IEC 61511-2

Edition 2.0 2016-07
REDLINE VERSION

INTERNATIONAL STANDARD

colour inside

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

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 ~~this International Standard~~ 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 "Requirementsof 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 ~~Requirements~~ Guidance to "Hardware fault tolerance" 50
A.11.5 Guidance to "Requirements for selection of ~~components and subsystems~~ 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 ~~SIF probability of failure~~ Guidance to "Quantification of random failure" 60

~~12 Requirements for application software, including selection criteria for utility software~~
~~12.1 Application software safety lifecycle requirements~~
~~12.2 Application software safety requirements specification~~
~~12.3 Application software safety validation planning~~
~~12.4 Application software design and development~~
~~12.5 Integration of the application software with the SIS subsystem~~
~~12.6 FPL and LVL software modification procedures~~
~~12.7 Application software verification~~
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
~~Annex A (informative) Example of techniques for calculating the probability of failure on demand for a safety instrumented function~~
~~Annex B (informative) Typical SIS architecture development~~
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
~~Annex C (informative) Application features of a safety PLC ....~~
Annex C (informative) Considerations when converting from NP technologies to PE technologies 129
~~Annex D (informative) Example of SIS logic solver application software development methodology ....~~
Annex D (informative) Example of how to get from a piping and instrumentation diagram (P&ID) to application program 135
~~Annex E (informative) Example of development of externally configured diagnostics for a safety-configured PE logic solver ....~~
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
~~Figure 2 – BPCS function and initiating cause independence illustration .....~~
~~Figure 3 – Software development lifecycle (the V-model) .....~~
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
~~Figure C.1 – Logic solver .....~~
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
~~Figure E.1 – EWDT timing diagram .....~~
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

~~Table 1 – Typical Safety Manual organisation and contents .....~~
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

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 1st 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.

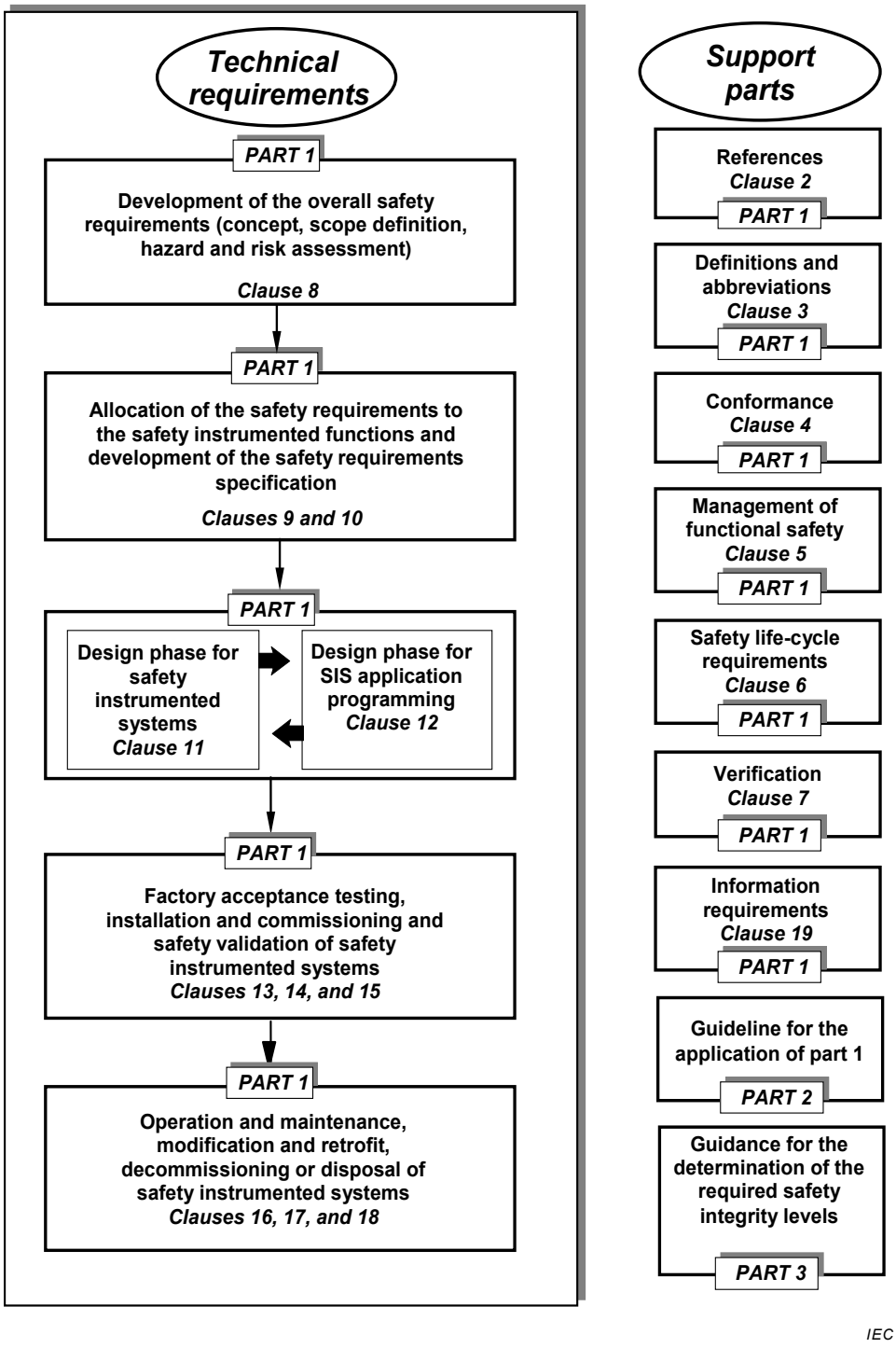


Figure 1 – Overall framework of IEC 61511 series

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. ~~This standard has been organized so that each clause and subclause number herein addresses the same clause number in IEC 61511-1 (with the exception of the annexes).~~

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*

IEC 61511-2

Edition 2.0 2016-07

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

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

Sécurité fonctionnelle – Systèmes instrumentés de sécurité pour le secteur des industries de transformation – Partie 2: Lignes directrices pour l'application de l'IEC 61511-1:2016

IEC 61511-2:2016-07(en-fr)

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 PFD_{avg} of each SIS device 139
Figure F.5 – S-1 Fault tree 140
Figure F.6 – SIF S-2 Bubble diagram showing the PFD_{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 PFD_{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

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 1st 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.

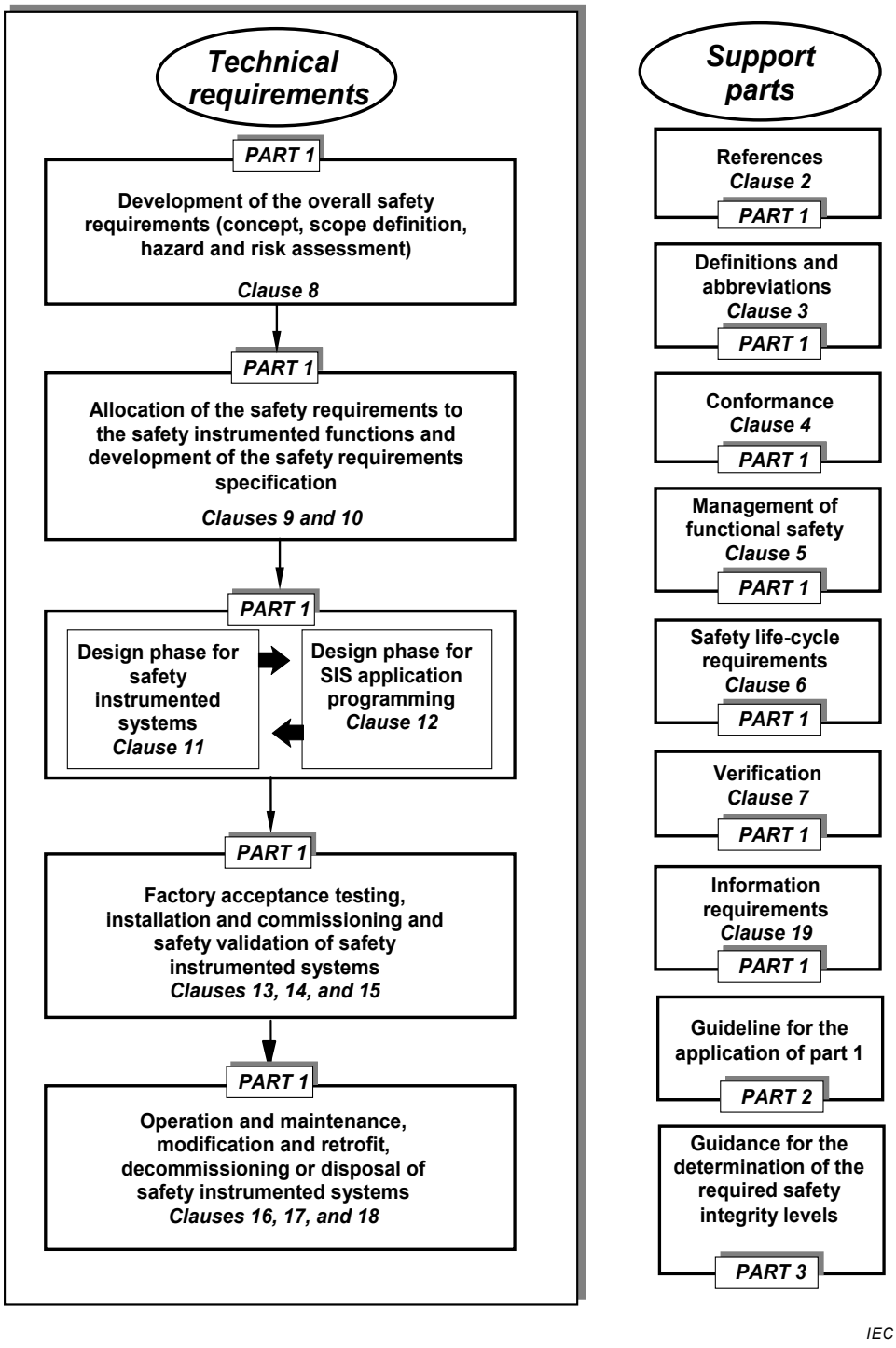


Figure 1 – Overall framework of IEC 61511 series

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*

SOMMAIRE

AVANT-PROPOS 211
INTRODUCTION 213
1 Domaine d'application 217
2 Références normatives 217
3 Termes, définitions et abréviations 217
Annexe A (informative) Lignes directrices pour l'IEC 61511-1 218
A.1 Domaine d'application 218
A.2 Références normatives 218
A.3 Termes, définitions et abréviations 218
A.4 Conformité à l'IEC 61511-1:2016 218
A.5 Gestion de la sécurité fonctionnelle 218
A.5.1 Objectif 218
A.5.2 Lignes directrices relatives aux "Exigences" 219
A.6 Exigences relatives au cycle de vie de sécurité 228
A.6.1 Objectifs 228
A.6.2 Lignes directrices relatives aux "Exigences" 228
A.6.3 Lignes directrices des "exigences relatives aux cycles de vie de sécurité du SIS du programme d'application" 229
A.7 Vérification 230
A.7.1 Objectif 230
A.7.2 Lignes directrices relatives aux "Exigences" 230
A.8 Analyse de danger et de risque (H&RA) 232
A.8.1 Objectifs 232
A.8.2 Lignes directrices relatives aux "Exigences" 232
A.9 Affectation des fonctions de sécurité aux couches de protection 236
A.9.1 Objectif 236
A.9.2 Lignes directrices relatives aux "Exigences relatives au processus d'allocation" 236
A.9.3 Lignes directrices relatives aux "Exigences relatives au système de commande de processus de base en tant que couche de protection" 238
A.9.4 Lignes directrices relatives aux "Exigences pour prévenir les défaillances de cause commune, les défaillances de mode commun et les défaillances dépendantes" 241
A.10 Spécification des exigences concernant la sécurité du SIS 242
A.10.1 Objectif 242
A.10.2 Lignes directrices relatives aux "Exigences générales" 242
A.10.3 Lignes directrices relatives aux "Exigences de sécurité du SIS" 243
A.11 Conception et ingénierie du SIS 248
A.11.1 Objectif 248
A.11.2 Lignes directrices relatives aux "Exigences générales" 248
A.11.3 Lignes directrices pour les "Exigences relatives au comportement du système lors de la détection d'une anomalie" 255
A.11.4 Lignes directrices pour la "Tolérance aux défauts du matériel" 255
A.11.5 Lignes directrices relatives aux "Exigences relatives au choix des appareils" 259
A.11.6 Appareils de terrain 262
A.11.7 Interfaces 262

A.11.8 Lignes directrices relatives aux "Exigences relatives à la maintenance ou à la conception des essais" 265
A.11.9 Lignes directrices relatives à la "Quantification de défaillance aléatoire" 266
A.12 Développement du programme d'application du SIS 273
A.12.1 Objectif 273
A.12.2 Lignes directrices relatives aux "Exigences générales" 273
A.12.3 Lignes directrices relatives à la "Conception du programme d'application" 274
A.12.4 Lignes directrices relatives à la "Mise en œuvre du programme d'application" 277
A.12.5 Lignes directrices relatives aux "Exigences relatives à la vérification du programme d'application (revue et essai)" 278
A.12.6 Lignes directrices relatives aux "Exigences relatives à la méthodologie et aux outils du programme d'application" 283
A.13 Essai de réception en usine (ERU) 285
A.13.1 Objectifs 285
A.13.2 Lignes directrices relatives aux "Recommandations" 285
A.14 Installation et mise en service du SIS 286
A.14.1 Objectifs 286
A.14.2 Lignes directrices relatives aux "Exigences" 286
A.15 Validation de sécurité du SIS 286
A.15.1 Objectif 286
A.15.2 Lignes directrices relatives aux "Exigences" 286
A.16 Fonctionnement et maintenance du SIS 287
A.16.1 Objectifs 287
A.16.2 Lignes directrices relatives aux "Exigences" 287
A.16.3 Essais périodiques et inspection 289
A.17 Modification du SIS 292
A.17.1 Objectif 292
A.17.2 Lignes directrices relatives aux "Exigences" 292
A.18 Déclassement du SIS 292
A.18.1 Objectifs 292
A.18.2 Lignes directrices relatives aux "Exigences" 292
A.19 Exigences relatives aux informations et à la documentation 293
A.19.1 Objectifs 293
A.19.2 Lignes directrices relatives aux "Exigences" 293
Annexe B (informative) Exemple de développement de programme d'application de solveur logique de SIS à l'aide d'un diagramme de bloc fonctionnel 294
B.1 Généralités 294
B.2 Développement du programme d'application et philosophie de validation 294
B.3 Description de l'application 296
B.3.1 Généralités 296
B.3.2 Description du processus 296
B.3.3 Fonctions instrumentées de sécurité 296
B.3.4 Réduction de risque et réaction en chaîne 298
B.4 Exécution du cycle de vie de sécurité du programme d'application 298
B.4.1 Généralités 298
B.4.2 Entrées pour le développement de la SRS du programme d'application 298
B.4.3 Conception et développement du programme d'application 303
B.4.4 Production du programme d'application 321

B.4.5 Vérification et essai du programme d'application 321
B.4.6 Validation 321
Annexe C (informative) Considérations lors de la conversion des technologies NP en technologies PE 322
Annexe D (informative) Exemple présentant le passage d'un schéma de tuyauterie et d'instrumentation (P&ID) à un programme d'application 324
Annexe E (informative) Méthodes et outils de programmation d'application 328
E.1 Jeu d'outils type pour la programmation d'application 328
E.2 Règles et contraintes pour la conception du programme d'application 329
E.3 Règles et contraintes pour la programmation d'application 330
Annexe F (informative) Exemple de projet de SIS présentant chaque phase du cycle de vie de sécurité avec le développement du programme d'application en utilisant le langage à relais 332
F.1 Présentation 332
F.2 Définition du projet 333
F.2.1 Généralités 333
F.2.2 Planification conceptuelle 333
F.2.3 Analyse des dangers du processus 333
F.3 Description simplifiée du processus 334
F.4 Conception préliminaire 335
F.5 Application de l'IEC 61511 335
F.5.1 Généralités 335
F.5.2 Etape F.1: Analyse de danger et de risque 340
F.5.3 Identification de danger 340
F.5.4 Evaluation de danger préliminaire 340
F.5.5 Historique de l'accident 341
F.6 Considérations de sécurité de conception du processus préliminaire 343
F.7 Dangers de processus reconnus 343
F.8 Stratégie des définitions de conception du processus 345
F.9 Evaluation du danger préliminaire 347
F.9.1 Généralités 347
F.9.2 Etape F.2: Affectation des fonctions de sécurité 353
F.10 Détermination du niveau d'intégrité de sécurité de la SIF 353
F.11 Analyse de la couche de protection (LOPA) appliquée à un exemple 353
F.12 Critères de risque tolérables 355
F.13 Etape F.3: Spécifications des exigences concernant la sécurité du SIS 357
F.13.1 Présentation 357
F.13.2 Exigences d'entrée 357
F.13.3 Exigences fonctionnelles de sécurité 358
F.13.4 Exigences d'intégrité de sécurité 359
F.14 Description fonctionnelle et modèle conceptuel 360
F.14.1 Texte rédactionnel pour l'exemple de logique du système du réacteur 361
F.15 Calculs de vérification du SIL 362
F.16 Exigences du programme d'application 372
F.17 Etape F.4: Cycle de vie de sécurité du SIS 386
F.18 Choix de la technologie et de l'appareil 386
F.18.1 Généralités 386
F.18.2 Solveur logique 386
F.18.3 Capteurs 387

F.18.4 Eléments terminaux 387
F.18.5 Electrovannes 387
F.18.6 Vannes de ventilation d'urgence 388
F.18.7 Vannes de modulation 388
F.18.8 Vannes de dérivation 388
F.18.9 Interfaces homme-machine (IHM) 389
F.18.10 Séparation 390
F.19 Défaillances de cause commune et défaillances systématiques 391
F.19.1 Généralités 391
F.19.2 Diversité 391
F.19.3 Erreurs de spécification 391
F.19.4 Erreurs de conception du matériel 391
F.19.5 Erreurs de conception du logiciel 391
F.19.6 Contraintes environnementales 392
F.19.7 Température 392
F.19.8 Humidité 392
F.19.9 Contaminants 392
F.19.10 Vibration 393
F.19.11 Mise à la terre 393
F.19.12 Conditionnement de la ligne d'alimentation 393
F.19.13 Compatibilité électromagnétique (CEM) 393
F.19.14 Sources utilitaires 394
F.19.15 Capteurs 395
F.19.16 Traitement de la corrosion ou de l'encrassement 395
F.19.17 Maintenance 395
F.19.18 Susceptibilité à la mauvaise manipulation 395
F.19.19 Architecture du SIS 395
F.20 Fonctionnalités de conception du programme d'application du SIS 397
F.21 Pratiques de câblage 397
F.22 Sécurité 398
F.23 Etape F.5: Installation, mise en service et validation du SIS 399
F.24 Installation 399
F.25 Mise en service 400
F.26 Documentation 401
F.27 Validation 401
F.28 Essais 402
F.29 Etape F.6: Fonctionnement et maintenance du SIS 417
F.30 Etape F.7: Modification du SIS 420
F.31 Etape F.8: Déclassement du SIS 420
F.32 Etape F.9: Vérification du SIS 421
F.33 Etape F.10: Gestion de la sécurité fonctionnelle et de la FSA du SIS 422
F.34 Gestion de la sécurité fonctionnelle 422
F.34.1 Généralités 422
F.34.2 Compétences du personnel 422
F.35 Evaluation de la sécurité fonctionnelle 422
Annexe G (informative) Lignes directrices relatives au développement de pratiques de programmation d'application 424
G.1 Objectif de ces lignes directrices 424
G.2 Attributs génériques de programmation sûre d'applications 424

G.3 Fiabilité 425
G.3.1 Généralités 425
G.3.2 Prévisibilité de l'utilisation de la mémoire 425
G.3.3 Prévisibilité du flux de contrôle 426
G.3.4 Comptabilité de la précision 429
G.3.5 Prévisibilité du planning 430
G.4 Prévisibilité du résultat mathématique ou logique 431
G.5 Robustesse 431
G.5.1 Généralités 431
G.5.2 Contrôle de l'utilisation de la diversité 432
G.5.3 Contrôle de l'utilisation de la gestion des exceptions 434
G.5.4 Vérification de l'entrée et de la sortie 434
G.6 Traçabilité 435
G.6.1 Généralités 435
G.6.2 Contrôle de l'utilisation des fonctions intégrées 435
G.6.3 Contrôle de l'utilisation des bibliothèques compilées 436
G.7 Maintenabilité 436
G.7.1 Généralités 436
G.7.2 Lisibilité 436
G.7.3 Abstraction des données 440
G.7.4 Cohérence fonctionnelle 441
G.7.5 Malléabilité 441
G.7.6 Portabilité 442
Bibliographie 443

Figure 1 – Cadre général de la série IEC 61511 216
Figure A.1 – Modèle en V du programme d'application 230
Figure A.2 – Indépendance d'une couche de protection BPCS et d'une source initiatrice dans le BPCS 240
Figure A.3 – Indépendance de deux couches de protection affectées au BPCS 241
Figure A.4 – Relations du système, du matériel du SIS et du programme d'application du SIS 247
Figure A.5 – Représentation des incertitudes d'un paramètre de fiabilité 270
Figure A.6 – Représentation de la limite supérieure de confiance à 70 % 271
Figure A.7 – Distribution probabiliste type des résultats cibles de la simulation de Monte-Carlo 272
Figure B.1 – Schéma de procédé de la SIF 02.01 297
Figure B.2 – Schéma de procédé de la SIF 06.02 298
Figure B.3 – Spécification fonctionnelle de la SIF 02.01 et de la SIF 06.02 299
Figure B.4 – Architecture fonctionnelle matérielle de la SIF 02.01 300
Figure B.5 – Architecture fonctionnelle matérielle de la SIF 06.02 300
Figure B.6 – Spécification matérielle pour une SOV extraite du schéma de tuyauterie et d'instrumentation 301
Figure B.7 – Architecture physique matérielle de la SIF 02.01 302
Figure B.8 – Architecture physique matérielle de la SIF 06.02 303
Figure B.9 – Structure hiérarchique d'intégration de modèle 307

Figure B.10 – Structure hiérarchique d'intégration de modèle comprenant des modèles de propriétés de sécurité et de la logique du BPCS 309
Figure B.11 – Diagramme de transition d'état 311
Figure B.12 – Diagramme de blocs type de la SOV 313
Figure B.13 – Diagramme de blocs de modèle type d'une SOV 315
Figure B.14 – Mise en œuvre du diagramme de blocs de modèle type – partie du BPCS 317
Figure B.15 – Mise en œuvre du modèle type de programme d'application de la SOV – partie du SIS 318
Figure B.16 – Modèle complet pour la vérification du modèle de mise en œuvre finale 320
Figure D.1 – Exemple de schéma de tuyauterie et d'instrumentation d'un séparateur d'huile et de gaz 324
Figure D.2 – Exemple de schéma de cause à effet d'une ESD (en partie) 326
Figure D.3 – Exemple de programme d'application (en partie) dans une programmation de blocs fonctionnels d'automate de sécurité 327
Figure F.1 – Schéma de procédé simplifié: processus pour le PVC 335
Figure F.2 – Phases de cycle de vie de sécurité du SIS et étapes de la FSA 337
Figure F.3 – Exemple de schéma de tuyauterie et d'instrumentation préliminaire pour unité de réacteur PVC 347
Figure F.4 – Schéma architectural de la SIF S-1 présentant la PFD_{avg} de chaque appareil du SIS 364
Figure F.5 – Arbre des défaillances S-1 366
Figure F.6 – Schéma architectural de la SIF S-2 présentant la PFD_{avg} de chaque appareil du SIS 367
Figure F.7 – Arbre des défaillances de la SIF S-2 369
Figure F.8 – Schéma architectural de la SIF S-3 présentant la PFD_{avg} de chaque appareil du SIS 370
Figure F.9 – Arbre des défaillances de la SIF S-3 372
Figure F.10 – Schéma de tuyauterie et d'instrumentation pour SIF d'unité de réacteur PVC 374
Figure F.11 – Légende *(1 de 5)* 377
Figure F.12 – SIS pour le réacteur VCM 397

Tableau B.1 – Modes de spécification de fonctionnement 304
Tableau B.2 – Tableau de transition d'état 310
Tableau F.1 – Vue d'ensemble du cycle de vie de sécurité du SIS 338
Tableau F.2 – Cycle de vie de sécurité du SIS – Zone 1 340
Tableau F.3 – Propriétés physiques du chlorure de vinyle 342
Tableau F.4 – Simulation/Liste de contrôle 349
Tableau F.5 – HAZOP 350
Tableau F.6 – Récapitulatif partiel de l'évaluation du danger pour le développement de stratégie SIF 351
Tableau F.7 – Cycle de vie de sécurité du SIS – Zone 2 353
Tableau F.8 – Classement du risque tolérable 355
Tableau F.9 – Exemple de réacteur VCM: Niveau d'intégrité LOPA 356
Tableau F.10 – Cycle de vie de sécurité du SIS – Zone 3 357

Tableau F.11 – Fonctions instrumentées de sécurité et SIL 357
Tableau F.12 – Relation fonctionnelle d'E/S pour la/les SIF 358
Tableau F.13 – Capteurs du SIS, plages de fonctionnement normal et points de déclenchement 358
Tableau F.14 – Schéma de cause à effet..... 361
Tableau F.15 – Chiffres MTTFd des appareils F.1 du SIS 362
Tableau F 16 – Cycle de vie de sécurité du SIS – Zone 4 386
Tableau F.17 – Cycle de vie de sécurité du SIS – Zone 5 399
Tableau F.18 – Liste des types d'instruments et des procédures d'essais utilisées 404
Tableau F.19 – Feuille de contrôle de dérivation/simulation de la procédure de vérification de verrouillage 417
Tableau F.20 – Cycle de vie de sécurité du SIS – Zone 6 417
Tableau F.21 – Journal de déclenchement du SIS 418
Tableau F.22 – Journal des défaillances de l'appareil du SIS..... 418
Tableau F.23 – Cycle de vie de sécurité du SIS – Zone 7 420
Tableau F.24 – Cycle de vie de sécurité d'un SIS – Zone 8..... 420
Tableau F.25 – Cycle de vie de sécurité du SIS – Zone 9 421
Tableau F.26 – Cycle de vie de sécurité du SIS – Zone 10 422

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

SÉCURITÉ FONCTIONNELLE – SYSTÈMES INSTRUMENTÉS DE SÉCURITÉ POUR LE SECTEUR DES INDUSTRIES DE TRANSFORMATION –

Partie 2: Lignes directrices pour l'application de l'IEC 61511-1:2016

AVANT-PROPOS

1) La Commission Electrotechnique Internationale (IEC) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de l'IEC). L'IEC a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. A cet effet, l'IEC – entre autres activités – publie des Normes internationales, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de l'IEC"). Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'IEC, participent également aux travaux. L'IEC collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
2) Les décisions ou accords officiels de l'IEC concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de l'IEC intéressés sont représentés dans chaque comité d'études.
3) Les Publications de l'IEC se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de l'IEC. Tous les efforts raisonnables sont entrepris afin que l'IEC s'assure de l'exactitude du contenu technique de ses publications; l'IEC ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.
4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de l'IEC s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de l'IEC dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de l'IEC et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
5) L'IEC elle-même ne fournit aucune attestation de conformité. Des organismes de certification indépendants fournissent des services d'évaluation de conformité et, dans certains secteurs, accèdent aux marques de conformité de l'IEC. L'IEC n'est responsable d'aucun des services effectués par les organismes de certification indépendants.
6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.
7) Aucune responsabilité ne doit être imputée à l'IEC, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de l'IEC, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de l'IEC ou de toute autre Publication de l'IEC, ou au crédit qui lui est accordé.
8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.
9) L'attention est attirée sur le fait que certains des éléments de la présente Publication de l'IEC peuvent faire l'objet de droits de brevet. L'IEC ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de brevets et de ne pas avoir signalé leur existence.

La Norme internationale IEC 61511-2 a été établie par le sous-comité 65A: Aspects systèmes, du comité d'études 65 de l'IEC: Mesure, commande et automation dans les processus industriels.

Cette deuxième édition annule et remplace la première édition parue en 2003. Cette édition constitue une révision technique. Cette édition inclut les modifications techniques majeures suivantes par rapport à l'édition précédente:

- description des exemples d'orientation, basés sur toutes les phases du cycle de vie de sécurité, réalisée avec des exemples basés sur l'expérience de l'utilisation de la norme IEC 61511 première édition;

- remplacement des annexes pour répondre à la transition de logiciel à programmation d'application.

Le texte de cette norme est issu des documents suivants:

FDIS	Rapport de vote
65A/783/FDIS	65A/787/RVD

Le rapport de vote indiqué dans le tableau ci-dessus donne toute information sur le vote ayant abouti à l'approbation de cette norme.

Cette publication a été rédigée selon les Directives ISO/IEC, Partie 2.

La présente Norme internationale doit être lue conjointement avec l'IEC 61511-1. Elle est basée sur la deuxième édition de cette norme.

Une liste de toutes les parties de la série IEC 61511, publiées sous le titre général *Sécurité fonctionnelle – Systèmes instrumentés de sécurité pour le secteur des industries de transformation*, peut être consultée sur le site web de l'IEC.

Le comité a décidé que le contenu de cette publication ne sera pas modifié avant la date de stabilité indiquée sur le site web de l'IEC sous "http://webstore.iec.ch" dans les données relatives à la publication recherchée. A cette date, la publication sera

- reconduite,
- supprimée,
- remplacée par une édition révisée, ou
- amendée.

IMPORTANT – Le logo *"colour inside"* qui se trouve sur la page de couverture de cette publication indique qu'elle contient des couleurs qui sont considérées comme utiles à une bonne compréhension de son contenu. Les utilisateurs devraient, par conséquent, imprimer cette publication en utilisant une imprimante couleur.

INTRODUCTION

Les systèmes instrumentés de sécurité (SIS, *Safety Instrumented System*) sont utilisés dans les industries de transformation depuis de nombreuses années pour remplir des fonctions instrumentées de sécurité (SIF, *Safety Instrumented Function*). Si l'instrumentation doit être effectivement utilisée pour réaliser des SIF, il est essentiel que cette instrumentation satisfasse à certaines normes minimales.

La série IEC 61511 concerne l'application des SIS aux industries de transformation. Elle traite également de l'interface entre les SIS et les autres systèmes de sécurité, et exige de procéder à une analyse de danger et de risque du processus. Le SIS comprend les capteurs, les solveurs logiques et les éléments terminaux.

La série IEC 61511 aborde deux concepts, qui sont fondamentaux vis-à-vis de son application: le cycle de vie de sécurité SIS et le niveau d'intégrité de sécurité (SIL, *Safety Integrity Level*). Le cycle de vie de sécurité SIS constitue le cadre central qui lie la plupart des concepts de cette Norme internationale.

Les solveurs logiques du SIS mentionnés dans cette norme incluent les technologies électriques (E)/électroniques (E)/et électroniques programmables (PE). Si d'autres technologies sont utilisées pour les solveurs logiques, les principes de base de la présente norme peuvent être appliqués afin de garantir que les exigences de sécurité fonctionnelle sont satisfaites. La série IEC 61511 concerne également les capteurs et les éléments terminaux des SIS, quelle que soit la technologie utilisée. La série IEC 61511 a été conçue pour être une mise en œuvre de la série IEC 61508 dans le secteur des industries de transformation. La série IEC 61511 est propre aux industries de transformation, dans le cadre de la série IEC 61508.

La série IEC 61511 définit une approche concernant les activités relatives au cycle de vie de sécurité des SIS dans le but de satisfaire à ces normes minimales. Cette approche a été adoptée afin de mettre en œuvre une politique technique cohérente et rationnelle. La présente partie de l'IEC 61511 a pour objet de fournir des lignes directrices sur la façon de satisfaire à l'IEC 61511-1:2016 .

Pour faciliter l'utilisation de l'IEC 61511-2:—, les numéros d'articles indiqués à l'Annexe A (informative) sont identiques à ceux du texte normatif correspondant de l'IEC 61511-1:2016 à l'exception de la notation "A".

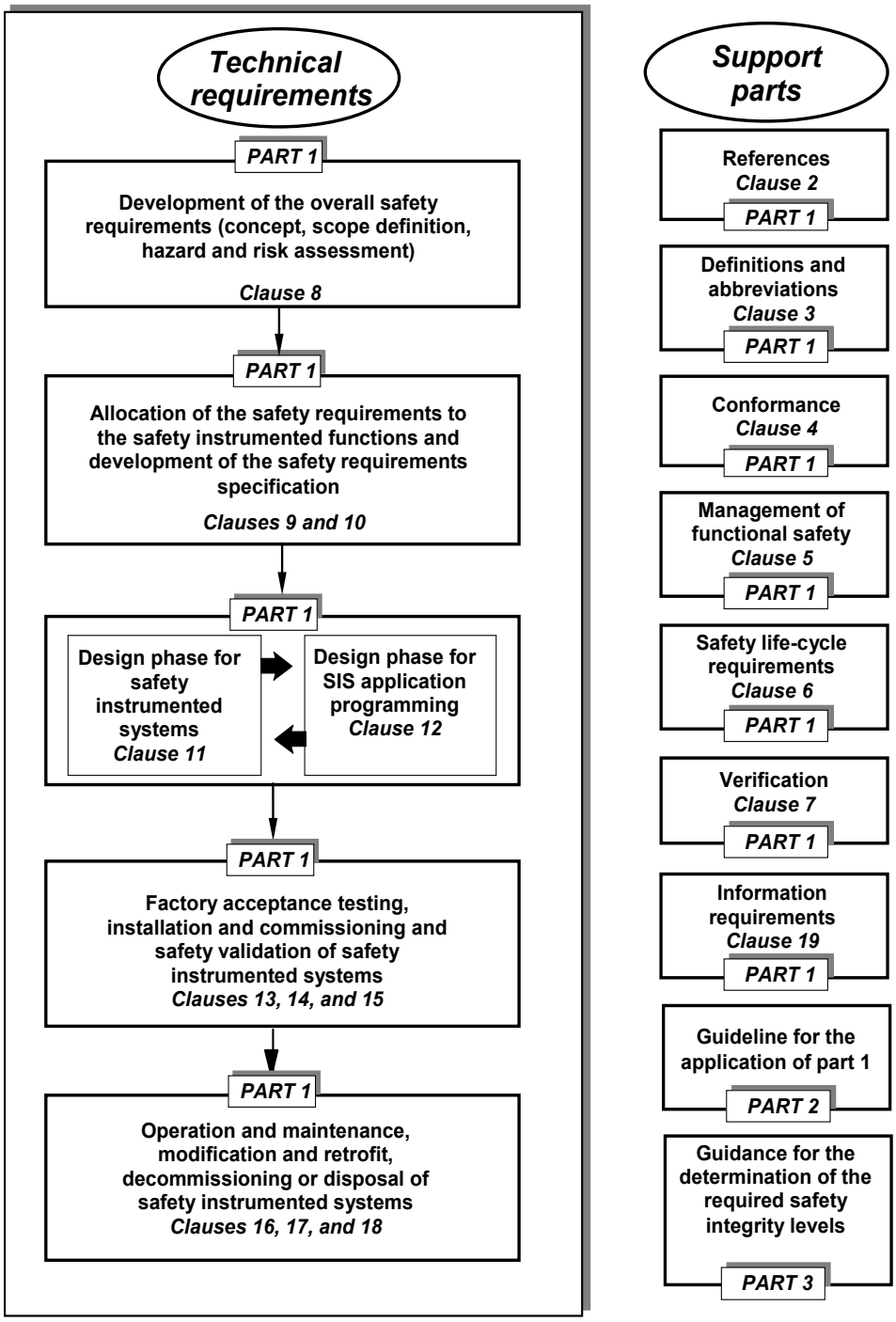
Dans la plupart des cas, la meilleure sécurité est obtenue, chaque fois que cela est possible, par des processus à conception à sécurité intrinsèque combinée, au besoin, avec un certain nombre de systèmes de protection, fondés sur différentes technologies (par exemple, chimique, mécanique, hydraulique, pneumatique, électrique, électronique, thermodynamique (par exemple, pare-feu), électronique programmable) couvrant tous les risques résiduels identifiés. Toute stratégie de sécurité prend en compte chacun des SIS individuellement, dans le contexte des autres systèmes de protection. Pour faciliter cette approche, l'IEC 61511-1:2016 :

- exige de procéder à une analyse de danger et de risque pour identifier les exigences de sécurité globales;
- exige l'allocation des exigences de sécurité aux fonctions de sécurité et aux systèmes de sécurité relatifs, par exemple aux SIS;
- s'inscrit dans un cadre applicable à toutes les méthodes instrumentées qui permettent d'obtenir la sécurité fonctionnelle;
- détaille l'utilisation de certaines activités, telles que la gestion de la sécurité, qui peuvent être applicables à toute méthode permettant d'obtenir la sécurité fonctionnelle;

- prend en compte les étapes pertinentes du cycle de vie de sécurité SIS, depuis la conceptualisation initiale, en passant par la conception, la mise en œuvre, le fonctionnement et la maintenance, jusqu'au déclassement;
- permet l'harmonisation des normes de l'industrie de transformation nationales existantes ou nouvelles par rapport à cette norme.

La série IEC 61511 vise à obtenir un haut niveau de cohérence (des principes sous-jacents, de la terminologie, de l'information, par exemple) dans le secteur des industries de transformation. Cela présenterait des avantages tant du point de vue de la sécurité que du point de vue économique.

La Figure 1 ci-dessous présente le cadre général de la série IEC 61511.



Anglais	Français
Technical requirements	Exigences techniques
PART 1	PARTIE 1
Development of the overall safety requirements (concept, scope definition, hazard and risk assessment) Clause 8	Développement des exigences de sécurité globales (concept, définition du domaine d'application, analyse de danger et de risque) Article 8

Anglais	Français
Allocation of the safety requirements to the safety instrumented functions and development of the safety requirements specification Clauses 9 and 10	Affectation des exigences de sécurité aux fonctions instrumentées de sécurité et développement de la spécification des exigences de sécurité Articles 9 et 10
Design phase for safety instrumented systems Clause 11	Phase de conception pour les systèmes instrumentés de sécurité Article 11
Design phase for SIS application programming Clause 12	Phase de conception pour la programmation d'application du SIS Article 12
Factory acceptance testing, installation and commissioning and safety validation of safety instrumented systems Clauses 13, 14, and 15	Essais de réception en usine, installation et mise en service, et validation de la sécurité des systèmes instrumentés de sécurité Articles 13, 14, et 15
Operation and maintenance, modification and retrofit, decommissioning or disposal of safety instrumented systems Clauses 16,17, and 18	Fonctionnement et maintenance, modification et remise à niveau, déclassement ou mise au rebut des systèmes instrumentés de sécurité Articles 16, 17, et 18
Support parts	Parties de prise en charge
References Clause 2	Références Article 2
Definitions and abbreviations Clause 3	Définitions et abréviations Article 3
Conformance Clause 4	Conformité Article 4
Management of functional safety Clause 5	Gestion de la sécurité fonctionnelle Article 5
Safety life-cycle requirements Clause 6	Exigences relatives au cycle de vie de sécurité Article 6
Verification Clause 7	Vérification Article 7
Information requirements Clause 19	Exigences relatives aux informations Article 19
Guideline for the application of part 1	Ligne directrice pour l'application de la partie 1
PART 2	PARTIE 2
Guidance for the determination of the required safety integrity levels	Conseils pour la détermination des niveaux exigés d'intégrité de sécurité
PART 3	PARTIE 3

Figure 1 – Cadre général de la série IEC 61511

ÉCURITÉ FONCTIONNELLE – SYSTÈMES INSTRUMENTÉS DE SÉCURITÉ POUR LE SECTEUR DES INDUSTRIES DE TRANSFORMATION –

Partie 2: Lignes directrices pour l'application de l'IEC 61511-1:2016

1 Domaine d'application

La présente partie de l'IEC 61511 donne les lignes directrices relatives à la spécification, la conception, l'installation, au fonctionnement et à la maintenance des SIF et des SIS associés, telles que définies dans l'IEC 61511-1:2016 .

NOTE 1 L'Annexe A (informative) a été organisée de sorte que tous les numéros d'articles et de paragraphes qu'elle contient correspondent à ceux de l'IEC 61511-1:2016 , sauf s'ils sont précédés de la lettre "A".

NOTE 2 L'Annexe A contient désormais les éléments précedemment présents dans le texte de la première édition. Ces changements sont exigés pour la conformité aux règles de l'IEC, lesquelles interdisent l'existence d'une norme intégralement informative.

NOTE 3 Pour assurer l'utilisation maximale de ces lignes directrices:

– passer en revue les lignes directrices de la section et celles de l'article spécifique (lors de la consultation des lignes directrices de 5.2.6.1.3, tenir compte de celles de 5.2.6, par exemple);

– lorsque les lignes directrices de l'article spécifique ne sont pas fournies (plus de lignes directrices fournies, par exemple), passer également en revue les lignes directrices de la section, tant que cela peut être applicable.

2 Références normatives

Les documents suivants sont cités en référence de manière normative, en intégralité ou en partie, dans le présent document et sont indispensables pour son application. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

IEC 61511-1:2016 , *Sécurité fonctionnelle – Systèmes instrumentés de sécurité pour le secteur des industries de transformation – Partie 1: Cadre, définitions, exigences pour le système, le matériel et la programmation d'application*