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

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

Documents
Document Sharing Hub

Full document details: IEC 61511-2 2016 RLV

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 Varembé
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00
info@iec.ch
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
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
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 It also gives information on projects, replaced and withdrawn publications.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
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
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
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
If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: csc@iec.ch.

AVA Documents
Document Sharing Hub

Full document details: IEC 61511-2 2016 RLV

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.

® Registered trademark of the International Electrotechnical Commission

Documents
Document Sharing Hub

Full document details: IEC 61511-2 2016 RLV

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

AVA Documents
Document Sharing Hub
Full document details: IEC 61511-2 2016 RLV

~~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

AVA Documents
Document Sharing Hub
Full document details: IEC 61511-2 2016 RLV

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

AVA Documents
Document Sharing Hub
Full document details: IEC 61511-2 2016 RLV

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 ... 199

AVA Documents
Document Sharing Hub
Full document details: IEC 61511-2 2016 RLV

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

Documents
Document Sharing Hub
Full document details: IEC 61511-2 2016 RLV

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

AVA Documents
Document Sharing Hub
Full document details: IEC 61511-2 2016 RLV

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

Documents
Document Sharing Hub

Full document details: IEC 61511-2 2016 RLV

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.

Documents
Document Sharing Hub

Full document details: IEC 61511-2 2016 RLV

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.

Documents
Document Sharing Hub

Full document details: IEC 61511-2 2016 RLV

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.

Documents
Document Sharing Hub
Full document details: IEC 61511-2 2016 RLV

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

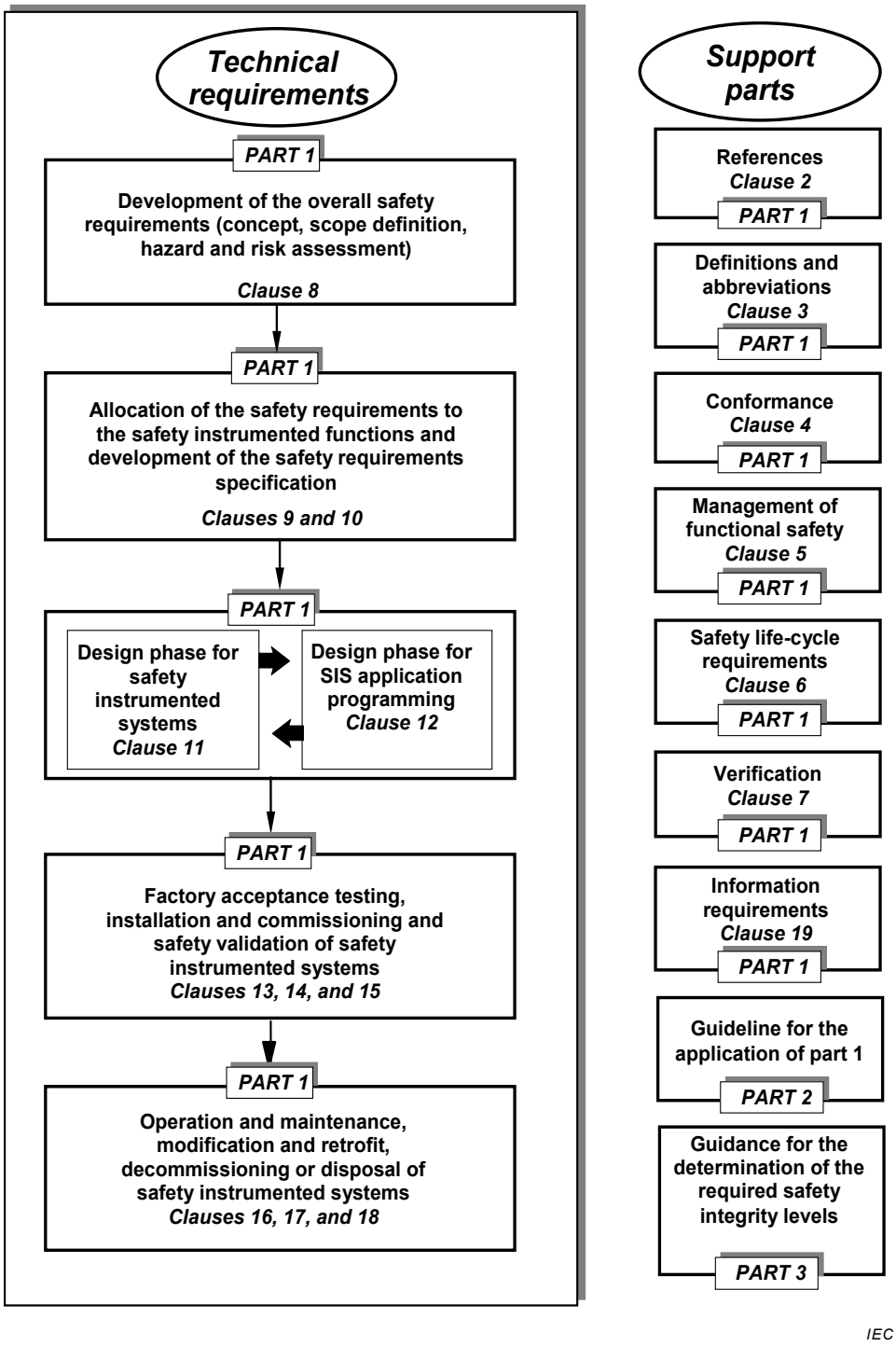


Figure 1 – Overall framework of IEC 61511 series

Documents
Document Sharing Hub
Full document details: IEC 61511-2 2016 RLV

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*

3 Terms, definitions, and abbreviations

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

Documents
Document Sharing Hub

Full document details: IEC 61511-2 2016 RLV

Annex A
(informative)

Guidance for IEC 61511-1

NOTE Clause and subclause numbers illustrated in Annex A are the same as those clause numbers in IEC 61511-1:2016 to facilitate cross-referencing.

A.1 Scope

No further guidance provided.

A.2 Normative references

No further guidance provided.

A.3 Terms, definitions and abbreviations

No further guidance provided~~ except for 3.2.68 and 3.2.71 of IEC 61511-1~~.

~~3.2.68~~ A.3.2.65
safety function
a safety function should prevent a specified hazardous event. For example, “prevent the pressure in vessel #ABC456 exceeding 100 bar.” A safety function may be achieved by:

- a single SIS, or
- one or more SIS and/or other protection layers.

Each SIS or other protection layer has to be capable of achieving the safety function and the overall combination has to achieve the required risk reduction (process safety target).

~~3.2.71~~ A.3.2.66
safety instrumented function
safety instrumented functions (SIF) are derived from the safety function, have an associated safety integrity level (SIL) and are carried out by a specific safety instrumented system (SIS). For example, “close valve #XY123 within 5 s when pressure in vessel #ABC456 reaches 100 bar”.~~ Note that components~~ Devices of a SIS may be used by more than one SIF.

A.4 Conformance to~~ this International Standard~~ the IEC 61511-1:–

No further guidance provided.

A.5 Management of functional safety

A.5.1 Objective

~~The objective of Clause 5 of IEC 61511-1 is to provide requirements for implementing the management activities that are necessary to ensure that the functional safety objectives are met.~~

No further guidance provided.

Documents
Document Sharing Hub
Full document details: IEC 61511-2 2016 RLV

A.5.2 Guidance to "Requirements"

A.5.2.1 General

~~5.2.1.1 No further guidance provided.~~

~~5.2.1.2~~ When an organization has responsibility for one or more activities necessary for functional safety and that organization works according to quality assurance procedures, then many of these activities described in Clause 5 of IEC 61511-1:2016 will already be carried out for the purposes of quality. Where this is the case, it may be unnecessary to repeat these activities for the purposes of functional safety. In such cases, the quality assurance procedures should be reviewed to establish that they are suitable so that the objectives of functional safety will be achieved.

A.5.2.2 Organization and resources

The organizational structure associated with SIS within a company/site/plant/project should be defined and the roles and responsibilities of each ~~element~~ person/department clearly understood and communicated. Within the structure, individual roles, including their description and purpose should be identified. For each role, unambiguous accountabilities should be identified; and specific responsibilities should be recognised. In addition, who makes the appointment and to whom the individual reports should be identified. The intent is to ensure that everyone in an organization understands their role and responsibilities for SIS.

The skills and knowledge required to implement ~~any~~ all of the activities of the SIS safety life-cycle relating to the SIS should be identified; and for each skill, the required competency levels should be defined. Resources should be assessed against each skill for competency and also the number of people per skill required. When differences are identified, development plans should be established to enable the required competency levels to be achieved in a timely manner. Persons should be available all through the phase they are made responsible for in order to sustain life-cycle background and experience transfer. When shortages of skills arise, suitably qualified and experienced personnel may be recruited or contracted.

A.5.2.2.1 No further guidance provided.

A.5.2.2.2 No further guidance provided.

A.5.2.2.3 No further guidance provided.

A.5.2.3 Risk evaluation and risk management

The requirement stated in 5.2.3 of IEC 61511-1:2016 is that hazards are identified, risks evaluated and the necessary risk reduction is determined. It is recognized that there are numerous different methodologies available for conducting these evaluations. IEC 61511-1:2016 does not endorse any particular methodology. ~~Instead, the reader is encouraged to review a number of methodologies on this issue in IEC 61511-3.~~ See A.8.2.1 for further guidance.

A.5.2.4 Safety planning

The intent of A.5.2.4 is to ensure that, within the overall project, adequate safety planning is conducted so that all of the required activities during each phase of the life-cycle (e.g., engineering design, plant operation) are addressed. The standard does not require any particular structure for these planning activities, but it does require periodic update or review of them.

Documents
Document Sharing Hub
Full document details: IEC 61511-2 2016 RLV

A.5.2.5 Implementing and monitoring

A.5.2.5.1 The intent of 5.2.5.1 of IEC 61511-1:2016 is to ensure that effective management procedures are in place to:

- ensure that all recommendations resulting from hazard analysis, risk assessment, other assessment and auditing activities, verification and validation activities are satisfactorily resolved;
- determine that the SIS is performing in accordance with its safety requirements specification (SRS) throughout its operational lifetime.

A.5.2.5.2 Note that, in this context, suppliers could include design contractors and maintenance contractors as well as suppliers of ~~components~~ devices. Hardware and software of SIS components should be manufactured under a recognised quality management system such as the ISO 9000 series standards.

A review of the SIS performance should be periodically undertaken to ensure that the original assumptions made during the development of the SRS are still adhered to. For example, a periodic review of the assumed failure rate of different ~~components~~ devices in a SIS should be carried out to ensure that it remains as originally defined. If the failure rates are worse than originally anticipated, a design modification may be necessary. Likewise, the demand rate on the SIS should be reviewed. If the rate is more than that which was originally assumed, then an adjustment in the SIL may be needed.

A.5.2.5.3 No further guidance provided.

A.5.2.5.4 No further guidance provided.

A.5.2.6 Assessment, auditing and revision

Assessments and audits are tools targeted at the detection and elimination of errors. The paragraphs below make clear the distinction between these activities.

Functional safety assessment (FSA) aims to evaluate whether provisions made during the assessed life-cycle phases are adequate for the achievement of safety. Judgements are made by assessors on the decisions taken by those responsible for the realisation of functional safety. An assessment would for example be made prior to commissioning as to whether procedures for maintenance are adequate.

Functional safety auditors will determine from project or plant records whether the necessary procedures have been applied at the specified frequency by persons with the necessary competence. Auditors are not required to make judgements on the adequacy of the work they are considering. However, if they became aware that there would be benefits in making changes, then an observation should be included in the report.

It should be noted that in many cases there can be an overlap between the work of the assessor and the auditor. For example either an assessor or auditor may need to determine not only whether an operator has been given the necessary training but in addition make judgements as to whether the training has resulted in the required competency.

A.5.2.6.1 Functional safety assessment (FSA)

The use of functional safety assessment (FSA) is fundamental in demonstrating that a SIS fulfils its requirements regarding SIF(s) and SIL(s), potentially using one or more application program (AP). The basic objective of this assessment is to demonstrate compliance with agreed standards and practices through independent assessment of the system's development process. An assessment of a SIS may be needed at different life-cycle stages. In order to conduct an effective assessment, a procedure should be developed that defines

AVA Documents
Document Sharing Hub
Full document details: IEC 61511-2 2016 RLV

the scope of this assessment along with some guidance on the makeup of the assessment team.

The following attributes are considered good practice for FSA:

a) A plan should be generated for each FSA identifying such arrangements as the scope of the assessment, the assessors, the competencies of the assessors and the information to be generated by the assessment.

b) The FSA should take into account other standards and practices, which may be contained within external or internal corporate standards, guides, procedures or codes of practice. The FSA plan should define what is to be assessed for the particular assessment/ system/application area.

c) The frequency of FSAs may vary across different system developments but as a minimum should always take place before the ~~potential~~ hazards being presented to the system. Some companies also like to conduct an assessment prior to the construction/installation phase to prevent costly rework later in the life-cycle.

d) FSA frequency and rigour should be defined taking into account system attributes such as:

- complexity;
- safety significance;
- previous experience of similar systems;
- standardization of design features.

e) Sufficient evidence of design, installation, verification and validation activities should be available prior to the assessment. The availability of sufficient evidence could itself be an assessment criterion. The evidence should represent the current/approved state of system design or installation:

- The independence of the assessor(s) ~~must~~ should be appropriate.
- The assessor(s) should have experience and knowledge appropriate to the technology and application area of the system being assessed.
- A systematic and consistent approach to FSA should be maintained throughout the life-cycle and across systems. FSA is a subjective activity therefore detailed guidance, possibly through the use of checklists, as to what is acceptable for an organization should be defined to remove as much subjectivity as possible.
- Inspection techniques to show that the Application Programme (AP) functions achieve the process hazard requirements.
- Functional testing to show that the AP executed the required functions and, as far as possible, that any extra functionality in either the AP or the embedded software would not result in hazardous conditions.
- Structural testing (see A.12.5.3) to show that the AP executed the required functions in the necessary timing and to identify whether there are any non-tested areas of the AP which, (as a result of not having been tested) may result in hazardous conditions.
- Functional failure analysis and “what if” analysis to show that AP functions would not result in hazardous conditions.
- Procedures are in place to show that a controlled process of development and verification is in place and both the correct AP version and the correct embedded software version are in use.
- Audit procedures and schedule have been specified.

Records generated from the FSA should be complete and the conclusions agreed with those responsible for the management of functional safety for the SIS prior to commencement of the next life-cycle phase.

The need for someone independent ~~to~~ from the project team is to increase objectivity in the assessment. The need for someone of senior stature (e.g., experience~~, grade level~~, position)

AVA Documents
Document Sharing Hub
Full document details: IEC 61511-2 2016 RLV

is to ensure their concerns are duly noted and addressed. As the note in 5.2.6.1.3 of IEC 61511-1:2016 also suggests, on some large projects or assessment teams, it may be necessary to have more than one senior person on this team that is independent to the original project team.

Depending upon the company organisation and expertise within the company, the requirement for an independent assessor may have to be met by using an external organisation. Conversely, companies that have internal organisations skilled in risk assessment and the application of SISs, which are independent to and separate (by ways of management and other resources) from those responsible for the project, may be able to use their own resources to meet the requirements for an independent organisation.

The amount of assessment depends on the size and complexity of a project. It may be possible to assess the results of different phases at the same time. This is particularly true in the case of small changes in a running plant.

In some countries, a FSA undertaken at stage 3 is often referred to as the Pre-Startup-Safety-Review (PSSR).

See Table F.1-box 10. The terms of reference for the FSA should be agreed during the safety planning.

The assessment team should have access to any information they deem necessary for them to conduct the assessment. This should include information from the H&RA, design phase through installation, commissioning and validation.

A.5.2.6.1.1 The FSA team can, in some cases, be a single person provided that the person has the required skills and experience for the activity.

A.5.2.6.1.2 The number of senior competent members on the assessment team may vary dependent on such items as the application size, technologies encompassed, communication requirements (e.g., with user/owner, integrator, manufacturer), and project timing.

The senior competent person should be competent in the various technologies that the application encompasses, applicable regulations, and available to meet project scheduling demands.

A.5.2.6.1.3 No further guidance provided.

A.5.2.6.1.4 No further guidance provided.

A.5.2.6.1.5 No further guidance provided.

A.5.2.6.1.6 The tools used in the design, development, operation and maintenance of the SIS may affect the integrity of the SIS by introducing faults into the final system. Tools may result in directly ''embedding'' part of the tool functionality into the SIS (e.g. user libraries, interpreters), or be ''off-line'' – i.e., used to generate information that can be separately checked (e.g. field variable calculation tools, test tools), or they may be tools that can be connected to an operating SIS – e.g., maintenance tools. In each case it is important to understand the potential failure modes and effects, and the means by which they are controlled. Typical approaches to controlling faults in tools include:

- confirming traceability to national and international standards (this may include calibration and/or functional standards depending on the nature of the tool);
- considering reports of user group experience and historical evidence of previous use of the tool;
- reviewing and functional testing of the output resulting from use of the tool;

Documents
Document Sharing Hub

- using diversity in the development and/or test tools – for example use of code derived from different compilers, inspection of the output of a design tool through use of a diverse type of inspection tool;
- tool is supplied as a integral part of an IEC 61508-2:2010 and IEC 61508-3:2010 device.

The FSA activity should examine the strategy that has been adopted to maintain the integrity of the output of the tools, taking into account whether they are ''embedded'' or ''off-line'' and make a judgement on whether the necessary level of tool assurance has been achieved.

A.5.2.6.1.7 No further guidance provided.

A.5.2.6.1.8 No further guidance provided.

A.5.2.6.1.9 No further guidance provided.

A.5.2.6.1.10 No further guidance provided.

A.5.2.6.2 Functional safety audit~~ing~~ and revision

~~**5.2.6.2.1** This subclause is intended to give guidance about auditing, using an example illustrating relevant activities.~~

a) Audit categories

SIS audits provide beneficial information to plant management, instrument maintenance engineers and instrument design engineers. This enables management to be proactive and aware of the degree of implementation and effectiveness of their SIS. Many types of audits, which can be carried out, exist. The actual type, scope, and frequency of the audit of any specific activity should reflect the potential impact of the activity on the safety integrity.

Types of audit activities may include:

- ~~audits, both independent and self-audit;~~
- inspections;
- safety visits (e.g., plant walk about and incident review);
- SIS surveys (via questionnaires).

A distinction ~~needs to~~ should be made between "surveillance and checking" and audit activities. Surveillance and checking focuses on evaluating the performance of specific life-cycle activities (e.g., supervisor checking completion of maintenance activity prior to the ~~component~~ device being returned to service). In contrast, audit activities are more comprehensive and focus on the overall implementation of SISs concerning the SIS safety life-cycle. An audit would include determination as to whether the surveillance and checking programme is carried out.

Audits and inspections may be carried out by a company's/site's/plant's/project's own staff (e.g., self-audit) or by independent persons (e.g., corporate auditors, quality assurance department, regulators, customers or third parties).

Management at the various levels may want to apply the relevant type of audit to gain information on the effectiveness of the implementation of their SIS. Information from audits could be used to identify the procedures that have not been properly applied, leading to improved implementation.

b) Audit strategy

Site/plant/project implementing audit programmes might consider rolling, independent or self-audit and inspection programmes.

AVA Documents
Document Sharing Hub

Full document details: IEC 61511-2 2016 RLV

Rolling programmes are updated regularly to reflect previous SIS performance and audit results, and current concerns and priorities. These cover all site/plant/project related activities and aspects of the SISs in an appropriate time period and to an appropriate depth.

The primary reason for, and the added value from audits comes from acting on the information they provide in a timely manner. The actions aim to strengthen the effectiveness of SIS, for example, to help minimize the risk of employees or members of the public being injured or killed, contribute to improving safety culture, contribute to prevent any avoidable release of substance into the environment.

In summary, the audit strategy may have a mix of audits types, driven by management (the customer), and in order to feed back the relevant information up the management chain for timely action.

c) Audit process and protocols

The overall aim is to establish the degree of compliance with IEC 61511-1 and achieve maximum value from the performance of the audit, which can only be achieved when all parties (including auditors, contact nominee, plant managers and head of departments, etc.) understand the need for and can influence each audit. The following audit process and protocols might help to ensure some consistency in the approach to achieving these aims. They bear on the following five key stages of the audit process:

1) Audit strategy and program:
   - the purpose of each audit should be clearly defined and the audit groups identified, together with the roles and responsibilities of each audit group;
   - there should be an auditing strategy;
   - there should be a program of audits;
   - there should be regular reviews of the audit process, program, and strategy implementation.
2) Audit preparation and pre-planning:
   - Prior to the commencement of an audit, the senior manager of the site/plant/project and/or the appropriate audit coordinator should identify a contact nominee.
   - The auditors and contact nominee should at an early stage discuss, understand and agree on:
     - the scope of the audit;
     - the timing of the audit;
     - the people who ~~need to~~ should be available;
     - the basis for the audit or audit standard;
     - putting the extra effort into the preparation stage and involving the plant personnel, thereby increasing the chances of a successful audit.
   - The following should be used as a guide for time to be spent at each stage:
     - audit preparation: 30 %;
     - conducting the audit: 40 %;
     - reporting of findings: 20 %;
     - audit follow-up: 10 %.
   - The auditor should prepare for the audit by gathering information, procedures/ instructions ~~etc., and~~, data and preparing checklists when appropriate.
   - The auditor should highlight and explain how the possibility of a change to the scope of the audit may occur during the audit, if serious observations/failings are discovered.
3) Conducting the audit:

AVA Documents Document Sharing Hub

Full document details: IEC 61511-2 2016 RLV

- The auditor is to conduct the audit within groups of consecutive days during the set audit period, taking due cognizance of possible disruption to site/plant/project personnel.
- The contact nominee should be periodically briefed during the audit of the findings identified, thereby avoiding surprises at the end of the audit.
- The auditor should try to involve plant personnel in the audit process in order to impart learning and understanding ~~(~~ of the process ~~and findings) to~~ so the plant personnel achieve ownership of the audit findings.
- The style of the auditor is crucial to the success of the audit – he should try to be helpful, constructive, courteous, focused and objective.
- As a minimum the auditor should try to achieve the agreed scope and timetable – variations ~~will need to~~ should be negotiated.

4) Reporting the findings:

- The auditor should hold a closing meeting either at the end of the audit or later, but before the final report is issued.
- The appropriate management should be given the opportunity to comment on the draft report and findings and discuss these at a formal close out meeting if desired.
- It is normal practice to request a plan of action from the site/plant/project to address the findings of the report.

5) Audit follow-up:

- Audit reports normally require a response in the form of an action plan. The auditor might verify satisfactory completion of the action at the due date or at the next audit, whichever is appropriate.
- Site/plant/project tracking systems may be used to check the implementation of action plans.
- A periodic review/summary of audit findings of each audit group should be considered and its results widely communicated.
- The findings/outcome from audits may be used to review the frequency of audits and are inputs to the management review of SIS.

A.5.2.6.2.1 No further guidance provided.

A.5.2.6.2.2 Functional Safety Audit can be carried out by a company's/site's/plant's/project's own staff (e.g., self-audit) or by independent persons (e.g., corporate auditors, quality assurance department, regulators, customers or third parties). See IEC 61508-1:2010, Table 4 and Table 5 for further guidance

A.5.2.6.2.3 ~~This~~ Subclauses 5.2.6.3, 5.2.6.4 and 5.2.6.5 of IEC 61511-1:2016 reinforce~~s~~ the role that management of change plays in the auditing process. If the original hazard analysis has taken credit for non-SIS safety layers which should be recorded in e.g. BPCS or operator procedures and alarms and any change to these systems should be monitored to ensure they do not reduce the protection provided by the non-SIS protection layers. In addition apparently small changes in versions or mod numbers within the SIS or the interfacing systems can introduce incompatibility between the AP, embedded software, hardware (consider for example how difficult it is to revert back to an earlier release of a software programme). It is therefore important to ensure that not only the individual items are controlled, but also that the overall configuration of items is controlled. In particular the version of AP and software must be consistent with the version of hardware and with the operating procedures and with the interfaces for which it was designed.

A.5.2.6.2.4 No further guidance provided.

Documents
Document Sharing Hub

Full document details: IEC 61511-2 2016 RLV

A.5.2.7 SIS configuration management

~~A.5.2.7.1 Requirements~~

A.5.2.7.1 To manage and maintain traceability of devices throughout the life-cycle, a mechanism to identify, control and track the model/versions of each device may be established.

At the earliest possible stage of the SIS safety life-cycle, unique plant identification should be given to each device. In some cases, earlier models/versions still in use may also be maintained and controlled. This is the first step in the configuration management program which should incorporate the following considerations.

The configuration management system may include:

a) the provision of a procedure for identification of all devices during all phases of the life-cycle;

b) the unique identification, of the model/version and build status of each device including embedded and utility software and AP, including the supplier, date and where applicable, change from the model/ version originally specified;

c) the identification and tracking of all actions and changes resulting from fault observations and audits;

d) control of the issue of a release into service, identifying the status and model/version of the associated devices;

e) safeguards that have been established to assure that unauthorized alterations/ modifications are not made to the SIS while in operation;

f) the identification of the versions of each ~~software item~~ part of the AP which together constitute a specific version of a complete ~~device~~ AP;

g) the provision of co-ordination for the updating of multiple SISs in one or more plants;

h) documented authorization of release into service;

i) an authorized list of signatures for device release into service;

j) the stage/phase devices are brought under configuration control;

k) control of the associated deliverable documentation;

l) identification of the each model/version of a device;

   – functional specification;

   – technical specification;

m) a link to the management of change procedure.

All departments/organizations involved in the management and maintenance of SISs ~~are~~ should be identified and responsibilities assigned and understood.

In principle, the requirements for AP configuration management are the same as those relating to hardware devices of the system. However, AP often merits a more rigorous approach than might be necessary for hardware alone because:

- the inherent ‘logical’ rather than ‘physical’ nature of the AP is such that its actual configuration is difficult to ‘observe’ except through reference to its supporting documents;
- it is easy to modify (it is not unusual for a programmer to be able to release several different versions within a single day);
- the functionality of the application is entirely dependent on the correct functioning of the AP and its correctness is therefore a key to the overall SIS correct operation;
- it may perform differently with different versions of the PE system, with changes in the interfaces to the external world, with different input and output data ranges, and even with different versions of its own development tools;

AVA Documents
Document Sharing Hub

- it may be specific to a particular specification set, build configuration, SIS subsystem, environment and location, yet cannot be differentiated except by its configuration management version and revision.

In addition to the standard configuration management requirements for identification, version and revision control and compatibility between items, typical aspects that should be used to maintain control over the AP include:

- use of embedded codes within the AP to ensure it can only be downloaded into its intended hardware host (useful particularly where multiple different configurations might be used at different sites);
- use of release notes requiring authorization by named authority or authorities before new versions of the program can be loaded into the SIS;
- maintaining records of the status and version of all items used in the development, test and maintenance of the AP traceable to the relevant specifications and verification results associated with the complete configuration;
- maintaining back-ups such that a system can revert to a previous build;
- use of controlled modification cycles, whereby changes will be organized into defined releases, this has the advantage that a number of different releases can be under development at different stages of maturity without interaction between the different releases, also allowing the test cycle to bring a level of stability to a particular release before it is released to site.

A.5.2.7.2 No further guidance provided.

A.6 Safety life-cycle requirements

A.6.1 Objectives

The functional safety achieved in any process facility is dependent on a number of activities being carried out in a satisfactory manner. The purpose of adopting a systematic SIS safety life-cycle approach towards a SIS is to ensure that all the activities necessary to achieve functional safety are carried out and that it can be demonstrated to others that they have been carried out in an appropriate order. IEC 61511-1:2016 sets out a typical life-cycle in its Figure 7 and Table 2. Requirements for each life-cycle phase are given in Clauses 8 through 18 of IEC 61511-1:2016.

The standard recognizes that the specified activities might be structured in different ways, provided that all the requirements are complied with. This restructuring can be beneficial if it allows safety activities to be better integrated into normal project procedures. The purpose of Clause 6 of IEC 61511-1:2016 is to ensure that if a different SIS safety life-cycle is used, the inputs and output of each phase of the life-cycle are defined and all essential requirements are incorporated.

A.6.2 Guidance to "Requirements"

A.6.2.1 The key consideration is to define in advance the SIS safety life-cycle of the SIS that is going to be used. Experience has shown that problems are likely to occur, unless this activity is planned well in advance and agreements are reached with all persons, departments and organizations taking responsibility. At best, some work will be delayed or have to be redone; at worst, safety can be compromised.

The responsibility hierarchy within each of the life cycle phases should be identified and communicated to the involved parties (e.g., sub-suppliers, system integrators, end users), making all aware of their responsibilities, how their activities are related to each other and the safety life cycle phases, and how their deliveries contribute to the overall functional safety and safety integrity requirements.

AVA Documents
Document Sharing Hub

Full document details: IEC 61511-2 2016 RLV

A.6.2.2 Although it is not a requirement, it is generally beneficial at an early stage to map the proposed safety life-cycle of the SIS onto the project life-cycle of the process including which of the boxes in IEC 61511-1:2016, Figure 7 apply to the project. When doing this, the information needed to begin a SIS safety life-cycle activity should be considered together with who is likely to be able to provide it so that safety life cycle responsibilities can be assigned to specific personnel. In some cases it may not be possible to determine accurate information on a particular issue until late in the design phase. In such cases, it may be necessary to make an estimate based on previous experience and then confirm the data at a later date. Where this is the case, it is important to note this on the SIS safety life-cycle.

A.6.2.3 Another important part of SIS safety life-cycle planning is to identify the techniques that will be used during each phase. The identification of such techniques is important since it is often necessary to use a specific technique that requires persons or departments with unique skills and experience. For instance, consequences in a particular application may be dependent on the maximum pressure developed after a failure event; and the only way this can be determined is to develop a dynamic model of the process. The information requirements for dynamic modelling will then have an important impact on the design process.

A.6.2.4 Since the detailed design, verification, validation, and test evidence was developed from other safety life cycle phases, it is important to confirm, after any change, that every phase of the safety life cycle remains consistent, that no new hazards have been introduced, and that the application still performs as required.

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

A.6.3.1 The SIS safety life-cycle of the AP starts in phase 3 of the SIS safety life-cycle (“SIS SRS”) and ends with stage 3 FSA.

Provided that the AP safety life-cycle satisfies the requirements of IEC 61511-1:2016,Table 3, it is acceptable to tailor the depth, number and size of the phases of the V-model (see Figure A.1) to take into account the safety integrity and the complexity of the project.

The type of AP language used and the closeness of the language to the application functions may impact the scope of the V-model phases. For example, when LVLs such as IEC 61131-3:2013 ladder diagram or function block diagram are used for the design, implementation, verification and validation of AP then only two levels of the standard AP “V” model may apply:

- “application module development” in the “V” model is interpreted as the design and implementation of the new function; and
- “application module testing” is interpreted as the verification and testing of the new function.

In the case where a new function is to be written in a FVL and therefore a more detailed AP (i.e., software code) development process is needed, then the developer should follow all of the life-cycle phases and procedures defined in IEC 61508-3:2010. The AP SRS may be included as part of the SIS SRS.

A.6.3.2 The selection of methods and techniques should depend upon the specific circumstances. The factors in this decision are likely to include:

- size of the AP;
- degree of complexity;
- SIL of the SIF to be implemented;
- degree of standardization of design tools (e.g. configuration tool);
- type of application language (e.g., function block in Annex B; cause and effect chart in Figure D.2 and Table F.14; relay ladder in Figure F.11).

Documents
Document Sharing Hub

Full document details: IEC 61511-2 2016 RLV

See examples of techniques and measures in A.12.6.2.

A.6.3.3 No further guidance provided.

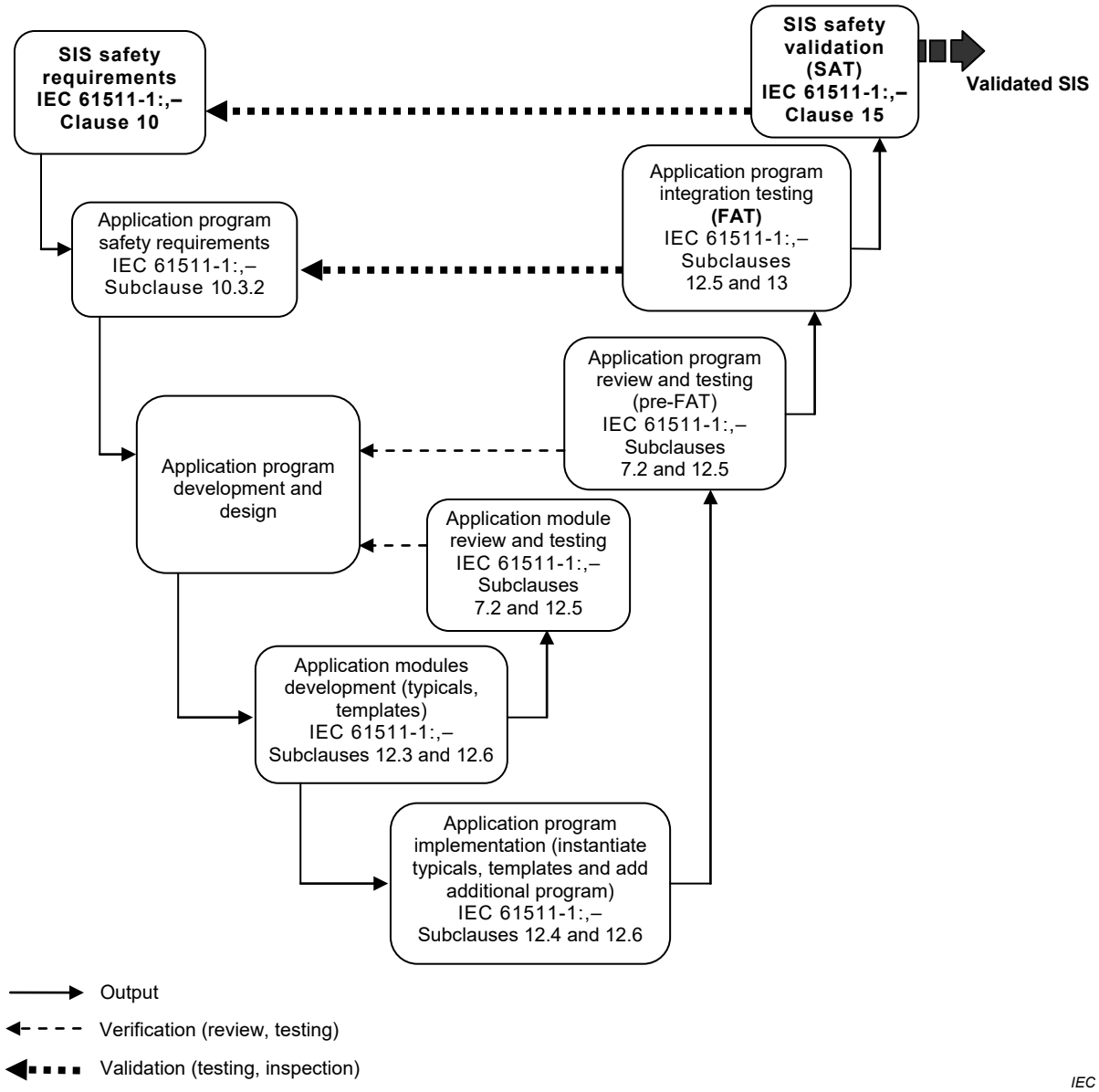


Figure A.1 – Application program V-Model

A.7 Verification

A.7.1 Objective

The purpose of verification is to ensure that the activities for each SIS safety life-cycle phase, as determined by verification planning, have, in fact, been carried out and that the required outputs of the phase, whether they be in the form of documentation, hardware or ~~software~~ AP, have been produced and are suitable for their purposes as phase deliverables.

A.7.2 Guidance to "Requirements"

A.7.2.1 IEC 61511-1:2016 recognizes that organizations will have their own procedures for verification and do not always require them to be carried out in the same way. Instead the

Documents
Document Sharing Hub
Full document details: IEC 61511-2 2016 RLV

intent of IEC 61511-1:2016 Clause 7 is that all verification activities are planned in advance, along with any procedures, measures and techniques that are to be used.

A.7.2.2 In order to reveal and remove faults that already exist in the AP, verification is required throughout the development life-cycle. In general, in order to ensure testability, it is recommended that the AP integration test specifications are considered during the design and development phase. The scope of the tests may take into account previous testing carried out.

At each distinct phase of the AP development cycle (including testing), verification should confirm that the phase has been successfully completed. Verification is, in general, completed by a verification that consists of one or more persons, as application needs dictate.

To reduce errors due to preconceived mind-sets, verification should be carried out by a qualified person, who is a peer not involved in the production of the application code and, for SIL 3 applications, by a person with an independent reporting route.

Where the AP development tools include some automatic verification operations (e.g., checking for double use of tags (named variables)) then the verification team should confirm that the tools have been properly used and the correct results obtained.

For all SILs, it is recommended that the test coverage encompasses all AP SIF and SIS failure responses (e.g., power supply failures, processor failure, input hardware failure, output hardware failure and communication failures). However to further reduce any errors remaining in the AP, it is recommended that the following additional testing is carried out:

- testing based on the internal structure (e.g., internal algorithms, internal states); and
- "stress testing" (e.g., abnormal range conditions of input variables and internal variables, abnormal combinations of inputs, abnormal sequences and loading).

For all SILs it is recommended that the verification and test documentation display that the verification and tests have been carried out and were successful. It is also recommended that:

- the documentation allows an assessment of the adequacy of the verification and testing; and
- the documentation allows an independent person to repeat the tests and review the coverage achieved.

Data verification includes confirmation that data used within the AP is correct and, where appropriate, unique (e.g., that tag names are uniquely assigned, that data is not misused by subsequent functions and that constants such as alarm set points are valid and correct).

Verification for protection against unauthorised change would include verification that the mechanisms exist (e.g., password protection with levels of access) and that these mechanisms have been adequately utilised.

A process system may have one or more embedded systems that comply to different standards (e.g. IEC 62061:2005 for machinery, NFPA 85:2015 for burners). Careful integration of hardware, AP and embedded software is required. One way to achieve this is to treat the non-process systems (i.e., systems that must comply with other standards (such as machinery, burner, etc.) as process equipment H&RA to ensure all possible hazards are identified and any identified additional protection provided.

A.7.2.3 No further guidance provided.

A.7.2.4 No further guidance provided.

Documents
Document Sharing Hub

Full document details: IEC 61511-2 2016 RLV

A.7.2.5 Once the AP reaches the verification and testing life-cycle phases, any modification or change to the AP could invalidate the evidence developed at a previous phase. One approach might be to repeat the entire life-cycle from the start, but this is expensive, introduces program delays and – in almost every case – would involve much unnecessary work. Instead an impact analysis should identify the areas that could have been impacted, and aim to focus effort into ensuring that those areas are revalidated.

A.7.2.6 It is important that the results of verification are available so that it can be demonstrated that effective verification has taken place at all phases of the SIS safety life-cycle.

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

A.8.1 Objectives

The overall objective is to establish the need for safety functions ~~(for example, protection layers) together with~~ and associated ~~levels of performance (risk reduction) that are needed~~ target failure measures to ensure a safe process. The safety functions are allocated to protection layers in accordance with Clause 9 of IEC 61511-1:2016. It is normal in the process sector to have multiple ~~safety~~ protection layers so that failure of a single layer will not lead to or allow a harmful consequence. Typical ~~safety~~ protection layers are represented in Figure 9 of IEC 61511-1:2016.

A.8.2 Guidance to "Requirements"

A.8.2.1 The requirements for H&RA are specified only in terms of the results ~~of the task~~. This means that an organization may use any technique that it considers to be effective, provided it results in a clear description of safety functions and associated ~~levels of performance~~ target failure measures.

A H&RA should identify and address the ~~hazards and~~ hazardous events that could occur under all reasonably foreseeable circumstances (including fault conditions and reasonably foreseeable misuse). Consideration should be given to past incidents, including the causes, system failures, and lessons learned to prevent reoccurrence.

On a typical project in the process sector, a preliminary H&RA ~~needs to~~ should be carried out early during the basic process design. An assumption at this stage is that hazards have been eliminated or reduced as far as is reasonably practicable, by the application of inherent safety principles and the application of good engineering practice (this activity of hazard reduction is not within the scope of IEC 61511). For the SIS, this preliminary H&RA is important because establishing, designing and implementing a SIS are complex tasks and can take a considerable length of time. Another reason for undertaking this work early is that information on system architecture will be needed before the process and instrumentation diagrams are finalized.

There will usually be sufficient information enabling preliminary H&RA to proceed once a process flow diagram has been completed and all of the initial process data are available. It should be recognised that additional ~~hazards~~ hazardous events may be introduced as detailed design proceeds. A final H&RA may therefore be necessary once the ~~process~~ piping and instrumentation diagrams have been finalized. This final analysis generally uses a formal and fully documented procedure such as hazard and operability study (HAZOP – see IEC 61882:2003). It should confirm that the ~~safety~~ protection layers as designed are adequate to ~~ensure~~ manage the ~~safety~~ risks of the plant. During this final analysis it is necessary to consider whether failures ~~in~~ of the ~~safety systems~~ protection layers (or successful activations of protection layers) introduce any new ~~hazards~~ hazardous events or demands. If any new ~~hazards~~ hazardous events are established at this stage, it may be necessary to define new safety functions. Another more likely outcome is that additional ~~events~~ causes are identified that lead to ~~the hazards~~ hazardous events that were already identified at the preliminary stage. It will then be necessary to consider if any revision of the safety functions and

AVA Documents
Document Sharing Hub
Full document details: IEC 61511-2 2016 RLV

~~performance~~ target failure measure requirements that were determined in the original analysis is needed.

The approach used to identify ~~hazards~~ hazardous events will depend on the application being considered. For certain simple processes where there is extensive operating experience of a standard design, such as simple off-shore wellhead towers, it may be sufficient to use industry developed check lists (e.g., the safety analysis checklists in ISO 10418:2003 and API RP 14C:2001). Where the design is more complex or a new process is being considered, a more ~~structured~~ rigorous approach may be necessary (e.g., ~~IEC 60300-3-9:1995~~ ISO 31000:2009).

NOTE Further information on selection of appropriate techniques is given in ISO 17776:2000, ''Petroleum and natural gas industries – Offshore production installations – Guidelines on tools and techniques for hazard identification and risk assessment''.

When considering the consequences of a particular ~~failure~~ hazardous event, all possible outcomes, and the frequency of the ~~failure~~ hazardous event as it contributes to each outcome, should be ~~analysed~~ considered. No credible outcome should be ignored or discarded ~~from a risk analysis~~. For example, exposing piping or vessels to pressures above design will not always result in catastrophic loss of containment. In many cases, equipment will have been subjected to test pressure greater than design and the only consequence may be leakage of flammable substances leading to the possibility of fire. In evaluating consequences, persons responsible for the mechanical integrity of the plant ~~will need to~~ should be consulted. They ~~will need to~~ should take into account the original test pressure but also whether the original design included corrosion allowances and whether a corrosion management programme is in place. Where consequences are based on such assumptions, it is important that this is clearly stated so that relevant procedures can be incorporated into the safety management system.

A further issue when considering consequences will be the number of persons likely to be affected by a particular hazard. In many cases, operational and maintenance staff will only be present in the hazardous zone on an infrequent basis and this ~~should~~ can be taken into account when predicting consequences. Care is needed when using this statistical approach since it will not be valid in all cases, such as where the ~~hazard only~~ hazardous event may occur~~s~~ during start-up ~~and~~ when staff are ~~always~~ frequently present. Also considerations should be given to the potential increased number of people being in the vicinity of the hazardous event as a result of investigating the symptoms during the build-up to the event.

~~When assessing the potential sources of demand on the SIS, the assessment should include the following situations: start-up, continuous operation, shutdown, maintenance errors, manual interventions (for example, controllers on manual) loss of services (for example, air, cooling water, nitrogen, power, steam, trace heating, etc.).~~

Intended process operating modes should be assessed, such as start-up, continuous operation, shutdown, maintenance, and cleaning cycles. Reasonably foreseeable sources of demand on the SIS should be considered e.g., equipment failures, control system, other protective layers, maintenance errors, manual interventions (e.g., BPCS control function in manual) and loss of utilities (e.g., air, cooling water, nitrogen, power, steam, trace heating, etc.) during each of the intended process operating modes.

When considering the frequency of demands, it may be necessary in some complex cases to undertake a fault tree analysis. This is often necessary where severe consequences only result from simultaneous (or sequential hidden) failure of more than one event (e.g., where relief headers are not designed for worst case relief from all sources). Judgement ~~will need to~~ should be made on when operator errors are to be included ~~in the list of events that can cause the hazard~~ as initiating causes of the identified hazardous events and the frequency to be used for such events. ~~Operator error could often be excluded if the action is subject to permit procedures or lock-off facilities are provided to prevent inadvertent action.~~ Care is also needed where credit is taken for reduction in demand frequency due to operator action. The credit ~~that can be taken will need to be~~ is limited by human factor issues such as how quickly action ~~needs to~~ can be taken and the complexity of the tasks involved. ~~Where an operator, as a result of an alarm, takes action and the risk reduction claimed is greater than a factor of 10,~~

AVA Documents Document Sharing Hub

~~then the overall system will need to be designed according to IEC 61511-1.~~ Human reliability analysis should be performed when credit >10 is claimed for an operator action. Where risk reduction >10 is claimed, the system should be designed according to IEC 61511-1:2016. The system that undertakes the safety function would then comprise the sensor detecting the hazardous condition, the alarm presentation, the human response and the equipment used by the operator to terminate any ~~hazard~~ abnormal situation. It should be noted that a risk reduction of ~~up to a factor of~~ ≤10 might be claimed without the need to comply with IEC 61511. Where such claims are made, the human factor issues ~~will need to~~ should be carefully considered. Any claims for risk reduction from an alarm layer of protection should be supported by a documented description of the necessary response for the alarm and justification that there is sufficient time for the operator to take the corrective action and assurance that the operator will be trained (initially and recurring) to take the preventive actions.

An alarm system can be used as a ~~method~~ means of risk reduction by reducing the demand rate on the SIS ~~providing~~, or as a separate protection layer safety function reducing the overall risk of the scenario. Design of the alarm system should consider:

- the sensor used for the alarm system ~~is not used for control purposes where loss of control would lead to a demand on the SIF~~ and the final elements used to take action on the process are not used for control functions where loss of control would lead to a demand on the alarm system, unless an analysis has been performed indicating the overall risk is acceptable. Common cause and common mode issues should be addressed;
- the sensor used for the alarm system ~~is not used as part of the SIS~~ and the final elements used to take action on the process are not claimed for risk reduction as part of the SIS for the same hazardous event unless the common cause failure has been taken into account during the risk reduction analysis;
- limitations have been taken into account with respect to risk reduction that can be claimed for the ~~BPCS and common cause issues~~ alarm system design and management, such as provisions for access security, management of change and inspection, preventive maintenance and testing.

Examples of techniques that can be used to establish the SIL of SISs are given in IEC 61511-3: — which also contains guidance on what to consider when selecting the method to use for a specific application.

When establishing whether risk reduction is required it is necessary to have some process safety and environmental targets. These may be specific to the particular site or operating company and will be compared with the level of risk without additional safety functions. After establishing the need for risk reduction, it will be necessary to consider what functions are required to be carried out to return the process to a safe state. In theory, the functions may be described in general terms without a reference to a particular technology. In the case of over-pressure protection for instance, the function may be described as prevention of pressure rise above a specified value. Either a relief valve or a SIS could then carry out this function. If the function is described as above, the selection of the type of technology to use would be decided in the next life-cycle step (allocation of SIF to protection layers). In practice, the functional requirements would be different depending on the type of system selected; and this stage, and the next, may in some cases be combined.

In summary, the H&RA should consider the following:

a) each determined hazardous event and the event sequences that contribute to it;

b) the consequences and likelihood of the event sequences with which each hazardous event is associated; these may be expressed quantitatively or qualitatively;

c) no further guidance provided;

d) the necessary risk reduction for each hazardous event;

e) the measures taken to reduce or remove hazards and risks;

Documents
Document Sharing Hub

Full document details: IEC 61511-2 2016 RLV

f) the assumptions made during the analysis of the risks, including the estimated demand rates and equipment failure rates; any credit taken for operational constraints or human intervention should be detailed;

g) no further guidance provided;

h) references to key information which relates to the safety-related systems at each SIS life-cycle phase (e.g. verification and validation activities).

The information and results which constitute the H&RA should be documented.

It may be necessary for the H&RA to be repeated at different stages in the overall SIS safety life-cycle, as decisions are taken and available information becomes more refined. Periodic revalidations of the H&RA should also be conducted and documented to ensure that assumptions match actual operational experience (see 5.2.5.3 of IEC 61511-1:2016) and current functional safety management plan (see 5.2.5.1 of IEC 61511-1:2016).

A.8.2.2 The BPCS includes all of the devices necessary to operate the process and its associated equipment in the desired manner (see IEC 61511-1:2016, 3.2.3). BPCS devices are generally not qualified in accordance with IEC 61511-1:2016 (see IEC 61511-1:201611.2.4), so the dangerous failure rate cannot be assumed to be $< 10^{-5}$ per hour.

~~In the process industry, an important cause of demands that will need to be considered in many applications is the BPCS failure. It should be noted that Failure of the BPCS may be caused by the sensor, valve or control system.~~

~~Sometimes, control systems used in the process industry have redundant processors but sensors and valves are usually non-redundant. When assigning a failure rate to the BPCS, there is an important limitation that needs to be recognised. IEC 61511-1 limits the dangerous failure rate, in relation to a particular hazard, that can be claimed to 10^{-5} per hour unless the system is implemented according to the requirements of this standard. The reason for the limit is that if a lower dangerous failure rate is claimed, it would be in the range of failure rates within Table 4 of IEC 61511-1. The limit ensures that high levels of confidence are not placed on systems that do not meet the requirements of IEC 61511-1.~~

In the process industry, BPCS failure is an important cause of demands that should be considered in the H&RA. Failure of the BPCS may be caused by anything responsible for correct BPCS operation, such as the sensor, valve, operator error, or logic solver.

IEC 61511-1:2016 limits the dangerous failure rate for the BPCS as an initiating source to 10^{-5} per hour unless the BPCS is implemented according to the requirements of this standard. The reason for the limit is that the functional safety management system of IEC 61511-1:2016 and its prescribed measures and techniques are necessary to lower the likelihood of systematic failures to a sufficiently low level to support a dangerous failure rate claim $< 10^{-5}$ per hour. The limit ensures that high levels of confidence are not placed on a BPCS that does not meet the requirements of IEC 61511-1:2016.

A.8.2.3 No further guidance provided.

A.8.2.4 For further guidance see ISA TR84.00.09:2013.

A.9 Allocation of safety functions to protection layers

A.9.1 Objective

In order to determine the need for a ~~SIS~~ SIF and specify its associated ~~SIL~~ safety integrity requirements, it is important to consider ~~what other~~ the planned (or installed) protection layers ~~exist (or need to exist)~~ and how much ~~protection~~ risk reduction they provide. ~~After considering the other protection layers, a determination should then be made on the need for a SIS~~

AVA Documents
Document Sharing Hub
Full document details: IEC 61511-2 2016 RLV

~~protection layer.~~ If a SIS protection layer is needed, a determination should ~~then~~ be made on the SILs ~~for the~~ of each SIF ~~of this~~ allocated to the SIS.

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

A.9.2.1 The requirement is to ~~agree on~~ identify the ~~safety~~ protection layers to be used and to allocate ~~performance targets for~~ risk reduction to the SIF. In practice, safety functions are ~~in many cases~~ only allocated to SISs where there are problems in using inherently safe designs or other technology systems.

Examples of such problems include limitations on flare capacity or protection against exothermic reactions. Any decision to use ~~instrument based~~ instrumented systems rather than more traditional approaches such as relief valves ~~will need to~~ should be supported by sound reasons that will stand up to regulatory authority challenge.

As stated above, the H&RA and allocation may be concurrent activities or allocation may in some circumstances take place prior to H&RA. Decisions on the allocation of safety functions to ~~safety~~ protection layers are often taken on the basis of what has been found to be practicable by the user organization. Established industry good practice should also be taken into account. Decisions will then be taken on the SISs, assuming credit for the other ~~safety~~ protection layers. For example, where relief valves have been installed and these have been designed and installed according to industry codes, it may then be decided that these are adequate on their own to achieve adequate risk reduction. SISs would then only limit pressure where size or performance of the relief valve(s) was insufficient for the application or release to the atmosphere is to be prevented.

A.9.2.2 No further guidance provided.

A.9.2.3 When a safety function is allocated to a SIS, it will be necessary to consider whether the application is ~~in~~ low demand mode or ~~in~~ high demand/continuous mode. ~~The majority of applications~~ In the process sector safety functions often operate in low demand mode where demands are normally infrequent. In such cases, Table 4 in IEC 61511-1:2016 is the appropriate measure to use. There are ~~some~~ an increasing number of applications operating in high demand mode where ~~demands are frequent (for example, greater than one per year) and~~ it is more appropriate to consider the application as continuous mode because the ~~probability of dangerous failure will be primarily determined by the failure rate of the SIS~~ hazardous event typically occurs as soon as the SIS fails to function. In such cases, Table 5 in IEC 61511-1:2016 is the appropriate measure to apply. Continuous mode applications where failure would result in an immediate hazard are rare. Burner or turbine speed control functions may be specified as continuous mode applications ~~if protection systems are insufficient for all failure modes of the control system~~ that are required to comply with IEC 61511-1:2016 if the required average frequency of failure to achieve the specified hazardous event frequency is lower than 10–5 per hour.

Table 4 of IEC 61511-1:2016 defines SIL in terms of PFD_{avg}. The target PFD_{avg} ~~will be~~ is determined by the required risk reduction. The required risk reduction can be determined by comparing the process risk without the SIS with the tolerable risk. This can be determined on a quantitative or qualitative basis using the techniques in IEC 61511-3:—.

Table 5 of IEC 61511-1:2016 defines SIL in terms of the ~~target~~ average frequency of dangerous failures to perform the SIF. This ~~will be~~ is determined by the tolerable failure rate of the SIS, taking into account the consequence of failure in a particular application. When Table 5 of IEC 61511-1:2016 is used to determine the required SIL, the target is based on the frequency of dangerous failure for the SIS. In using Table 5 of IEC 61511-1:2016, it is incorrect to convert the frequency of dangerous failure into a probability of dangerous failure on demand using the proof test interval or the demand rate. While the units may appear to be correct, this results in an inappropriate conversion of Table 5 of IEC 61511-1:2016 and may result in under-specification of the ~~safety function~~ SIL requirements.

AVA Documents
Document Sharing Hub
Full document details: IEC 61511-2 2016 RLV

The targets for average probability of failure on demand or frequency of dangerous failures ~~per hour~~ apply to the SIF, not to individual components, devices or SIS subsystems. A component, device or SIS subsystem (e.g., sensor, logic solver, final element) cannot have a SIL assigned to it outside its ~~use in~~ association with a specific SIF. However, ~~it can have an independent maximum SIL capability claim~~ a component can have a systematic capability that relates to the measures and techniques used to reduce the likelihood of systematic errors causing a dangerous failure of the SIS.

The outcome of the H&RA and allocation process should be a clear description of the safety functions to be carried out by the ~~safety systems, including potential safety instrumented systems together with safety integrity level requirements (along with mode of operation, continuous or demand) for any safety instrumented function~~ protection layers. For the SISs, this description should include the mode of operation, i.e., continuous, low or high demand, and SIL requirements for each SIF. This forms the basis for the SIS's SRS. The description of the safety functions should be clear as to what ~~needs to~~ should be done to ensure that ~~safety is maintained~~ the functional and safety integrity requirements are understood.

At this stage of the implementation, it is unnecessary to specify architectural details for sensors and valves. Decisions on architectures are complex and whether a particular system requires 2oo3 sensors and 1oo2 valves will depend on many factors.

A.9.2.4 The implications of Tables 4 and 5 of IEC 61511-1:2016 ~~need to~~ should be fully understood. In particular, the PFD_{avg} that can be claimed for a single SIF is limited to 10^{-5}, corresponding to a risk reduction of 10^5 (SIL 4). Reliability analysis may indicate that it is possible to achieve a PFD_{avg} due to random hardware failures of less than 10^{-5}, but IEC 61511-1:2016 presumes that systematic failures and common mode failures will limit the actual ~~performance~~ risk reduction that can be achieved. It is strongly recommended that where risk analysis shows such a high risk reduction to be necessary, the difficulty of achieving a SIL 4 SIF in the process sector should be noted. Consideration should be given to removal or reduction of the hazard at source, introducing risk reduction measures not based on SISs, reducing the likelihood of causes of the hazardous event or using multiple independent SIFs, of lower safety integrity. Where multiple SIFs are used the dependencies between the SIFs should be considered including the effects of synchronised proof testing. One method of considering the effect is to model the overall arrangement using a holistic approach (see IEC 61511-3:—, Annex J).

~~With reference to Note 4:~~

A.9.2.5 No further guidance provided.

A.9.2.6 Multiple ~~SISs~~ SIFs may be utilized in order to achieve higher levels of risk reduction (e.g., greater than 10^3). When using multiple ~~SISs~~ SIFs to achieve higher risk reduction, it is important that each of the ~~SISs~~ SIFs is independently able to carry out the safety function and that there is sufficient independence between the SISs. ~~For example, it might not be advisable to combine a SIL 2 pressure sensing loop with a SIL 1 level sensing loop to achieve an over pressure safety function having a risk reduction requirement of 10^3 because by the time the level sensor detected a high level, the vessel might have already exceeded its pressure constraints.~~

Furthermore, where multiple ~~SISs~~ SIFs are used, one should take into account common cause failures. In addition, all of the other requirements defined in IEC 61511-1:2016 should be satisfied, including the minimum fault tolerance requirements defined in Table 6 of IEC 61511-1:2016.

To illustrate how combining multiple ~~SISs~~ SIFs might be used to achieve higher levels of risk reduction, consider the following example:

A 2oo3 transmitter set, a 2oo3 logic solver and a 1oo2 final element set which yields a ~~SIS~~ SIF with a PFD_{avg} of $3{,}05 \times 10^{-4}$. This ~~SIS~~ SIF achieves a risk reduction of approx. $3{,}9 \times 10^3$.

AVA Documents
Document Sharing Hub
Full document details: IEC 61511-2 2016 RLV

It would be incorrect to assume that using two such systems together would result in a risk reduction of 10×10^6 (i.e., $3{,}3 \times 10^3 \times 3{,}3 \times 10^3$). Common cause factors, such as using similar technologies, designing both systems from the same functional specification, human factors (e.g., programming, installation, maintenance), external factors (e.g., corrosion, plugging, freezing of air lines, lightning) and dependencies due to synchronised proof testing will limit the system improvement. It ~~would~~ is also ~~be~~ necessary to take into account any components shared between the two systems.

A more feasible solution may be to utilize a non-redundant second system using ~~components~~ devices as diverse as possible (in order to minimize potential common cause problems). Using diverse components may, however, make the maintenance more difficult. A thorough analysis should be undertaken to select the best solution for the individual application.

~~For example consider a SIS comprising a single switch, relay logic and a single final element which yields a system with a PFD_{avg} of $7{,}7 \times 10^{-3}$. This system achieves a risk reduction of approx. $1{,}3 \times 10^2$.~~

~~Combining the software based SIS with the simplex relay SIS results in an overall theoretical risk reduction of $4{,}3 \times 10^5$ ($3{,}3 \times 10^3 \times 1{,}3 \times 10^2$). While combining the performance as shown above appears to be theoretically possible (since either SIS could shut the process unit down), once again, common cause factors have to be taken into account, and the achieved risk reduction will be somewhat less due to these factors.~~

Further guidance on how to evaluate the dependency and common cause between protection layers is given in Annex J of IEC 61511-3:—.

A.9.2.7 See guidance on how to evaluate the dependencies and common cause effects between protection layers in Annex J of IEC 61511-3:—.

~~**9.3 Additional requirements for safety integrity level 4**~~

A.9.2.8 No further guidance provided.

A.9.2.9 No further guidance provided.

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

A.9.3.1 The BPCS may be identified as a protection layer subject to certain conditions. ~~If functions are implemented in the BPCS for the purpose of reducing the process risk, the BPCS can be allocated a risk reduction for the identified risks it is intended to reduce.~~

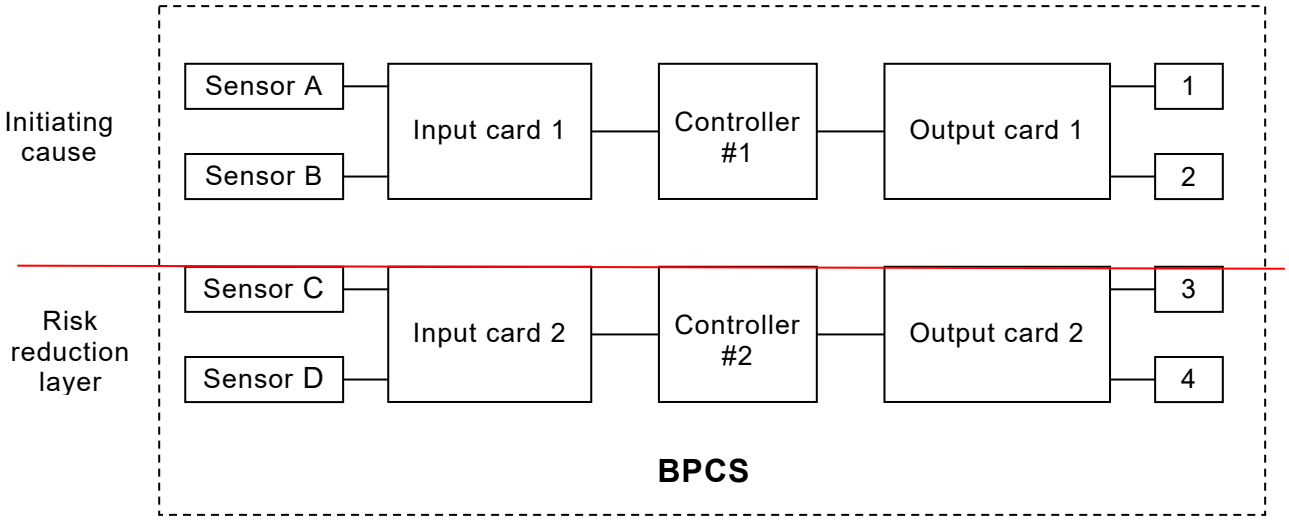
SIFs may not be implemented in the BPCS unless the BPCS is designed in accordance with the standard. IEC 61511-1:2016, 11.2.4 states, “If it is intended not to qualify the BPCS to this standard, then the SIS should be designed to be separate and independent to the extent that the safety integrity of the SIS is not compromised.” Designing and managing the BPCS as a SIS requires the application of the life-cycle requirements in the standard, including the hazard and risk analysis, design documentation, functional safety management, validation of changes, and management of change.

Risk reduction can only be allocated to one BPCS protection layer, unless the requirements of 9.3.4 and 9.3.5 of IEC 61511-1:2016 are met and further quantitative risk analysis in accordance with IEC 61511-1:2016 is conducted. This analysis is not trivial and involves a detailed assessment of the overall BPCS design, including hardware, software, communications, power supplies, interfaces, etc. At a minimum, this analysis should take into account the integrity of the hardware, separation of the protection layers to prevent common cause failures, management of the application programming systematic errors, access security to hardware and software, management of changes, operator interaction, configuration control, and periodic validation.

AVA Documents
Document Sharing Hub

When considering a BPCS protection layer, the design and management of the BPCS should be assessed to ensure that the likelihood of common cause, common mode, and systematic failure between the BPCS protection layer and the initiating source and between the BPCS protection layer and other protection layers is sufficiently low in comparison to the overall risk reduction requirements for the BPCS.

A.9.3.2 Risk reduction of ~~less than~~ ≤ 10 may be claimed from ~~instrumented systems~~ a BPCS protection layer without the need to comply with IEC 61511-1:2016. This allows the BPCS to be used for some risk reduction without the need to implement ~~such systems~~ BPCS protection layers to the requirements of IEC 61511-1:2016. ~~Any claim made should be justified by consideration of the integrity of the BPCS (determined by reliability analysis or performance data) and the procedures used for configuration, modification and operation and maintenance. When allocating risk reduction to functions in the BPCS, it is important to ensure that access security and change management are provided. The risk reduction that can be claimed for a BPCS function is also determined by the degree of independence between the BPCS function and the initiating cause. Figure 2 illustrates independence of the BPCS function and the initiating cause.~~



~~**Figure 2 – BPCS function and initiating cause independence illustration**~~ *IEC 1828/03*

~~For example, consider the case where a flow control loop is the initiating cause. This initiating cause includes a flow transmitter, a controller, and a control valve. In order to allocate risk reduction to a pressure control loop in the BPCS, the pressure transmitter should be wired to an independent controller, modulating an independent final element (for example, vent valve to flare system).~~

The risk reduction claim of ≤ 10 for the BPCS protection layer should be justified by consideration of the risk reduction capability of the BPCS (determined by reliability analysis or prior use data) and the procedures used for configuration, modification and operation and maintenance.

Any BPCS protection layer should be documented in a functional specification, which describes how the BPCS is designed, maintained, inspected, tested, and operated to achieve the allocated risk reduction.

Faults associated with devices of the BPCS protection layer may be revealed through process operation, automated diagnostics, mechanical integrity activities, or initiation of another hazardous event but not the one where it is used for risk reduction. Detection of a fault should result in the BPCS protection layer taking a specified action to achieve or maintain a safe state. The specified action (fault reaction) required to achieve or maintain a safe state may consist, for example, of the safe shutdown of the process (or that part of the process that

AVA Documents Document Sharing Hub

relies on the faulty SIS subsystem for risk reduction) or a specified compensating measure that ensures safe operation whilst repair is completed. The fault reaction should be able to take effect in less than the process safety time.

When allocating risk reduction to a BPCS protection layer, it is important to ensure that access security and change management are provided. Administrative controls should be used to control access to and modification of the protection layer within the BPCS. Bypassing a BPCS protection layer (e.g., placing BPCS function in manual) should require approval and compensating measures should be in place prior to bypassing to ensure the required risk reduction is maintained. Means should be provided to validate the functionality of the protection layer after changes are made to the BPCS that could affect the operation of the BPCS protection layer.

A.9.3.3 No further guidance provided.

A.9.3.4 The risk reduction that can be claimed for a BPCS protection layer is also constrained by the degree of independence between the BPCS protection layer, other protection layers and the initiating source of the hazardous event.

A detailed analysis of the overall BPCS should demonstrate that the control and protective devices within the BPCS are sufficiently independent and separate, such that it is possible to conclude that a failure of the BPCS as an initiating source has a sufficiently low probability of causing the failure of the BPCS protection layer. In such cases, it may be appropriate to take credit for a BPCS protection layer, even if the BPCS can initiate the hazardous event.

When a BPCS is the initiating source, no more than one BPCS protection layer may be claimed for the same hazardous event, unless the BPCS is designed and managed in accordance with IEC 61511-1:2016. Figure A.2 illustrates independence of the BPCS protection layer and an initiating cause in the BPCS.

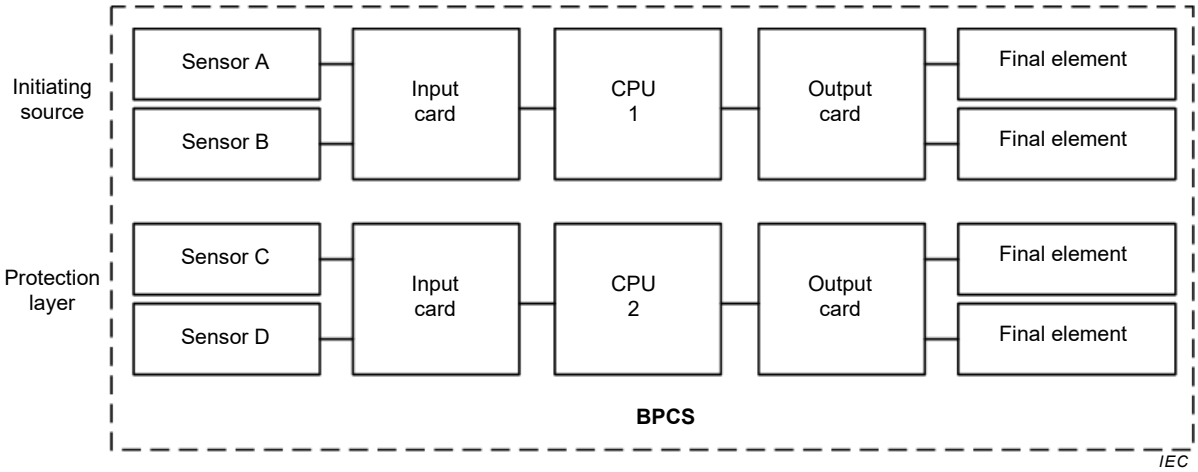


Figure A.2 – Independence of a BPCS protection layer and an initiating source in the BPCS

For example, consider the case where a flow control loop is the initiating source. This initiating source includes a flow transmitter, a BPCS logic solver, and a control valve. In order to allocate risk reduction to a pressure vent in the BPCS, the pressure transmitter should be wired to an independent BPCS logic solver, which actuates an independent final element (e.g., vent valve to flare system). The protection layer may also be an alarm and operator response function.

Documents
Document Sharing Hub
Full document details: IEC 61511-2 2016 RLV

When making claims for the BPCS as an initiating source and as a protection layer for the same hazardous event, the overall BPCS (including any of its devices as illustrated in Figure A.2) should be designed and managed such that it supports the claimed average frequency of failure (e.g., $\leq 10^{-5}$/hr × $\leq 10^{-1}$ = $\leq 10^{-6}$/hr). The claim should be justified by a quantitative analysis of the BPCS that considers the likelihood of common cause and common mode failures between the devices comprising the BPCS. Common cause due to random and systematic failures may limit the capability of the BPCS to achieve the claimed average frequency of failure.

When the initiating source is not related to failure of a BPCS, no more than two protection layers may be claimed for the same hazardous event, unless the BPCS is designed and managed in accordance with IEC 61511-1:2016. Figure A.3 below illustrates independence of two BPCS protection layers allocated to the BPCS.

A.9.3.5 When making claims for two BPCS protection layers for the same hazardous event, the overall BPCS (including any of the devices as illustrated in Figure A.3) should be designed and managed such that it supports the claimed risk reduction (e.g., ≤1/10 × ≤1/10 = ≤1/100). The conditions and considerations in IEC 61511-1:2016 9.4.1 and 9.4.2 apply to both BPCS protection layers. The claimed risk reduction should be justified by a quantitative analysis of the BPCS that considers the likelihood of common cause and common mode failures between the devices comprising the BPCS. Common cause due to random and systematic failures may limit the capability of the BPCS to achieve the claimed risk reduction.

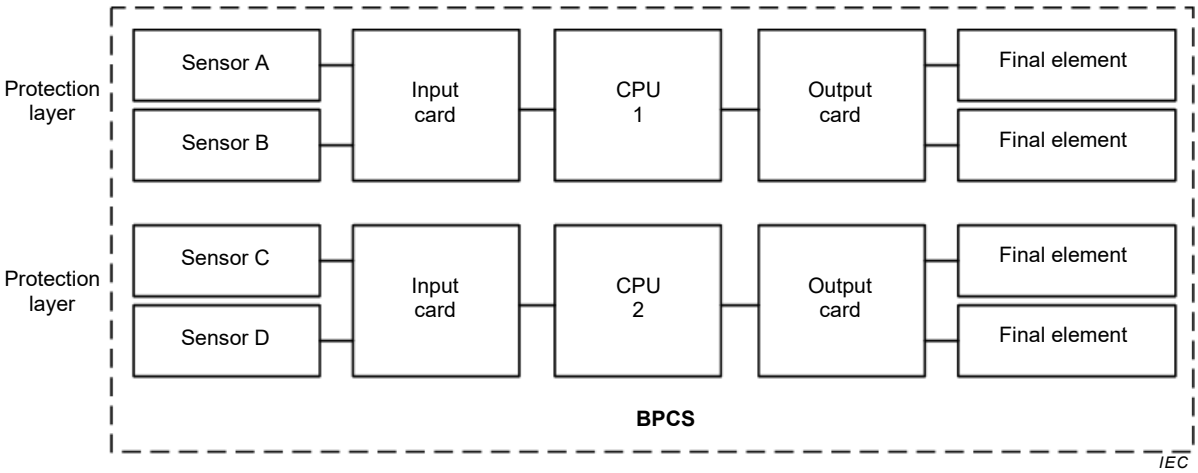


Figure A.3 – Independence of two protection layers allocated to the BPCS

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

A.9.4.1 An important issue to be considered at an early stage is whether there are any common cause failures between redundant parts within each layer (e.g., between 2 pressure relief valves on the same vessel), between safety layers or between safety layers and the BPCS. An example of this could be where failure of a BPCS measurement could cause a demand on the SIS and a device with the same characteristics is used within the SIS. In such cases it will be necessary to establish if there are credible failure modes that could cause failure of both devices at the same time. Where a common cause of failure is identified then the following actions can be taken.

a) The common cause can be reduced by changing the design of the SIS or the basic process control system. Diversity of design and physical separation are two effective methods of reducing the likelihood of common cause failures. This is usually the preferred approach.

Documents
Document Sharing Hub
Full document details: IEC 61511-2 2016 RLV

b) The likelihood of the common cause event should be taken into account when determining whether the overall risk reduction is adequate. This may require a fault tree analysis to be constructed that includes demand causes as well as protection system failures. Common cause failures can be represented on such fault trees and their effect on overall risk can be quantified through appropriate modeling methods.

It should be noted that any sensors or actuators that are shared by the BPCS and SIS are very likely to introduce common cause failures~~ and that the approach to such sharing of devices should be as discussed in this subclause~~.

A.9.4.2 The considerations listed below apply when an assessment is carried out on the likelihood of common cause, common mode and dependent failures. The extent, formality and depth of the assessment will depend on the SIL of the intended function. The effect of common cause, common mode and dependent failures may be dominant for SIL 3 or~~ higher~~ SIL 4. The following should be considered:

- independence between protection layers – a failure modes and effects analysis should be carried out to establish if a single event can cause failure of more than one protection layer or failure of the BPCS and a protection layer. The depth and rigor of the analysis will depend on the risk;
- diversity between protection layers –the aim should be diversity between protection layers and the BPCS but this is not always achievable.~~ An example could be over pressure protection where a failure of the BPCS pressure control loop would cause a demand. The BPCS and the SIS will both require pressure measurement and there will be a limit on the suitable equipment available.~~ Some diversity can be achieved by using equipment from different manufacturers but if SIS and BPCS sensors are connected to the process using the same type of hook up, then the diversity may be of limited value;
- physical separation between different protection layers – physical separation will reduce the impact of common cause failures due to physical causes. Measurement connection locations for BPCS and SIS should be given maximum physical separation subject to functional needs such as accuracy and response time.

A.10 SIS safety requirements specification

A.10.1 Objective

The development of the SIS SRS is one of the most important activities of the whole SIS safety life-cycle. It is through this specification that the user is able to define how he wants each SIF to be designed and integrated into a SIS.

Final validation of the SIS is carried out using this specification.

A.10.2 Guidance to "General requirements"

~~10.2.1~~ The SIS SRS may be a single document or a collection of several documents including procedures, drawings or corporate standard practices. These requirements may be developed by the H&RA team and/or the project team itself.

A.10.3 Guidance to "SIS safety requirements"

A.10.3.1 As described in IEC 61511-1:-, there are a number of design requirements that ~~need to~~ should be defined early in a project to ensure the SIF provides the desired protection.

~~Safety requirements specifications for individual subsystems may also be derived from this overall specification.~~

Some considerations with respect to the SRSs are as follows:

Documents
Document Sharing Hub
Full document details: IEC 61511-2 2016 RLV

a) The first items that ~~will need to~~ should be defined are the SIF along with its SIL. An example of a SIF is "protect the reactor from overpressure by shutting down the inlet valves on high pressure". Typically the function description will comprise the following ~~elements~~ topics:

- Which ~~measurements need to be taken to detect the onset of~~ process parameters should be monitored to detect the hazardous conditions

  EXAMPLE A pressure rise above a specified value ~~needs to be~~ is detected. The value of the parameter at which action ~~should be~~ is taken ~~will need to be~~ is outside the normal operating range and less than the value that will result in the hazardous condition. An allowance ~~will need to be~~ is made for the response of the system and the accuracy of measurement. In setting the limit, ~~there will therefore need to be~~ a discussion with those responsible for the design and implementation of the SIS took place.

- The actions that ~~need to~~ should be taken ~~that will~~ and when they should be taken to prevent the hazardous ~~condition~~ event. A simple example could be to reduce the flow of steam to a reboiler within a specified time. It should be noted that it is not usually sufficient to state that steam flow to the reboiler should be shut-off. The designer will need to know what is necessary for successful operation. In heating duties it may for example be sufficient to reduce flow to less than 10 % of flow within one minute. In other examples it may be necessary to have tight shut-off within a few seconds.

- The actions not needed to prevent the hazardous ~~condition~~ event that may be of benefit for operational reasons. Such actions may include presentation of alarms, shut down of upstream or downstream units to reduce demands on other protection systems or actions that will enable fast start up once the cause of the hazard has been eliminated. It is important to separate these non-safety actions from the actions necessary to prevent the hazardous condition so as to ~~minimize costs and~~ restrict the boundary of the SIS to what is necessary.

- Any identified process states or sequences of the SIS operation which should be prevented because they will result in hazardous situations. A further analysis of risk should be needed after design of the SIS to consider if partial failures or spurious operation of the SIS could result in a new hazard or be an additional cause of a hazard already identified.

b) This specification should define the safe state of the process for each identified function in terms of which flows should be started or stopped, which process valves should be opened or closed and the state of operation of any rotating equipment (pumps, compressors, agitators). If bringing the process to a safe state involves sequencing, the sequencing ~~should~~ can also be identified.

~~NOTE~~ In defining the final elements, consideration ~~should~~ can be given to the benefits of diversity, for example, shutting off the product stream and shutting off the steam flow to reduce high pressure.

c) The requirement for a desired proof test interval ~~should~~ can be defined at the beginning so the design of the SIS can take it into consideration. For example, if proof testing is to be performed during planned shutdowns (e.g., every 3 years), the design might require more redundancy than if the proof test interval is to be annual.

Consideration can be given to:

- test duration;
- state of the tested device (off-line/on-line);
- state of the process during test;
- detection of common cause failures;
- prevention of errors (such as the SIS remains isolated after test complete);
- test documentation requirements;
- archiving requirements;
- the need to ensure management is aware of what is planned;
- the need to ensure adjacent and other impacted areas are aware of the impending test;

AVA Documents Document Sharing Hub

Full document details: IEC 61511-2 2016 RLV

- the technical qualification and experience of the person(s) developing the test procedures;
- the technical qualification and experience of the person(s) implementing the test procedures.

d) The maximum allowable response time of a SIS starts when the process is at trip condition, and ends at the last time when the final elements reaching their safe states will still be able to prevent the hazard. Requirements for being able to manually bring the process to a safe state should be defined. For example, if there is a requirement for the operator to be able to manually shutdown a piece of equipment from either the control room or from a field location, then this ~~needs to~~ should be specified. Any requirement for independence of manual shutdown switches from the SIS logic solver also ~~needs to~~ should be defined.

e) All requirements for restarting the process after a shutdown ~~need to~~ should be specified. For example, some users have electronic reset switches on the main control panel or in the field and others like to use solenoids with latching handles. If there is a specific requirement like this reset action, it should be part of the SRS.

f) If there is a target frequency for nuisance trips, this also should be specified as part of the SRS. This will be a factor in the design of the SIS.

g) The interfaces between the SIS and the operator ~~need to~~ should be fully described, including alarms (pre-shutdown alarms, shutdown alarms, bypass alarms, diagnostic alarms), graphics, sequence of events recording.

h) There may be a need for bypasses to allow the SIS to be tested or maintained while the process is running. If there are specific requirements for bypassing such devices as key lock or passwords, these also ~~need to~~ should be specified as part of the SRS.

i) The failure modes and response of the SIS on the detection of faults should be defined. For example, a transmitter can be ~~designed~~ configured to fail toward a trip condition or away from a trip condition. If it is designed to fail away from the trip condition, then it is important that the operator gets an alarm on the transmitter failure and is trained to take ~~the necessary~~ corrective actions ~~to get the transmitter repaired as quickly as possible~~. See also IEC 61511-1:2016, 11.3 relating to requirements on detection of a fault.

A.10.3.2 No further guidance provided.

A.10.3.3 This subclause relates to application programming safety requirements guidance. An AP SRS identifies the minimum capabilities of the PE AP functionality and also constrains the development of any functionality which would result in an unsafe condition. The AP safety requirements that have already been specified in the requirements for the SIS need not be repeated as a separate AP SRS.

The AP SRS typically takes into account the SIS system architecture. The system architecture defines the major devices, SIS subsystems, embedded software and AP, as well as how they are interconnected and how the required attributes, particularly safety integrity, are achieved. Examples of embedded software modules include operating systems, databases, and communication SIS subsystems. Examples of AP modules include application functions which are replicated throughout the plant.

The AP architecture should also be determined by the underlying architecture of the SIS subsystem(s) provided by the supplier(s). The AP architecture should not undermine the hardware redundancy – for example if the processor redundancy is lower (e.g., 1 out of 1) than the sensor redundancy (e.g. 2 out of 3) then the associated AP should facilitate the required voting of the sensors (i.e., 2 out of 3).

The detailed functional safety requirements for each SIF can typically be defined by use of logic diagrams or cause and effect (see Figure D.2) drawings. In many cases, the programming languages provided by the logic solver vendor can be used to define the requirements. Typical languages that can be used are function block diagram or cause effect matrix. Specialised formats such as unified modelling language (UML) are also available and

AVA Documents
Document Sharing Hub

useful when the use of model checking techniques is foreseen. The vendor supplied language selected should be suitable for the application. The use of the vendor supplied languages to define the detailed requirements can often avoid errors that occur in the translation of the requirements from other forms of documentation. Liberal use of comments should be provided to define safety and non-safety functions and the SIL requirements of all safety functions.

It may be appropriate to implement additional requirements beyond those necessary for the basic individual SIF functional behavior (e.g. to manage the plant shutdown and start up) either in the BPCS or in a completely separate part of the application programme from the SIF, with clear links into the SIF. In addition the AP may include functions to implement the overall SIS architecture, end to end diagnostics and behavior under abnormal conditions. For example, the architecture of the sensors (voting principle: 1oo2, 2oo3, etc.) associated with the SIF in combination with the safety principle ''De-energise to Trip'' or ''Energise to Trip'' define how the sensor voting should be realised in the AP. It is important to ensure that no combination of the additional functions can override the basic application safety functions.

If multiple SISs are used to implement a single SIF, documentation should be provided to explain which functions are to be implemented in each SIF. If multiple SIFs are used to implement the same overall SIF (e.g. to combine two lower SIL rated SIFs to achieve a higher SIL) then the interaction and independence of each SIF should be documented. (See Clause F.4, System Architecture and IEC 61511-3:—, Annex J).

NOTE 1 An AP SRS identifies the minimum capabilities of the PE AP functionality and also constrains the development of any functionality which would result in an unsafe condition.

NOTE 2 The AP safety requirements that have already been specified in the requirements for the SIS need not be repeated.

NOTE 3 The system architecture defines the major devices and SIS subsystems of embedded software and AP, how they are interconnected, and how the required attributes, particularly safety integrity, are achieved.

NOTE 4 The AP architecture can take into account the underlying architecture of the SIS subsystem(s) provided by the supplier(s).–The AP architecture should not undermine the hardware redundancy – for example if the processor redundancy is lower (e.g., 1 out of 1) than the sensor redundancy (e.g., 2 out of 3) then the associated AP should facilitate the required voting of the sensors (e.g., 2 out of 3).

NOTE 5 An SIS usually consists of three architectural SIS subsystems: sensors, logic solver and final elements. Furthermore, SIS subsystems could have redundant devices to achieve the required integrity level.

NOTE 6 An SIS hardware architecture with redundant sensors can place additional requirements on the SIS logic solver (e.g., implementation of 1oo2 logic).

Any conflicts, discrepancies and omissions in the SIS SRS which come to the attention of the AP designers should be addressed. One example might be the effect of the order of execution of the SIF within the AP. Another example would be the response of the AP as it relates to energy outages.

NOTE 7 The AP designers can review the information in the specification to ensure that the requirements are unambiguous, consistent and understandable. Any deficiencies in the specified safety requirements can be identified to the SIS designer.

NOTE 8 As the AP safety requirements and the possible AP architecture become more precise, there may be an impact on the SIS hardware architecture (see Figure A.4 below) and, for this reason, close cooperation between the SIS architecture developer, the SIS subsystem supplier and the AP developer can be essential.

Documents
Document Sharing Hub

Full document details: IEC 61511-2 2016 RLV

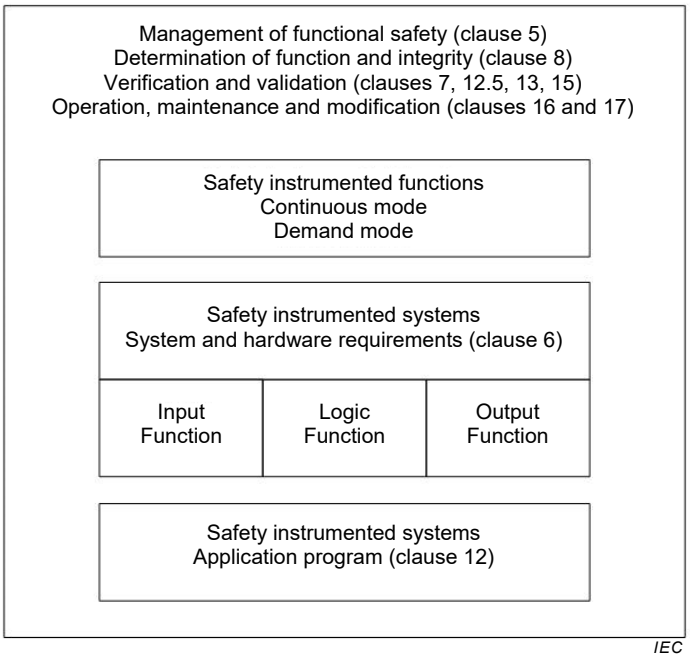


Figure A.4 – Relationship of system, SIS hardware, and SIS application program

The AP SRS should include all necessary functions during all modes of operation of the process being protected, including start-up permissive, operation, shutdown and additionally, the periodic testing of the SIF. This typically requires the definition of maintenance override capabilities so that the sensors and final elements can be tested without shutting down the process. Factors to be addressed include:

a) functionality and timing requirements needed to implement the user-defined SIF;

b) AP system's interface with the process and people;

c) relationship between the process hazards and the functionality provided by the AP;

d) boundaries of behaviour of the AP which are permitted in order to remain within the safety envelope of the process (e.g., must be able to deal with erroneous input conditions);

e) allowable functionality of the utility software provided within the logic solver, (e.g., prioritization of the safety logic and I/O over communications, error handling and logic solver diagnostics);

f) hardware platform and embedded software on which the AP executes and the configuration of the hardware and embedded software;

g) hazards which could arise in the process as a result of the functionality of the system of which the AP is a part (e.g., inappropriate hardware failure modes on removal of power);

h) constraints on the methods and procedures which could be used by the designers as a result of the safety manual for the supporting logic solver;

i) Data integrity and reasonableness checks, for example end-to-end checks in communication links, bounds checking on sensor inputs, bounds checking on data parameters and diverse execution of application functions;

j) the detection criteria for and response to detected logic solver hardware faults and to failed data integrity and reasonableness checks;

In order to avoid difficulties at later stages of the development process, it is also important to consider the strategy by which it is intended to show that the AP requirements have been achieved.

Documents
Document Sharing Hub
Full document details: IEC 61511-2 2016 RLV

A.10.3.4 In the case of FPL (devices (e.g. Intelligent Sensors, Smart Transmitters, HMI graphic panels) the requirements for configuration of the devices can be specified as part of the SRS.

A.10.3.5 Clauses B.1, F.17, F.20 and G.2 provide additional guidance for the implementation of IEC 61511-1:201610.3.2.3 and of how the AP safety requirements might look. The additional guidance provided is diverse in terms of width of scope, AP language and process application, complexity, in order to depict the variety of the existing possibilities typically satisfying this.

A.10.3.6 For an example of how to structure AP safety requirements see Clause B.3.2.1 and Annex F, Step F.3.

A.11 SIS design and engineering

A.11.1 Objective

The objective of A.11.1 is to provide guidance in the design of the SIS. Each SIF has its own SIL. A ~~component~~ device of a SIS, for example, a logic solver, may be used by several SIF with different SILs.

A.11.2 Guidance to "General requirements"

A.11.2.1 No further guidance provided.

A.11.2.2 ~~No further guidance provided.~~ For AP guidance see A.12.2.4.

A.11.2.3 ~~No further guidance provided.~~ Where the AP in a SIS is to implement SIFs of different SILs, they should be clearly labelled. This allows the AP of each SIF to be traceable to the proper sensor and final element redundancy. It also allows the functional and validation testing of the functions to be commensurate with the SIL. The labelling should identify the SIF and the SIL.

A.11.2.4 Sometimes SIS devices are additionally used by the BPCS for operational reasons. IEC 61511–1:—, Clause 11, has a number of design requirements for ~~a~~ SIS. One item of concern is independence between the SIS and the BPCS.

The SIS is normally separated from the BPCS for the following reasons:

~~a) To reduce the effects of the BPCS on the SIS, especially when they share common equipment. For example if the BPCS and SIS share a common valve for shutdown and control, then in the event of a dangerous failure of that valve, it would not be available to perform a SIS shutdown function.~~

~~b) To retain flexibility for changes, maintenance , testing and documentation relating to the BPCS.~~

~~NOTE 1 The SIS normally has more robust requirements than the BPCS and the intent is not to subject the BPCS to the same robust requirements that are required for the SIS. However it should be noted that uncontrolled BPCS modifications can be a cause of increased demand on the SIS.~~

~~c) To facilitate the validation and functional safety assessment of the SIS.~~

~~d) Access to the programming or configuration functions of the BPCS may need to be limited to meet the modification management arrangements if the BPCS is combined with the SIS.~~

~~Where a failure of the common equipment can cause a demand on the SIS, then an analysis should be conducted to ensure the overall hazard rates satisfies the expectations. The overall hazard rate will be the sum of the dangerous failure rate of the common elements and the~~

AVA Documents
Document Sharing Hub
Full document details: IEC 61511-2 2016 RLV

~~hazard rate from other sources of demand (including dangerous failure of the independent parts of the SIS).~~

a) To reduce common cause, common mode and systematic failures, minimizing the impact of BPCS failure on the SIS.

NOTE 1 A separate SIS and BPCS is aligned with the concept of protection layers. The separate SIS is an independent protection layer when the BPCS fails.

b) To retain flexibility for changes, maintenance, testing and documentation relating to the BPCS.

NOTE 2 The SIS normally has more robust requirements than the BPCS and the intent is not to subject the BPCS to the same robust requirements that are required for the SIS. However, uncontrolled BPCS modifications can be a cause of increased demands on the SIS.

NOTE 3 Separation of SIS and BPCS allows for separate maintenance of the respective systems, often by different operating staff.

NOTE 4 Access to the programming or configuration functions of the BPCS can be limited to meet the SIS management of change and configuration management requirements if the BPCS is combined with the SIS.

NOTE 5 Means can be provided to validate the SIS after changes are made to any devices shared between the BPCS and SIS.

c) To facilitate the identification and management of the SIS devices, making the validation and FSA of the SIS more straightforward and clear.

d) To support access security and enhance cyber security for the SIS, such that revision to BPCS functions or data do not impact the SIS.

NOTE 6 Shared interfaces and devices can be managed as SIS components and devices unless hardware and software configuration provides functional separation.

NOTE 7 Special considerations can be given to restriction of writes to prevent unauthorized or unintended writes to the SIS.

e) To reduce the amount of analysis that should occur to ensure that the SIS and BPCS are properly designed, verified, and managed.

NOTE 8 Where a failure of common equipment can cause a demand on the SIS, an analysis can be conducted to ensure the overall average frequency of failure satisfies the expectations. The analysis can cover all BPCS and SIS devices such as sensors, logic solvers, final elements, data communications, utilities, operator stations, and engineering workstations.

If any BPCS device is shared with the SIS, further analysis should be conducted to demonstrate that the design and management of the BPCS device:

- achieves the functional requirements for the BPCS function and the SIF;

  NOTE 9 The failure of any hardware or software outside the SIS can not prevent any SIF from operating correctly.

- meets the integrity requirements necessary to achieve the target average frequency of failure for the combined system;

  NOTE 10 The failure of a BPCS device can not result in the initiating cause for the hazardous event or the dangerous failure (or defeat/bypass) of the SIF that protects against the specific event under evaluation, unless a redundant device is able to actuate the SIS. An analysis can be carried out to evaluate the effect of sharing of BPCS and SIS devices.

  NOTE 11 The probability of common mode, common cause or dependent failures, such as plugged lead lines, maintenance activity including bypasses, incorrectly operated line isolation valves, etc., can be adequately evaluated and determined to be sufficiently low.

- is managed according to IEC 61511-1:2016, including proof testing, access security and management of change.

Separation between the SIS and the BPCS may use identical or diverse separation. Identical separation would mean using the same technology for both the BPCS and SIS whereas diverse separation would mean using different technologies from the same or different manufacturer.

Compared with identical separation, which helps against random failures, diverse separation offers the additional benefit of reducing the probability of systematic faults ~~and of reducing common cause failures~~ affecting multiple channels at the same time and/or from the same cause and hence reduces correlated failure of multiple channels.

AVA Documents
Document Sharing Hub

Full document details: IEC 61511-2 2016 RLV

Identical separation between the SIS and BPCS may have some advantages in design and maintenance because it reduces the likelihood of maintenance errors. This is particularly the case if diverse ~~components~~ devices are to be selected which ~~have~~ has not been used before within the user's organization.

Identical separation between SIS and BPCS may be acceptable for SIL 1 and SIL 2 ~~and SIL 3~~ applications although the sources and effects of common cause failures should be considered and their likelihood reduced. Some examples of common cause failures are:

- plugging of instrument connections and impulse lead lines;
- corrosion and erosion;
- hardware faults due to environmental causes;
- software errors;
- power supplies and power sources;

  NOTE 12 Utilities (e.g., power supply) can be analyzed by conventional reliability methods. The use of beta factor is not relevant in this case.

- human errors.

~~Diverse separation offers the additional benefit of reducing the probability of systematic failures (a factor especially important in SIL 3 and SIL 4 applications) and reducing common cause failures.~~

There are four areas where separation between the SIS and BPCS is generally provided:

- field sensors;
- final elements;
- logic solver;
- wiring.

Physical separation between BPCS and SIS may not be necessary provided independence is maintained, and the equipment arrangements and the procedures applied ensure the SIS will not be dangerously affected by:

- failures of the BPCS; and
- work carried out on the BPCS e.g., maintenance, operation or modification.

Where procedures are necessary to ensure the SIS is not dangerously affected, the SIS designer ~~will then need to~~ should specify the procedures to be applied.

a) Field sensors

Using a single sensor for both the BPCS and SIS requires further review and analysis. The additional review and analysis is necessary because a failure of this single sensor could result in a hazardous situation.

NOTE 13 For example, a single level sensor used for both the BPCS and a SIS high level trip could create a demand if the sensor fails low (i.e., below the set point of the level controller). As a result of the sensor failing low, the controller would drive the valve open. Since the same sensor is used for the SIS, then it will not detect the resultant high level condition.

Where a single sensor is used for both a BPCS and SIS function, the requirements of IEC 61511-1:2016 will normally only be satisfied if the sensor diagnostics can reduce the dangerous failure rate sufficiently and the SIS is capable of placing the process in a safe state within the required time. ~~In practice this is difficult to achieve even for SIL 1 applications. For a SIL 2, SIL 3 or SIL 4 safety instrumented function, separate SIS sensors with identical or diverse redundancy will normally be needed to meet the required safety integrity.~~

Shared sensor (e.g. transmitter, analyzer, and switch) should be powered by the SIS. Consideration should also be given to the compensating measures to be implemented

AVA Documents Document Sharing Hub

during periods where the shared device is out of service due to detected faults, maintenance or testing. For higher SILs, separate SIS sensors with identical or diverse redundancy will normally be needed to meet the required safety integrity.

~~NOTE 2 When~~ Where a single separate SIS sensor is used, there may be advantages to repeating the signal to the BPCS through suitable isolators or other means that ensure that no failure of the BPCS causes a dangerous failure of the SIS. Such an arrangement can lead to improved diagnostic coverage by allowing signal comparison between BPCS and SIS sensors.

When redundant SIS sensors are used, the sensors may also be connected to the BPCS through suitable isolators or other means that ensure that no failure of the BPCS causes a dangerous failure of the SIS. Suitable algorithms in the BPCS such as “middle of three” may increase safety by reducing the demand rate on the SIS.

For a SIL 2, SIL 3 or SIL 4 SIF, separate SIS sensors with identical or diverse redundancy will normally be needed to meet the hardware fault tolerance requirements and the required safety integrity.

b) Final Element

~~In the same way as for~~ Similar to the sensors, using a single ~~valve~~ final element for both the BPCS and SIS requires further review and analysis, since the failure of the single final element could result in a hazardous situation. ~~In general, a single valve used for both the SIS and BPCS in not recommended if a failure of the valve would place a demand on the SIS.~~

NOTE 14 For example, a single valve used for both the SIS and BPCS can create a demand if the valve fails in the open position and a dangerous failure of the SIS if the valve fails to close as specified when the demand occurs.

Where a single ~~valve~~ final element is used by both the BPCS and SIS functions, the requirements of IEC 61511-1:2016 will normally only be satisfied if the ~~valve~~ final element diagnostics can reduce the dangerous failure rate sufficiently and the SIS is capable of placing the process in a safe state within the required time.

In practice, this is difficult to achieve for SIL 1 applications even when the shared final element design ensures that the SIS action overrides the BPCS action. Consideration should also be given to the compensating measures to be implemented during periods where the shared device is out of service due to detected faults, maintenance or testing. For a SIL 2, SIL 3 or SIL 4 SIF, separate SIS ~~valves~~ final elements with identical or diverse redundancy will normally be needed to meet the required safety integrity. SIS action overriding the BPCS can, as an example, be achieved for a pneumatically operated valve by having the SIS directly connected to a solenoid operated valve that vents the air from the valve actuator, e.g., located between the valve positioner and the actuator. For electrically operated valves, the wiring can be such that the SIS places and maintains the control valve in the safe state until reset.

~~Where a single valve is used for both BPCS and SIS functions, the design should ensure that the SIS action overrides the BPCS action. This is normally achieved by having the SIS directly connected to a solenoid valve that removes the power source directly at the actuator, for example, between the valve positioner and the actuator.~~

When redundant ~~SIS valves~~ final elements are used, the ~~valves~~ final elements may be connected to both the SIS and BPCS.

~~NOTE 3~~ Even with redundant ~~valves~~ final elements, ~~it is important to~~ consider common cause failures between the BPCS and SIS.

Staggering the tests of redundant valves, and provided a relevant procedure is implemented, may reduce the impact of common cause failures.

When the final element is a valve, additional considerations ~~for determining the valve requirements~~ are:

- The valve is designed such that there is no BPCS failure that could result in the SIS not being able to take action with the shared valve.
- The valve design is functionally compatible with both SIS and BPCS service.

NOTE 15 This can be difficult as many BPCS valves are installed “flow to open” and many SIS valves are installed “flow to close.” Actuator power requirements for a SIS valve may differ from that of a control valve.

AVA Documents Document Sharing Hub

- Shutoff requirements.

NOTE 16 The process leakage rate through the control valve can be tolerable when not affecting the ability of the SIF to perform the specified function and prevent the hazard.

- The shared final element design should ensure that the SIS action overrides the BPCS action.
- Reliability experience with the valve in similar process applications.
- Unsafe failure modes of the valve.
- Operating procedures~~that make the valve less effective (for example, bypass valves being opened)~~ to ensure the SIS integrity.

NOTE 17 For example, bypass valves can be locked in the closed position and subject to management procedures, and similarly, valves located in return lines (e.g., hydraulic) of a spring-to-close valve locked in the open position.

- Proof testing requirements.

NOTE 18 Consideration can be given to any partial stroke testing or on-line testing requirements and how it may affect operations.

c) Logic Solver

The ability to achieve separation and independence with BPCS and SIS logic solvers varies with the technology (i.e., electrical, electronic, and programmable electronic) used in the application.

- Electrical

  Many past and some existing processes utilize BPCSs with pneumatic technology and SISs with electrical technology. Separation and independence in this type of application is readily achievable with these technologies since they require different enclosures, different physical layouts, and direct wiring communications.

- Electronic

  Many past and some existing processes utilize BPCSs with electronic technology having no embedded programmable electronic capability and SISs with electrical technology. Separation and independence in this type of application is readily achievable with these technologies. The use of electronic SISs without embedded programmable electronic technology is a viable approach as well.

- Programmable electronics (PE)

  Some applications utilize PE technology for their BPCS and electrical technology for their SIS. These configurations are inherently separate and independent since communications is direct wired and an integrated physical arrangement is not advantageous.

  Presently, the preferred BPCS/SIS technical arrangement in the process sector is to utilize PE technology for both the BPCS and the SIS. This configuration offers the maximum flexibility because of its ability to remotely alter the APs of the BPCS and the SIS and the ability to interchange information between the BPCS and the SIS. Unfortunately these characteristics can be counterproductive when trying to maintain separation and independence between the BPCS and the SIS unless appropriate analysis is performed in the design stages of the safety life-cycle and functional independence is demonstrated (e.g., by diverse technology).

  The SRS (Clause 10 of IEC 61511-1:2016) should provide the guidance on how to achieve separation and independence with this BPCS and SIS technology arrangement. This effort has also received an added boost from the introduction of new tools providing added security to the BPCS and the SIS. See ISA TR84.00.09:2013 for practical BPCS/SIS control system configurations and security tools that provide varying levels of separation and independence between the SIS and the BPCS.

  Some PE logic suppliers provide controllers with the BPCS and the SIS in the same physical enclosure. Use of this approach should be preceded by careful analysis of the logic solver's safety manual and how the requirements it places on the operation and

AVA Documents
Document Sharing Hub
Full document details: IEC 61511-2 2016 RLV

maintenance of the BPCS and the SIS adhere to the facility's process safety management criteria and the SRS.

d) Wiring

On energize to trip systems, the BPCS and relevant field device wiring is normally separated from wiring to the SIS and its relevant field devices because of the possibility of accidentally deactivating the safety function without noticing it. Typical guidelines for these types of systems include installing separate multi-conductor cables and junction boxes dedicated to the SIS and BPCS. Where the wiring is not separated, use of good labeling and maintenance procedures is recommended to minimize the potential of errors caused during maintenance resulting in deactivation of the SIS ~~are suggested~~.

NOTE 19 Energize to trip refers to SIF circuits where the outputs and devices are de-energized under normal operation. Application of power (e.g., electricity, air) causes a trip action.

The cable support system (e.g., cable trays, conduit) may be common for both de-energize to trip and energize to trip systems, unless separation is required for other reasons (e.g., electromagnetic interference). On energize to trip systems, consideration ~~may~~ should be given to adding fire protection to the cable trays in fire risk areas.

A.11.2.5 ~~See 11.8 of this standard for guidance as well as following guidance relating to the Note in 11.2.5 of IEC 61511-1.~~

The operators, maintenance staff, supervisors and managers all have roles in safe plant operation. However, humans can make errors or be unable to perform a task, just as instruments and equipment are subject to malfunction or failure.

Human performance is therefore a system design ~~element~~ and integrity factor. The human machine interface (HMI) is particularly important in communicating the status of the SIS to operating and maintenance personnel.

Human reliability analysis (HRA) identifies conditions that cause people to err and provides estimates of error rates based on past statistics and behavioral studies. Some examples of human error contributing to chemical process safety risk include:

- undetected errors in design;
- errors in operations (e.g., wrong set point);
- improper maintenance (e.g., replacing a valve with one having the incorrect failure action);
- errors in calibrating, testing or interpreting output from control systems;
- failure to respond properly to an emergency.

NOTE Additional guidance can be found in the following references:

- ~~CCPS/AIChE Guidelines for Improved Human Performance in Process Safety, New York: American Institute of Chemical Engineers (1994).~~
- CCPS/AICHE Human Factors Methods for Improving Performance in the Process Industries (1st edition), John Wiley & Sons (2007), ISBN 0 4701 1754 0;
- Guidelines for Preventing Human Error in Process Safety (1st edition), John Wiley & Sons (2004), ISBN 08169 0461 8;
- CCPS/AIChE Guidelines for Chemical Process Quantitative Risk Analysis (second edition), New York: American Institute of Chemical Engineers (2000), 0 8169 0720 X;.
- HSE Reducing error and influencing behavior, HSG48, Health and Safety Executive, London (~~1999~~ 2009), ISBN ~~0 7176 2452 8~~ 978 0 7176 2452 2.
- ISA TR84.00.04:2015 part 1, Annex B, *Guidelines on the Implementation of ANSI/ISA-84.00.01-2004 (IEC 61511)*

A.11.2.6 No further guidance provided.

A.11.2.7 IEC 61511-1:2016 addresses the ~~potential~~ hazard that may be created if a SIS automatically restarts the process immediately after the trip condition is corrected. Each SIF

AVA Documents
Document Sharing Hub

Full document details: IEC 61511-2 2016 RLV

should be analysed to determine how it should be reset once the trip condition is corrected. Normally restarting should only be possible after a manual action of the operator.

An example of a function that would ensure that once placed in a safe state the process remains in the safe state is illustrated in Figure F.11 – sheet 4 – line 1 of this standard for guidance.

A.11.2.8 Manual means that are independent of both the SIS logic solver and the BPCS control system may be provided to allow the operator to initiate a shutdown in an emergency. The manual means of operating the SIS final element can be taken into account in meeting safety function integrity requirements, but the relevant human factors and common cause failures shall be properly considered. The requirements for manual shutdown are normally defined in the SRS.

In some cases, manual shutdown can offer additional risk to the facility (for example where shutdown sequencing is required); in this case the manual shutdown may be an input to the SIS to provide a staged shutdown.

The emergency stop may be connected to the SIS PE logic solver (e.g., when a sequenced shut down is required) provided that it is necessary and deemed appropriate by the H&RA team.

A.11.2.9 IEC 61511-1:2016 indicates the need for analysis of independence between the SIS and other protection layers, not just between the SIS and BPCS (see IEC 61511-1:2016, Figure 9).

Staggering of proof testing between the SIS and protection layers will reduce the probability of coincident failures.

Under some circumstances it may be acceptable that there is incomplete separation between BPCS and the SIS. This is particularly the case where a failure of the common equipment will not cause a demand on the SIS. In such cases, it is necessary to implement the common or shared equipment in accordance with IEC 61511-1:2016.

~~Where a failure of the common equipment can cause a demand on the SIS, then an analysis should be conducted to ensure the overall hazard rate satisfies the expectations. The overall hazard rate will be the sum of the dangerous failure rate of the common elements and the hazard rate from other sources of demand (including dangerous failure of the independent parts of the SIS).~~ Where the same type of equipment is used for both the BPCS and the SIS then if a common cause failure of the common equipment can lead to a hazardous event causing a demand on the SIS, then an analysis should be conducted to ensure the overall average frequency of failure satisfies the expectations. To establish the hazards associated with dangerous failures of the common equipment~~, the following cases should be considered:~~.

~~a) Where one element of the redundant configuration is used as a BPCS, consider the hazards arising from dangerous failures of common equipment taking into consideration the performance of the SIS which has been degraded by the failed instruments;~~

~~b) Where the shared instruments are not redundant, consider the hazards arising from dangerous failures of the common equipment assuming the SIS did not respond.~~

IEC 61511-1:2016 also indicates the need to ensure that the design of the interface between the SIS and other systems maintains the necessary independence – i.e., that the non-safety independence designed into the SIS is not undermined by the BPCS. For example if application data generated for use in the BPCS or other non-SIS devices and tools is used in the design of the SIS there would be a potential to propagate a common failure mode between the two systems. Another example would be an AP that allowed an override from the BPCS to be implemented in the system without a separate ‘permissive’ switch separate from the BPCS. Other examples arise from ‘mirroring’ where application data is ‘leaked’ to another system and start-up overrides.

AVA Documents
Document Sharing Hub