	201
Table F.25 – SIS safety life-cycle – Box 9 .....	202
Table F.26 – SIS safety life-cycle – Box 10.....	203

This page intentionally left blank.

## US NATIONAL FOREWORD FOR ISA-61511-2

*as approved by the ISA84 Committee*

The ballot to adopt IEC 61511-2:2016 as an ANSI/ISA standard without modification was approved by a majority of the ISA84 committee voting members. However, several members expressed concerns about the guidance and interpretation of the document. For this reason, users are referred to the ISA84 technical reports listed below for guidance on the same topics.

In order to promote consistency in usage across IEC member countries, ISA is adopting IEC 61511-2:2016 as an ISA and American National Standard despite those concerns, with the following comments:

1. The concerns from the ISA84 ballot regarding the guidance included in the informative annexes of IEC 61511-2:2016 will be communicated by the ISA84 liaisons to IEC TC65/SC65A for deliberation. ISA and IEC will strive for closer collaboration on future editions of IEC 61511.
2. The following ISA84 Technical Reports (or more recent editions when completed by ISA84) provide background and information that is helpful in understanding ISA/IEC 61511:
  - ISA-TR84.00.02-2015, *Safety Integrity Level (SIL) Verification of Safety Instrumented Functions*
  - ISA-TR84.00.03-2012, *Mechanical Integrity of Safety Instrumented Systems (SIS)*
  - ISA-TR84.00.04-2015, Part 1, *Guideline for the Implementation of ANSI/ISA-84.00.01-2004 (IEC 61511 Mod)*
  - ISA-TR84.00.04-2005, Part 2, *Example Implementation of ANSI/ISA-84.00.01-2004 (IEC 61511 Mod)*
  - ISA-TR84.00.05-2009, *Guidance on the Identification of Safety Instrumented Functions (SIF) in Burner Management Systems (BMS)*
  - ISA-TR84.00.06-2009, *Safety Fieldbus Design Considerations for Process Industry Sector Applications*
  - ISA-TR84.00.07-2010, *Guidance on the Evaluation of Fire, Combustible Gas and Toxic Gas System Effectiveness*
  - ISA-TR84.00.08-2017, *Guidance for Application of Wireless Sensor Technology to Non-SIS Independent Protection Layers*
  - ISA-TR84.00.09-2017, *Cybersecurity Related to the Functional Safety Lifecycle*

For a description of the scope and contents of each of these ISA84 technical reports, visit [www.isa.org/findstandards](http://www.isa.org/findstandards). Users are referred to the most recent edition of each as listed at that address.

3. Questions and suggestions regarding ISA-61511 may be sent to [standards@isa.org](mailto:standards@isa.org) for possible referral to IEC TC65/SC65A.
4. Experts from any country are welcome to join the ISA84 committee by contacting [standards@isa.org](mailto:standards@isa.org). There is no fee to participate.

This page intentionally left blank.

## INTERNATIONAL ELECTROTECHNICAL COMMISSION

---

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

#### Part 2: Guidelines for the application of IEC 61511-1:2016

#### 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 61511-2 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:

- guidance examples based on all phases of the safety life cycle provided based on usage experience with IEC61511 1<sup>st</sup> edition;
- annexes replaced to address transition from software to application programming.

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

FDIS	Report on voting
65A/783/FDIS	65A/787/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.

This International Standard is to be read in conjunction with IEC 61511-1. It is based on the second edition of that standard.

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 (SISs) have been used for many years to perform safety instrumented functions (SIFs) in the process industries. If instrumentation is to be effectively used for SIFs, it is essential that this instrumentation achieves certain minimum standards.

The IEC 61511 series addresses the application of SISs for the process industries. It also deals with the interface between SISs and other safety systems in requiring that a process H&RA be carried out. The SIS includes sensors, logic solvers and final elements.

The IEC 61511 series has two concepts, which are fundamental to its application; SIS safety life-cycle and the safety integrity level (SIL). The SIS safety life-cycle forms the central framework which links together most of the concepts in this International Standard.

The SIS 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 can be applied to ensure the functional safety requirements were met. The IEC 61511 series also addresses the SIS sensors and final elements regardless of the technology used. The IEC 61511 series has been developed as a process sector implementation of the IEC 61508 series. The IEC 61511 series is process industry specific within the framework of the IEC 61508 series.

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. The objective of this part of IEC 61511 is to provide guidance on how to comply with IEC 61511-1:2016.

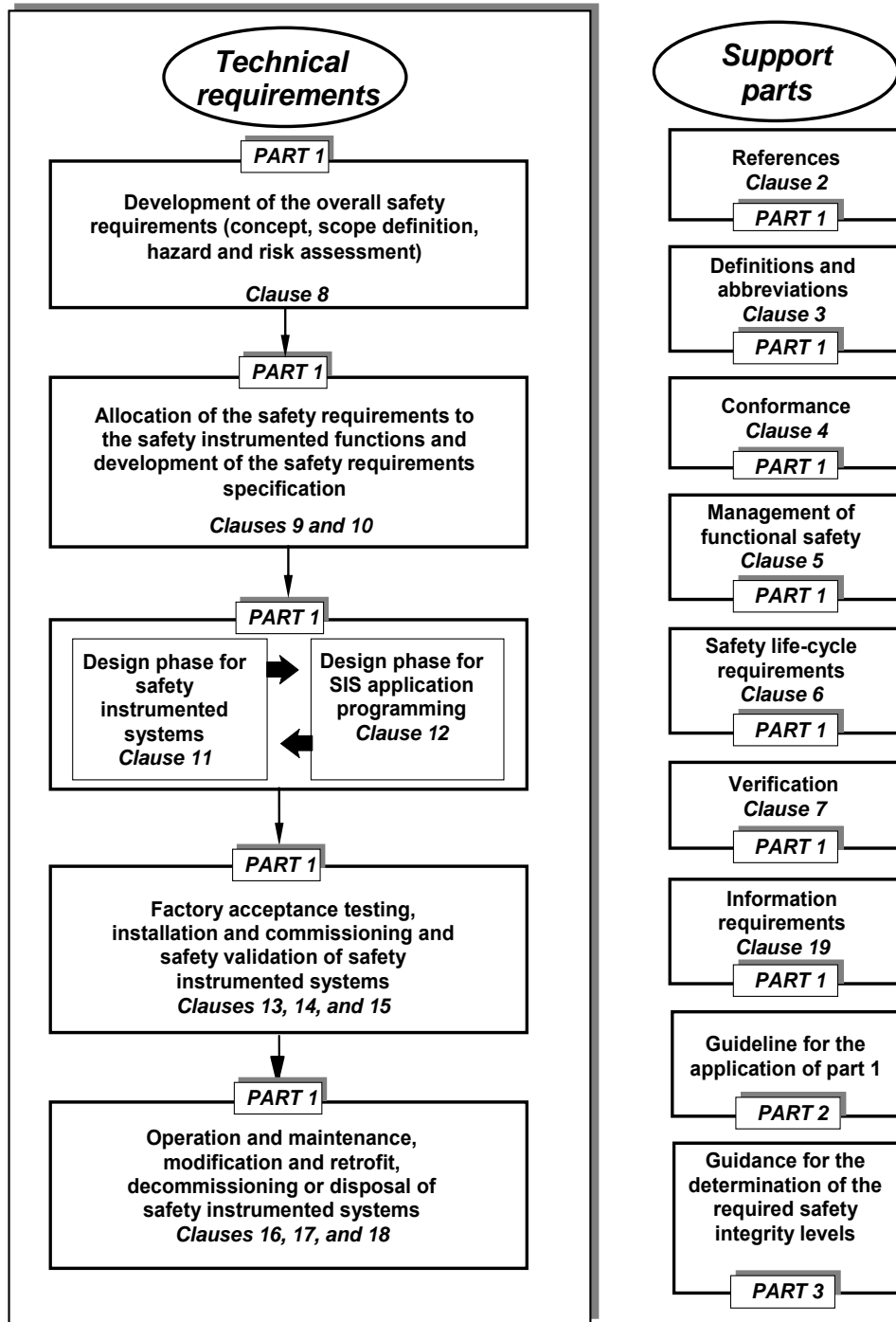
To facilitate use of IEC 61511-1:2016, the clause numbers provided in Annex A (informative) are identical to the corresponding normative text in IEC 61511-1:2016 except for the “A” notation.

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 (e.g., chemical, mechanical, hydraulic, pneumatic, electrical, electronic, thermodynamic (e.g., flame arrestors), programmable electronic) which manage any residual identified risk. Any safety strategy considers each individual SIS in the context of the other protective systems. To facilitate this approach, IEC 61511-1:2016:

- requires that a H&RA 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 SIS(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.
- addresses relevant SIS safety life-cycle 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.

The IEC 61511 series is intended to lead to a high level of consistency (e.g., of underlying principles, terminology, information) within the process industries. This should have both safety and economic benefits.

Figure 1 below shows the overall framework of the IEC 61511 series.



IEC

Figure 1 – Overall framework of IEC 61511 series

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

## **Part 2: Guidelines for the application of IEC 61511-1:2016**

### **1 Scope**

This part of IEC 61511 provides guidance on the specification, design, installation, operation and maintenance of SIFs and related SIS as defined in IEC 61511-1:2016.

NOTE 1 Annex A (informative) has been organized so that each clause and subclause number therein addresses the corresponding clause and subclause number in IEC 61511-1:2016 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 compliance with IEC rules which prohibit a standard being wholly informative.

NOTE 3 To achieve maximum use of this guideline;

- review the section guidance as well as the specific clause guidance. (e.g., when looking for guidance on 5.2.6.1.3, consider guidance in 5.2.6);
- 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 IEC 61511 requirements in a specific instance, and the user should satisfy themselves that the chosen methods and techniques are appropriate to their situation.

### **2 Normative references**

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 61511-1:2016, *Functional safety – Safety instrumented systems for the process industry sector – Part 1: Framework, definitions, system, hardware and application programming requirements*

### **3 Terms, definitions, and abbreviations**

For the purposes of this document, the terms, definitions, and abbreviations given in IEC 61511-1:–, Clause 3 apply.