

# INTERNATIONAL STANDARD



**Functional safety – Safety instrumented systems for the process industry sector –  
Part 2: Guidelines for the application of IEC 61511-1:2016**

Document Preview

[IEC 61511-2:2016](#)

<https://standards.iteh.ai/catalog/standards/iec/f93f8b02-1d58-4a76-b321-df8609422e5e/iec-61511-2-2016>



## THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2016 IEC, Geneva, Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester. If you have any questions about IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

IEC Central Office  
3, rue de Varembe  
CH-1211 Geneva 20  
Switzerland

Tel.: +41 22 919 02 11  
Fax: +41 22 919 03 00  
[info@iec.ch](mailto:info@iec.ch)  
[www.iec.ch](http://www.iec.ch)

### About the IEC

The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

### About IEC publications

The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigenda or an amendment might have been published.

#### IEC Catalogue - [webstore.iec.ch/catalogue](http://webstore.iec.ch/catalogue)

The stand-alone application for consulting the entire bibliographical information on IEC International Standards, Technical Specifications, Technical Reports and other documents. Available for PC, Mac OS, Android Tablets and iPad.

#### IEC publications search - [www.iec.ch/searchpub](http://www.iec.ch/searchpub)

The advanced search enables to find IEC publications by a variety of criteria (reference number, text, technical committee,...). It also gives information on projects, replaced and withdrawn publications.

#### IEC Just Published - [webstore.iec.ch/justpublished](http://webstore.iec.ch/justpublished)

Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and also once a month by email.

#### Electropedia - [www.electropedia.org](http://www.electropedia.org)

The world's leading online dictionary of electronic and electrical terms containing 20 000 terms and definitions in English and French, with equivalent terms in 15 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

#### IEC Glossary - [std.iec.ch/glossary](http://std.iec.ch/glossary)

65 000 electrotechnical terminology entries in English and French extracted from the Terms and Definitions clause of IEC publications issued since 2002. Some entries have been collected from earlier publications of IEC TC 37, 77, 86 and CISPR.

#### IEC Customer Service Centre - [webstore.iec.ch/csc](http://webstore.iec.ch/csc)

If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: [csc@iec.ch](mailto:csc@iec.ch).

<https://standards.iteh.ai/catalog/standards/iec/93f8b02-1d58-4a76-b321-df8609422e5e/iec-61511-2-2016>

<https://standards.iteh.ai/catalog/standards/iec/93f8b02-1d58-4a76-b321-df8609422e5e/iec-61511-2-2016>



IEC 61511-2

Edition 2.0 2016-07  
REDLINE VERSION

# INTERNATIONAL STANDARD



---

**Functional safety – Safety instrumented systems for the process industry  
sector –  
Part 2: Guidelines for the application of IEC 61511-1:2016**

Document Preview

[IEC 61511-2:2016](https://standards.iteh.ai/catalog/standards/iec/193f8b02-1d58-4a76-b321-df8609422e5e/iec-61511-2-2016)

<https://standards.iteh.ai/catalog/standards/iec/193f8b02-1d58-4a76-b321-df8609422e5e/iec-61511-2-2016>

INTERNATIONAL  
ELECTROTECHNICAL  
COMMISSION

---

ICS 13.110; 25.040.01

ISBN 978-2-8322-3549-2

**Warning! Make sure that you obtained this publication from an authorized distributor.**

## 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 <del>this International Standard</del> the IEC 61511-1:- .....	14
A.5 Management of functional safety.....	14
A.5.1 Objective .....	14
A.5.2 Guidance to "Requirements" .....	15
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" .....	31
A.9.3 Guidance to "Requirements on the basic process control system as a protection layer" .....	33
A.9.4 Guidance to "Requirements for preventing common cause, common mode and dependent failures" .....	36
A.10 SIS safety requirements specification .....	37
A.10.1 Objective .....	37
A.10.2 Guidance to "General requirements" .....	37
A.10.3 Guidance to "SIS safety requirements" .....	37
A.11 SIS design and engineering .....	42
A.11.1 Objective .....	42
A.11.2 Guidance to "General requirements".....	42
A.11.3 Guidance to "Requirements for system behaviour on detection of a fault".....	50
A.11.4 <del>Requirements</del> Guidance to "Hardware fault tolerance".....	50
A.11.5 Guidance to "Requirements for selection of <del>components and subsystems</del> devices" .....	53
A.11.6 Field devices .....	57
A.11.7 Interfaces .....	57
A.11.8 Guidance to "Maintenance or testing design requirements".....	59
A.11.9 <del>SIF probability of failure</del> Guidance to "Quantification of random failure".....	60

<del>12</del>	<del>Requirements for application software, including selection criteria for utility software</del>	<del>81</del>
<del>12.1</del>	<del>Application software safety lifecycle requirements</del>	<del>81</del>
<del>12.2</del>	<del>Application software safety requirements specification</del>	<del>81</del>
<del>12.3</del>	<del>Application software safety validation planning</del>	<del>81</del>
<del>12.4</del>	<del>Application software design and development</del>	<del>81</del>
<del>12.5</del>	<del>Integration of the application software with the SIS subsystem</del>	<del>81</del>
<del>12.6</del>	<del>FPL and LVL software modification procedures</del>	<del>81</del>
<del>12.7</del>	<del>Application software verification</del>	<del>81</del>
A.12	SIS application program development	81
A.12.1	Objective	81
A.12.2	Guidance to "General requirements"	81
A.12.4	Guidance to "Application program implementation"	84
A.12.3	Guidance to "Application program design"	82
A.12.5	Guidance to "Requirements for application program verification (review and testing)"	85
A.12.6	Guidance to "Requirements for application program methodology and tools"	89
A.13	Factory acceptance testing (FAT)	91
A.13.1	Objectives	91
A.13.2	Guidance to "Recommendations"	91
A.14	SIS installation and commissioning	91
A.14.1	Objectives	91
A.14.2	Guidance to "Requirements"	92
A.15	SIS safety validation	92
A.15.1	Objective	92
A.15.2	Guidance to "Requirements"	92
A.16	SIS operation and maintenance	93
A.16.1	Objectives	93
A.16.2	Guidance to "Requirements"	93
A.16.3	Proof testing and inspection	94
A.17	SIS modification	97
A.17.1	Objective	97
A.17.2	Guidance to "Requirements"	97
A.18	SIS decommissioning	98
A.18.1	Objectives	98
A.18.2	Guidance to "Requirements"	98
A.19	Information and documentation requirements	98
A.19.1	Objectives	98
A.19.2	Guidance to "Requirements"	98
<del>Annex A (informative) Example of techniques for calculating the probability of failure on demand for a safety instrumented function</del>		
<del>Annex B (informative) Typical SIS architecture development</del>		
Annex B (informative) Example of SIS logic solver application program development using function block diagram		
		106
B.1	General	106
B.2	Application program development and validation philosophy	106
B.3	Application description	107
B.3.1	General	107

B.3.2	Process description.....	107
B.3.3	Safety instrumented functions .....	108
B.3.4	Risk reduction and domino effects .....	109
B.4	Application program safety life-cycle execution .....	109
B.4.1	General .....	109
B.4.2	Inputs to application program SRS development .....	109
B.4.3	Application program design and development .....	112
B.4.4	Application program production .....	126
B.4.5	Application program verification and testing .....	126
B.4.6	Validation .....	126
<del>Annex C (informative) Application features of a safety PLC .....</del>		
Annex C (informative)	Considerations when converting from NP technologies to PE technologies .....	129
<del>Annex D (informative) Example of SIS logic solver application software development methodology .....</del>		
Annex D (informative)	Example of how to get from a piping and instrumentation diagram (P&ID) to application program .....	135
<del>Annex E (informative) Example of development of externally configured diagnostics for a safety-configured PE logic solver .....</del>		
Annex E (informative)	Methods and tools for application programming .....	141
E.1	Typical toolset for application programming .....	141
E.2	Rules and constraints for application program design.....	142
E.3	Rules and constraints for application programming .....	142
Annex F (informative)	Example SIS project illustrating each phase of the safety life cycle with application program development using relay ladder language .....	144
F.1	Overview .....	144
F.2	Project definition .....	144
F.2.1	General .....	144
F.2.2	Conceptual planning .....	145
F.2.3	Process hazards analysis .....	145
F.3	Simplified process description .....	145
F.4	Preliminary design .....	147
F.5	IEC 61511 application .....	147
F.5.1	General .....	147
F.5.2	Step F.1: Hazard & risk assessment .....	151
F.5.3	Hazard identification .....	151
F.5.4	Preliminary hazard evaluation .....	151
F.5.5	Accident history .....	151
F.6	Preliminary process design safety considerations .....	154
F.7	Recognized process hazards .....	154
F.8	Process design definitions strategy.....	155
F.9	Preliminary hazard assessment .....	158
F.9.1	General .....	158
F.9.2	Step F.2: Allocation of safety functions .....	162
F.10	SIF safety integrity level determination .....	163
F.11	Layer of protection analysis (LOPA) applied to example .....	163
F.12	Tolerable risk criteria.....	164
F.13	Step F.3: SIS safety requirements specifications.....	167
F.13.1	Overview .....	167

F.13.2	Input requirements .....	167
F.13.3	Safety functional requirements .....	168
F.13.4	Safety integrity requirements .....	169
F.14	Functional description and conceptual design .....	170
F.14.1	Narrative for example reactor system logic .....	170
F.15	SIL verification calculations .....	171
F.16	Application program requirements .....	178
F.17	Step F.4: SIS safety life-cycle .....	185
F.18	Technology and device selection .....	185
F.18.1	General .....	185
F.18.2	Logic solver .....	185
F.18.3	Sensors .....	186
F.18.4	Final elements .....	186
F.18.5	Solenoid valves .....	186
F.18.6	Emergency vent valves .....	187
F.18.7	Modulating valves .....	187
F.18.8	Bypass valves .....	187
F.18.9	Human-machine interfaces (HMIs) .....	187
F.18.10	Separation .....	188
F.19	Common cause and systematic failures .....	189
F.19.1	General .....	189
F.19.2	Diversity .....	189
F.19.3	Specification errors .....	189
F.19.4	Hardware design errors .....	189
F.19.5	Software design errors .....	190
F.19.6	Environmental overstress .....	190
F.19.7	Temperature .....	190
F.19.8	Humidity .....	190
F.19.9	Contaminants .....	191
F.19.10	Vibration .....	191
F.19.11	Grounding .....	191
F.19.12	Power line conditioning .....	191
F.19.13	Electro-magnetic compatibility (EMC) .....	191
F.19.14	Utility sources .....	192
F.19.15	Sensors .....	193
F.19.16	Process corrosion or fouling .....	193
F.19.17	Maintenance .....	193
F.19.18	Susceptibility to mis-operation .....	193
F.19.19	SIS architecture .....	193
F.20	SIS application program design features .....	194
F.21	Wiring practices .....	195
F.22	Security .....	195
F.23	Step F.5: SIS installation, commissioning, validation .....	196
F.24	Installation .....	196
F.25	Commissioning .....	197
F.26	Documentation .....	198
F.27	Validation .....	198
F.28	Testing .....	199
F.29	Step F.6: SIS operation and maintenance .....	212

F.30	Step F.7: SIS Modification .....	215
F.31	Step F.8: SIS decommissioning .....	215
F.32	Step F.9: SIS verification .....	215
F.33	Step F.10: Management of functional safety and SIS FSA .....	217
F.34	Management of functional safety .....	217
F.34.1	General .....	217
F.34.2	Competence of personnel .....	217
F.35	Functional safety assessment .....	217
Annex G (informative)	Guidance on developing application programming practices .....	218
G.1	Purpose of this guidance .....	218
G.2	Generic safe application programming attributes .....	218
G.3	Reliability .....	218
G.3.1	General .....	218
G.3.2	Predictability of memory utilisation .....	219
G.3.3	Predictability of control flow .....	220
G.3.4	Accounting for precision and accuracy .....	222
G.3.5	Predictability of timing .....	224
G.4	Predictability of mathematical or logical result .....	224
G.5	Robustness .....	225
G.5.1	General .....	225
G.5.2	Controlling use of diversity .....	225
G.5.3	Controlling use of exception handling .....	226
G.5.4	Checking input and output .....	227
G.6	Traceability .....	228
G.6.1	General .....	228
G.6.2	Controlling use of built-in functions .....	228
G.6.3	Controlling use of compiled libraries .....	228
G.7	Maintainability .....	228
G.7.1	General .....	228
G.7.2	Readability .....	229
G.7.3	Data abstraction .....	232
G.7.4	Functional cohesiveness .....	233
G.7.5	Malleability .....	233
G.7.6	Portability .....	233
Bibliography	.....	235

Figure 1 – Overall framework of IEC 61511 series .....	12
--	----

<del>Figure 2 – BPCS function and initiating cause independence illustration .....</del>	<del>.....</del>
--	------------------

<del>Figure 3 – Software development lifecycle (the V-model) .....</del>	<del>.....</del>
--	------------------

Figure A.1 – Application program V-Model .....	25
--	----

Figure A.2 – Independence of a BPCS protection layer and an initiating source in the BPCS .....	35
---	----

Figure A.3 – Independence of two protection layers allocated to the BPCS .....	36
--	----

Figure A.4 – Relationship of system, SIS hardware, and SIS application program .....	41
--	----

Figure A.5 – Illustration of uncertainties on a reliability parameter .....	64
---	----

Figure A.6 – Illustration of the 70 % confidence upper bound .....	65
--	----

Figure A.7 – Typical probabilistic distribution of target results from Monte Carlo simulation .....	66
---	----



Figure B.1 – Process flow diagram for SIF 02.01 .....	108
Figure B.2 – Process flow diagram for SIF 06.02 .....	109
Figure B.3 – Functional specification of SIF02.01 and SIF 06.02 .....	110
Figure B.4 – SIF 02.01 hardware functional architecture .....	110
Figure B.5 – SIF 06.02 hardware functional architecture .....	111
Figure B.6 – Hardware specification for SOV extracted from piping and instrumentation diagram.....	111
Figure B.7 – SIF 02.01 hardware physical architecture .....	112
Figure B.8 – SIF 06.02 hardware physical architecture .....	112
Figure B.9 – Hierarchical structure of model integration .....	116
Figure B.10 – Hierarchical structure of model integration including models of safety properties and of BPCS logic .....	118
Figure B.11 – State transition diagram .....	119
Figure B.12 – SOV typical block diagram.....	120
Figure B.14 – Typical model block diagram implementation – BPCS part.....	123
Figure B.13 – SOV typical model block diagram .....	121
Figure B.15 – SOV application program typical model implementation – SIS part .....	124
Figure B.16 – Complete model for final implementation model checking .....	126
<del>Figure C.1 – Logic solver .....</del>	<del>.....</del>
Figure D.1 – Example of P&ID for an oil and gas separator.....	135
Figure D.2 – Example of (part of) an ESD cause & effect diagram (C&E).....	136
Figure D.3 – Example of (part of) an application program in a safety PLC function block programming .....	137
<del>Figure E.1 – EWDT timing diagram .....</del>	<del>.....</del>
Figure F.1 – Simplified flow diagram: the PVC process .....	146
Figure F.2 – SIS safety life-cycle phases and FSA stages.....	148
Figure F.3 – Example of the preliminary P&ID for PVC reactor unit .....	157
Figure F.4 – SIF S-1 Bubble diagram showing the $PFD_{avg}$ of each SIS device.....	173
Figure F.5 – S-1 Fault tree .....	174
Figure F.6 – SIF S-2 Bubble diagram showing the $PFD_{avg}$ of each SIS device.....	175
Figure F.7 – SIF S-2 fault tree .....	176
Figure F.8 – SIF S-3 Bubble diagram showing the $PFD_{avg}$ of each SIS device.....	177
Figure F.9 – SIF S-3 fault tree.....	178
Figure F.10 – P&ID for PVC reactor unit SIF.....	179
Figure F.11 – Legend (1 of 5).....	180
Figure F.12 – SIS for the VCM reactor.....	194
<del>Table 1 – Typical Safety Manual organisation and contents .....</del>	<del>.....</del>
Table B.1 – Modes of operation specification.....	113
Table B.2 – State transition table .....	119
Table F.1 – SIS safety life-cycle overview .....	149
Table F.2 – SIS safety life-cycle – Box 1 .....	151
Table F.3 – Some physical properties of vinyl chloride.....	153
Table F.4 – What-If/Checklist .....	159

Table F.5 – HAZOP .....	160
Table F.6 – Partial summary of hazard assessment for SIF strategy development .....	161
Table F.7 – SIS safety life-cycle – Box 2 .....	163
Table F.8 – Tolerable risk ranking .....	165
Table F.9 – VCM reactor example: LOPA based integrity level.....	166
Table F.10 – SIS safety life-cycle – Box 3 .....	167
Table F.11 – Safety instrumented functions and SILs.....	167
Table F.12 – Functional relationship of I/O for the SIF(s) .....	168
Table F.13 – SIS sensors, normal operating range & trip points .....	168
Table F.14 – Cause and effect diagram .....	171
Table F.15 – MTTFd figures of SIS F.1 devices .....	172
Table F.16 – SIS safety life-cycle – Box 4 .....	185
Table F.17 – SIS safety life-cycle – Box 5 .....	196
Table F.18 – List of instrument types and testing procedures used.....	200
Table F.19 – Interlock check procedure bypass/simulation check sheet.....	212
Table F.20 – SIS safety life-cycle – Box 6 .....	212
Table F.21 – SIS trip log .....	213
Table F.22 – SIS device failure log.....	213
Table F.23 – SIS safety life-cycle – Box 7 .....	215
Table F.24 – SIS safety life-cycle – Box 8 .....	215
Table F.25 – SIS safety life-cycle – Box 9 .....	216

ITC Standards  
 (https://standards.itech.ai)  
 Document Preview

[IEC 61511-2:2016](#)

<https://standards.itech.ai/catalog/standards/iec/193f8b02-1d58-4a76-b321-df8609422e5e/iec-61511-2-2016>

## 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.

**This redline version of the official IEC Standard allows the user to identify the changes made to the previous edition. A vertical bar appears in the margin wherever a change has been made. Additions are in green text, deletions are in strikethrough red text.**

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 ~~hazard and risk assessment~~ 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 ~~may also~~ 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 ~~and subclause~~ numbers provided in Annex A (informative) are identical to the corresponding normative text in IEC 61511-1:2016 ~~(excluding the annexes)~~ 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:

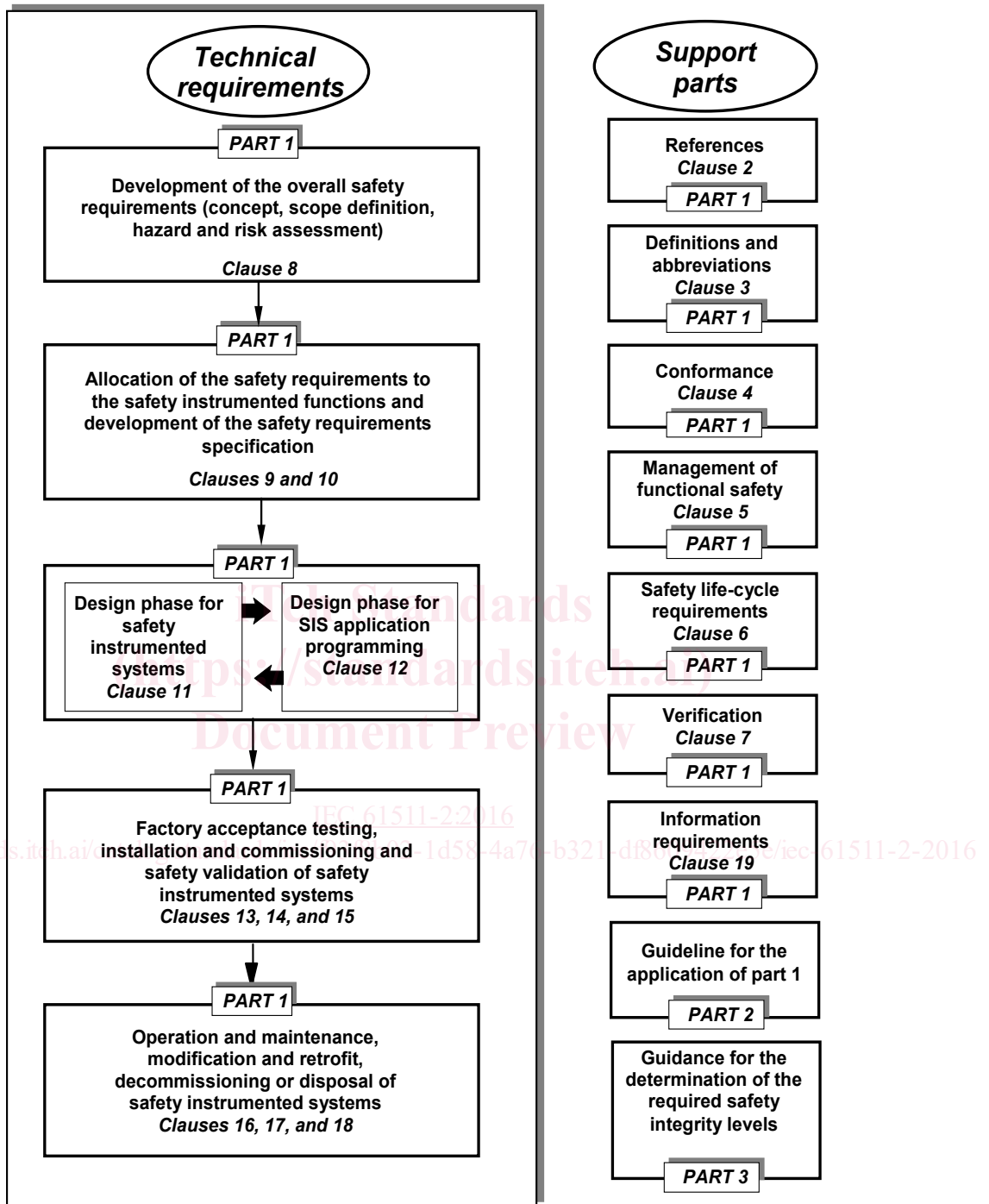
- requires that a H&RA is carried out to identify the overall safety requirements;
- requires that an allocation of the safety requirements to the safety functions and related safety systems, such as the SIS(s), is carried out;
- works within a framework which is applicable to all instrumented methods 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.

~~This International Standard on safety instrumented systems for the process industry:~~

- 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